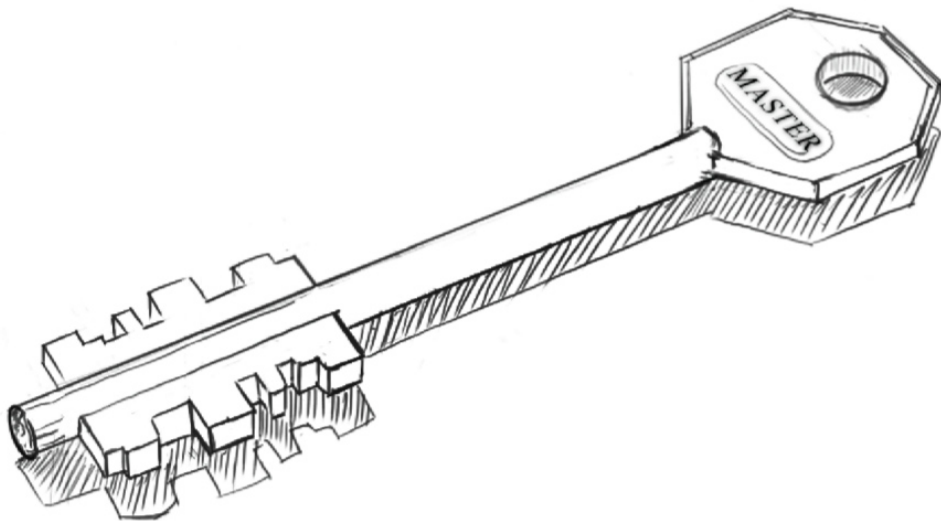


the
CryptoParty
handbook



the CryptoParty handbook
Version: 2015-07-14

Contents

1	Introducing Cryptoparty	13
1.1	About This Book	13
1.2	A CryptoParty Manifesto	15
1.3	How To CryptoParty	17
1.4	Party like it's december 31st 1983	20
1.4.1	What is CryptoParty?	20
1.5	Preface	21
1.6	Why Privacy Matters	21
2	Understanding Email	23
2.1	Basic Tips	23
2.1.1	In brief:	23
2.1.2	Passwords	23
2.1.3	Reading Email in Public Places	24
2.1.4	Cache Cunning	24
2.1.5	Securing your communication	25
2.1.6	DNSSEC & DANE	25
2.1.7	Account Separation	26
2.1.8	A note about hosted email	26
2.2	Types of Email	26
2.2.1	Remotely hosted email ('webmail'), resourced using a web browser	26
2.2.2	Remotely hosted email, resourced using an email program or using a web browser	27
2.2.3	Context considerations	27
2.2.4	Email & Metadata	28
2.2.5	Self-administered email server	28
2.2.6	'Free' email services	28
2.2.7	Non-profit	28
2.2.8	Notes on email forwarding	29
2.3	Fears	29
2.3.1	Random abuse and theft by malicious hackers	30
2.3.2	Targeted abuse, harassment, and spying	31
2.3.3	When Encryption Goes Wrong	31
2.4	Secure Connections	32

2.4.1	Can other people read along when I check my email?	32
2.4.2	Notes	33
2.5	Secure Emails	33
2.5.1	What software can I use to encrypt my email?	34
3	Understanding Browsing	35
3.1	Basic Tips	35
3.1.1	In Brief:	35
3.1.2	Your browser talks about you behind your back	35
3.1.3	Web sites can track you as you browse	35
3.1.4	Searching online can give away information about you	36
3.1.5	More eyes than you can see	36
3.1.6	Your right to be unknown	37
3.2	Fears	37
3.2.1	Social Networking - what are the dangers?	37
3.2.2	Who can steal my identity?	38
3.2.3	Can I get in trouble for Googling weird stuff?	39
3.2.4	Who is keeping a record of my browsing and am I allowed to hide from them?	39
3.2.5	How to not reveal my Identity?	40
3.2.6	How to avoid being tracked?	40
3.3	What happens when you browse	40
3.3.1	A topography of you: footprints	41
3.4	Accounts and Security	43
3.4.1	Can malicious web sites take over my accounts?	43
3.5	Tracking	44
3.5.1	How do they track us?	44
3.5.2	How can I prevent tracking?	45
3.5.3	A word of warning	52
3.6	Anonymity	52
3.6.1	Intro	52
3.6.2	Proxy	52
3.6.3	Tor	53
3.7	VPN	54
4	Publishing And Distribution	57
4.1	Publishing Anonymously	57
4.1.1	Several Don'ts	58
4.2	Anonymous Email	59
4.2.1	Sending From Throw-away Email Accounts	59
4.2.2	Be Careful about what you say!	60
4.3	File Sharing	60
4.3.1	BitTorrent	61
4.3.2	SoulSeek	63

4.3.3	I2P	64
5	Secure Calls And Sms	65
5.1	Secure Calls	65
5.1.1	iOS - Installing Signal	65
5.1.2	Android - Installing RedPhone	65
5.2	Secure Messaging	66
5.2.1	Android	66
6	Basic Email Security	67
6.1	Start Using Thunderbird	67
6.1.1	Installing Thunderbird on Windows	67
6.1.2	Installing Thunderbird on Ubuntu	72
6.1.3	Installing Thunderbird on Ubuntu 12.04 or newer	72
6.1.4	Installing Thunderbird on Mac OS X	73
6.1.5	Starting Thunderbird for the first time	76
6.2	Setting up secure connections	76
6.2.1	Configuration requirements	77
6.2.2	Preparing a Gmail account for use with Thunderbird	77
6.2.3	Configuring Thunderbird to use SSL/TLS	78
6.2.4	Manual setup	80
6.2.5	Finishing the setup, different encryption methods	82
6.2.6	Returning to the configuration screens	83
6.3	Some Additional Security Settings	83
6.3.1	Junk mail settings	83
6.3.2	Scam detection and warning system	84
6.3.3	Anti-virus integration	85
6.3.4	Set a master password	86
6.3.5	Adaptive junk mail controls	90
7	Email Encryption	93
7.1	Introducing mail encryption (PGP)	93
7.1.1	Using a key-pair to encrypt your mail	94
7.1.2	Sending encrypted mails to other people: you need their public key	94
7.1.3	Receiving encrypted mails from other people: they need my pub- lic key	94
7.1.4	Conclusion: encryption requires public key distribution!	94
7.2	Installing PGP on Windows	94
7.2.1	Installing PGP (GPG) on Microsoft Windows	95
7.2.2	Installing with the Enigmail extension	95
7.2.3	Installation steps	96
7.3	Installing PGP on OSX	98
7.3.1	Getting started	98
7.3.2	Downloading and installing the Software	98

Contents

7.3.3	Installing up Engimail	107
7.4	Installing PGP on Ubuntu	110
7.5	Installing GPG on Android	111
7.5.1	APG	111
7.5.2	GPG enabled e-mail on Android: K-9 Mail	112
7.6	Creating your PGP keys	112
7.7	Daily PGP usage	122
7.7.1	Encrypting attachments	122
7.7.2	Entering your pass-phrase	123
7.7.3	Receiving encrypted e-mails	123
7.7.4	Sending and receiving public keys	124
7.7.5	Receiving public keys and adding them to your keyring	125
7.7.6	Using public key servers	128
7.7.7	Signing emails to an individual	134
7.7.8	Sending encrypted mails to an individual	135
7.7.9	Automating encryption to certain recipients	136
7.7.10	Verifying incoming e-mails	141
7.7.11	Revoking your GPG key-pair	142
7.7.12	What to do when you have lost your secret key, or forgot your passphrase	142
7.7.13	What to do when your secret key has been stolen, or compromised	142
7.7.14	Receiving a revocation certificate	143
7.7.15	Preparing for the worst: backup your keys	143
7.7.16	Further reading	146
7.8	Webmail and PGP	146
8	Safer Browsing	147
8.1	Why Firefox?	147
8.2	Accessing Firefox on Ubuntu	147
8.3	Installing on Mac OS X	148
8.4	Installing Firefox on Windows	153
8.4.1	Troubleshooting	157
8.5	Extending Firefox	157
8.5.1	HTTPS Everywhere	158
8.5.2	Installation	158
8.5.3	Configuration	160
8.5.4	Usage	160
8.5.5	If networks block HTTPS	163
8.5.6	Adding support for additional sites in HTTPS Everywhere	163
8.5.7	Enforcing secure HTTPS server connections	163
8.5.8	Adblock Plus	164
8.5.9	Getting started with Adblock Plus	164
8.5.10	Choosing a filter subscription	164
8.5.11	Creating personalized filters	166

8.5.12	Enabling and disabling Adblock Plus for specific elements or Web sites	166
8.5.13	Other extensions that can improve your security	166
8.6	Proxy Settings	167
8.6.1	Default Firefox proxy configuration	168
8.7	Using Tor?	170
8.7.1	Using Tor Browser Bundle	171
8.7.2	Downloading Tor Browser Bundle	171
8.7.3	Running a Relay or Bridge	171
8.8	Extending Google Chrome	172
8.8.1	Disabling Instant Search	172
8.8.2	Adblock for Chrome	172
8.8.3	HTTPS Everywhere	172
8.8.4	PrivacyFix	172
9	Passwords	173
9.1	Keeping passwords safe	173
9.1.1	Password length and complexity	173
9.1.2	Easy to remember and secure passwords	173
9.1.3	Minimizing damage	173
9.1.4	Using a password manager	174
9.1.5	Physical protection	174
9.1.6	Other caveats	174
9.2	Installing KeePass	174
9.2.1	Installing KeePassX on Ubuntu	174
9.2.2	Installing KeePass on Windows	175
9.2.3	Installing KeePass on Mac OS X	181
9.3	Encrypting Passwords with a Password Manager	189
9.3.1	Encrypting Passwords with KeePassX on Ubuntu	189
9.3.2	Encrypting Passwords with KeePass on Windows	195
9.3.3	Encrypting Passwords with Keychain on Mac OSX	201
10	Using Vpn	205
10.1	Getting, setting-up and testing a VPN account	205
10.1.1	An account from a commercial VPN provider	205
10.1.2	Setting up OpenVPN client	207
10.1.3	Caveats & Gotchas	208
10.2	VPN on Ubuntu	208
10.2.1	Preparing Network Manager for VPN networks	208
10.2.2	Configuring an OpenVPN network	214
10.2.3	Using your new VPN connection	220
10.3	VPN on MacOSX	222
10.3.1	Setup	222
10.4	VPN on Windows	235

10.4.1	Setup	235
10.5	Making Sure Your VPN Works	248
11	Disk Encryption	249
11.1	Installing TrueCrypt	249
11.1.1	Installing on Ubuntu/Debian	249
11.1.2	Installing on OSX	252
11.1.3	Installing on Windows	256
11.2	Using TrueCrypt	256
11.2.1	Creating a TrueCrypt Container	256
11.2.2	Mounting the Encrypted Volume	262
11.2.3	What does this mean?	265
11.2.4	Remember to dismount!	265
11.3	Setting up a hidden volume	265
11.4	Securely destroying data	270
11.4.1	A note on Solid State Hard Drives	271
11.4.2	Securely delete data under Windows	271
11.4.3	Securely delete data under MacOSX	273
11.4.4	Securely delete data under Ubuntu/Linux	278
11.5	About LUKS	285
11.5.1	Starting <i>Disks</i>	285
11.5.2	Encrypting a device	287
11.5.3	Using an encrypted device	291
12	Call Encryption	293
12.1	Installing CSipSimple	293
12.1.1	Introducing The OSTN Network	293
12.1.2	CSipSimple	294
13	Instant Messaging Encryption	299
13.1	Setting up Encrypted Instant Messaging	299
13.1.1	Android - Installing Gibberbot	299
13.1.2	iOS - Installing ChatSecure	299
13.1.3	Ubuntu - Installing Pidgin	299
13.1.4	OS X - Installing Adium	300
13.1.5	Windows - Installing Pidgin	300
13.1.6	All OS - crypto.cat	300
13.1.7	Chat Log Files	301
14	Secure File Sharing	303
14.1	Installing I2P on Ubuntu Lucid Lynx (and newer) and derivatives like Linux Mint & Trisquel	303
14.2	Instructions for Debian Lenny and newer	306
14.3	Starting I2P	306

14.4	Anonymous Bittorrent with I2PSnark	306
15	Appendices	309
15.1	Cryptography and Encryption	309
15.1.1	Encryption examples	310
15.1.2	A Warning!	310
15.1.3	Historical ciphers	311
15.1.4	Modern ciphers	313
15.1.5	Quantum Cryptography	314
15.1.6	Challenges & Implications	314
15.2	Glossary	315
15.2.1	aggregator	315
15.2.2	anonymity	315
15.2.3	anonymous remailer	315
15.2.4	ASP (application service provider)	316
15.2.5	backbone	316
15.2.6	badware	316
15.2.7	bandwidth	316
15.2.8	bash (Bourne-again shell)	316
15.2.9	BitTorrent	316
15.2.10	blacklist	316
15.2.11	bluebar	317
15.2.12	block	317
15.2.13	bookmark	317
15.2.14	bridge	317
15.2.15	brute-force attack	317
15.2.16	cache	317
15.2.17	sensor	317
15.2.18	sensorware	317
15.2.19	CGI (Common Gateway Interface)	318
15.2.20	chat	318
15.2.21	cipher	318
15.2.22	circumvention	318
15.2.23	Common Gateway Interface	318
15.2.24	command-line interface	318
15.2.25	cookie	318
15.2.26	country code top-level domain (ccTLD)	318
15.2.27	cryptography	319
15.2.28	DARPA (Defense Advanced Projects Research Agency)	319
15.2.29	decryption	319
15.2.30	disk encryption	319
15.2.31	domain	319
15.2.32	DNS (Domain Name System)	319
15.2.33	DNS leak	320

Contents

15.2.34	DNS server	320
15.2.35	DNS tunnel	320
15.2.36	Eavesdropping	320
15.2.37	e-mail	320
15.2.38	embedded script	321
15.2.39	encryption	321
15.2.40	exit node	321
15.2.41	file sharing	321
15.2.42	file spreading engine	321
15.2.43	filter	321
15.2.44	Firefox	321
15.2.45	forum	321
15.2.46	frame	322
15.2.47	FTP (File Transfer Protocol)	322
15.2.48	full disk encryption	322
15.2.49	gateway	322
15.2.50	GNU Privacy Guard	322
15.2.51	GPG	322
15.2.52	honeypot	322
15.2.53	hop	322
15.2.54	HTTP (Hypertext Transfer Protocol)	323
15.2.55	HTTPS (Secure HTTP)	323
15.2.56	IANA (Internet Assigned Numbers Authority)	323
15.2.57	ICANN (Internet Corporation for Assigned Names and Numbers)	323
15.2.58	Instant Messaging (IM)	323
15.2.59	Intermediary	323
15.2.60	Internet	323
15.2.61	IP (Internet Protocol) Address	323
15.2.62	IRC (Internet relay chat)	324
15.2.63	ISP (Internet Service Provider)	324
15.2.64	JavaScript	324
15.2.65	KeePass, KeePassX	324
15.2.66	keychain software	324
15.2.67	keyword filter	324
15.2.68	latency	324
15.2.69	log file	324
15.2.70	low-bandwidth filter	325
15.2.71	malware	325
15.2.72	man in the middle	325
15.2.73	middleman node	325
15.2.74	monitor	325
15.2.75	network address translation (NAT)	325
15.2.76	network operator	325
15.2.77	node	326

15.2.78	non-exit node	326
15.2.79	obfuscation	326
15.2.80	open node	326
15.2.81	OTR/Off-the-Record messaging	326
15.2.82	packet	326
15.2.83	password manager	326
15.2.84	pastebin	327
15.2.85	peer-to-peer	327
15.2.86	perfect forward secrecy	327
15.2.87	Pretty Good Privacy (PGP)	327
15.2.88	PHP	327
15.2.89	plain text	327
15.2.90	plaintext	327
15.2.91	privacy	328
15.2.92	private key	328
15.2.93	POP3	328
15.2.94	port	328
15.2.95	protocol	328
15.2.96	proxy server	328
15.2.97	Psiphon node	328
15.2.98	private node	329
15.2.99	public key	329
15.2.100	public key encryption/public-key cryptography	329
15.2.101	publicly routable IP address	329
15.2.102	regular expression	329
15.2.103	remailer	329
15.2.104	router	330
15.2.105	root name server	330
15.2.106	RSS (Real Simple Syndication)	330
15.2.107	scheme	330
15.2.108	shell	330
15.2.109	SOCKS	330
15.2.110	screenlogger	330
15.2.111	script	331
15.2.112	smartphone	331
15.2.113	spam	331
15.2.114	SSH (Secure Shell)	331
15.2.115	SSL (Secure Sockets Layer)	331
15.2.116	steganography	331
15.2.117	subdomain	332
15.2.118	threat analysis	332
15.2.119	Top-Level Domain (TLD)	332
15.2.120	TLS (Transport Layer Security)	332
15.2.121	TCP/IP (Transmission Control Protocol over Internet Protocol)	332

Contents

15.2.122 Tor bridge	332
15.2.123 traffic analysis	332
15.2.124 tunnel	333
15.2.125 UDP (User Datagram Packet)	333
15.2.126 URL (Uniform Resource Locator)	333
15.2.127 Usenet	333
15.2.128 VoIP (Voice over Internet Protocol)	333
15.2.129 VPN (virtual private network)	333
15.2.130 whitelist	334
15.2.131 World Wide Web (WWW)	334
15.2.132 Webmail	334
15.2.133 Web proxy	334
15.2.134 WHOIS	334
15.3 The necessity of Open Source	335

1 Introducing Cryptoparty

1.1 About This Book

The CryptoParty Handbook was born from a suggestion by Marta Peirano (<http://petitemedia.es>) and Adam Hyde (<http://booksprints.net>) after the first Berlin CryptoParty, held on the 29th of August, 2012. Julian Oliver (<http://julianoliver.com>) and Danja Vasiliev (<http://k0a1a.net>), co-organisers of the Berlin CryptoParty along with Marta were very enthusiastic about the idea, seeing a need for a practical working book with a low entry-barrier to use in subsequent parties. Asher Wolf, originator of the CryptoParty movement, was then invited to run along and the project was born.

This book was written in the first 3 days of October 2012 at Studio Weise7, Berlin, surrounded by fine food and a small ocean of coffee. Approximately 20 people were involved in its creation, some more than others, some local and some far.

The writing methodology used, BookSprint (<http://booksprints.net>), is all about minimising any obstruction between expertise and the published page. Face-to-face discussion and dynamic task-assignment were a huge part of getting the job done, like any good CryptoParty!

The open source, web-based (HTML5 and CSS) writing platform BookType (<http://booktype.pro>) was chosen for the editing task, helping such a tentacular feat of parallel development to happen with relative ease. Asher also opened a couple of TitanPad pages to crowd-source the Manifesto and HowTo CryptoParty chapters.

Combined, this became the official CryptoParty Handbook by midnight October the 3rd, GMT+1.

The Book Sprint was 3 days in length and the full list of onsite participants included:

- Adam Hyde (facilitator)
- Marta Peirano
- Julian Oliver
- Danja Vasiliev
- Asher Wolf (<http://cryptoparty.org>)
- Jan Gerber
- Malte Dik
- Brian Newbold
- Brendan Howell (<http://wintermute.org>)
- AT
- Carola Hesse

1 Introducing Cryptoparty

- Chris Pinchen (<http://chokepointproject.net>).
- Cover art by Emile Denichaud (<http://about.me/denichaud>)

This version of the handbook has since moved to github to collaboratively edit it. Find it at <https://github.com/cryptoparty/handbook>. If you see areas that need improvement or simply come across a typo, create a github account and start editing, commenting or creating issues. For help using git and github, see <https://help.github.com/>.

CryptoParty HandBook Credits

Facilitated by:

- Adam Hyde

Core Team:

- Marta Peirano
- Asher Wolf
- Julian Oliver
- Danja Vasiliev
- Malte Dik
- Jan Gerber
- Brian Newbold
- Brendan Howell

Assisted by:

- Teresa Dillon
- AT
- Carola Hesse
- Chris Pinchen
- ‘LiamO’
- ‘13lackEyedAngels’
- ‘Story89’
- Travis Tueffel

Github migration, packaging and maintenance by:

- Yuval Adam
- Samuel Carlisle
- Daniel Kinsman
- pettter
- Jens Kubieziel
- Uwe Lippmann
- Kai Engert

Cover Image by Emile Denichaud.

Other material included:

- <https://www.flossmanuals.net/bypassing-censorship>

The manuals used in the second half of this book borrow from 2 books sprinted by FLOSS Manuals:

- “How to Bypass Internet Censorship” 2008 & 2010 Adam Hyde (Facilitator), Alice Miller, Edward Cherlin, Freerk Ohling, Janet Swisher, Niels Elgaard Larsen, Sam Tennyson, Seth Schoen, Tomas Krag, Tom Boyle, Nart Villeneuve, Ronald Deibert, Zorrino Zorrinno, Austin Martin, Ben Weissmann, Ariel Viera, Niels Elgaard Larsen, Steven Murdoch, Ross Anderson, helen varley jamieson, Roberto Rastapopoulos, Karen Reilly, Erinn Clark, Samuel L. Tennyson, A Ravi
- “Basic Internet Security” 2011 Adam Hyde (Facilitator), Jan Gerber, Dan Hassan, Erik Stein, Sacha van Geffen, Mart van Santen, Lonneke van der Velden, Emile den Tex and Douwe Schmidt

All content in the CryptoParty Handbook is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0).

All chapters Â the contributors unless otherwise noted below.

1.2 A CryptoParty Manifesto

“Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth.” - Oscar Wilde

In 1996, John Perry Barlow, co-founder of the Electronic Frontier Foundation (EFF), wrote ‘A Declaration of the Independence of Cyberspace’. It includes the following passage:

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

1 *Introducing Cryptoparty*

Sixteen years later, and the Internet has changed the way we live our lives. It has given us the combined knowledge of humankind at our fingertips. We can form new relationships and share our thoughts and lives with friends worldwide. We can organise, communicate and collaborate in ways never thought possible. This is the world we want to hand down to our children, a world with a free Internet.

Unfortunately, not all of John Perry Barlow's vision has come to pass. Without access to online anonymity, we can not be free from privilege or prejudice. Without privacy, free expression is not possible.

The problems we face in the 21st Century require all of humanity to work together. The issues we face are serious: climate change, energy crises, state censorship, mass surveillance and on-going wars. We must be free to communicate and associate without fear. We need to support free and open source projects which aim to increase the commons' knowledge of technologies that we depend on <http://opensourceecology.org/wiki> Contribute!

To realise our right to privacy and anonymity online, we need peer-reviewed, crowd-sourced solutions. CryptoParties provide the opportunity to meet up and learn how to use these solutions to give us all the means with which to assert our right to privacy and anonymity online.

1. We are all users, we fight for the user and we strive to empower the user. We assert user requests are why computers exist. We trust in the collective wisdom of human beings, not software vendors, corporations or governments. We refuse the shackles of digital gulags, lorded over by vassal interests of governments and corporations. We are the CypherPunk Revolutionaries.
2. The right to personal anonymity, pseudonymity and privacy is a basic human right. These rights include life, liberty, dignity, security, right to a family, and the right to live without fear or intimidation. No government, organisation or individual should prevent people from accessing the technology which underscores these basic human rights.
3. Privacy is the right of the individual. Transparency is a requirement of governments and corporations who act in the name of the people.
4. The individual alone owns the right to their identity. Only the individual may choose what they share. Coercive attempts to gain access to personal information without explicit consent is a breach of human rights.
5. All people are entitled to cryptography and the human rights crypto tools afford, regardless of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, political, jurisdictional or international status of the country or territory in which a person resides.
6. Just as governments should exist only to serve their citizens - so too, cryptography should belong to the people. Technology should not be locked away from the people.

7. Surveillance cannot be separated from censorship, and the slavery it entails. No machine shall be held in servitude to surveillance and censorship. Crypto is a key to our collective freedom.
8. Code is speech: code is human created language. To ban, censor or lock cryptography away from the people is to deprive human beings from a human right, the freedom of speech.
9. Those who would seek to stop the spread of cryptography are akin to the 15th century clergy seeking to ban the printing press, afraid their monopoly on knowledge will be undermined.

1.3 How To CryptoParty

- Throw a party. All you need is a time, a date and a location. Add it to the wiki: <https://cryptoparty.org>.
- Make sure you have Internet connectivity and enough power sources for all devices. If you do not have a place to hold a CryptoParty, find a pub or park where you can meet and squeeze the public bandwidth. That will really hone your skills!
- Bring USB sticks and printed handouts for those who need them, and set up old computers for people to fiddle with and try out new skills.
- Talk about Linux to everyone you meet at your CryptoParty. If you are new to CryptoParties - ask someone “what is Linux?” ASAP.
- Make entry free for all if possible - CryptoParties are not-for-profit, not commercially aligned and especially important for those without other resources.
- Teach basic cryptographic tools to the masses. Crowd-source the best crypto. We suggest PGP, OTR, and Tor as the first tools to install.
- Invite experts and non-experts from all fields. Everyone is an expert on something.
- If you want CryptoParty to do something, start doing it. Organise organically and chaotically. Have no clear leadership. Urge people to take on a sudo leadership role - take a tutorial, fix the wifi, update the wiki, or organise the next CryptoParty. If someone claims others are doing it wrong - invite them to nominate themselves to do it better.
- Ask for feedback. Assimilate critics - ask them for their help in creating a better CryptoParty. Do not be scared to troll the trolls back or boot them from your space. Share feedback on the wiki. Iterate.
- A successful CryptoParty can have as many or as few as two people. Size doesn't count, it's what you do with it that matters. The criterion for success should be that everyone had fun, learned something and wants to come to the next party.

1 *Introducing Cryptoparty*

- Think of the CryptoParty movement as a huge Twitter hive ready to swarm at any moment. Tweet a lot, and make your tweets meaningful. ReTweet other CryptoPartiers frequently.
- Make sure the way crypto is taught at your party could be understood by a 10 year old. Then have the 10 year old teach it to an 80 year old. Breach the digital divide with random acts of awesomeness such as unfettered use of images of kittens in all CryptoParty literature. Red underpants on heads is only mandatory if you wish to bid in our spectrum auction.
- Consider hosting private, off-the-radar CryptoParties for activists, journalists and in individuals working in dangerous locations.
- Don't scare non-technical people. Don't teach command lines before people know where the on-off buttons are located on their laptops. Everyone learns at their own pace - make sure there is support for those in need of help.
- Doing excellent stuff at CryptoParty does not require permission or an official consensus decision. If you're uncertain about the excellence of something you want to do, you should ask someone else what they think.
- Consider the need for a bouncer, particularly if your CryptoParty expects over 50 people. Dress the bouncer up as a Sumo wrestler. Do not be afraid to bounce people who breach CryptoParty's anti-harassment policy.
- CryptoParty is dedicated to providing a harassment-free sharing experience for everyone, regardless of gender, sexual orientation, disability, physical appearance, body size, heritage, or religion. Behaving like an asshole may mean you are permanently uninvited to CryptoParties events. Harassment includes:
 - hurtful or offensive comments
 - deliberate intimidation
 - direct or indirect threats
 - stalking
 - following
 - inappropriate physical contact
 - unwelcome sexual attention.
- Encourage a culture of sharing. Encourage advanced users to help not-so advanced ones. Delegate.
- Use online meeting platforms like mumble, or even chatrooms (e.g. #cryptoparty room on <http://occupytalk.org/>) when physical meetups are not possible or impractical.
- Copy from other cryptoparties. Remix, Reuse and Share. Create a basket of old devices people are willing to donate to more needy CryptoPartiers.

1.3 How To CryptoParty

- Get the word out! Print posters and/or flyers and distribute them in your neighbourhood, post online versions to social networks and mail them to friends, for them to distribute the info even further.
- Don't sell out to sponsors for pizza and beer money. Ask people to try and bring food and drink to share. Host CryptoPicnics as often as possible. Make friends with librarians. They wield power over keys to local, public meeting rooms that may be free of charge to utilize.
- Invite all the people. Bring people together who have a wide range of skills and interests - musicians, political pundits, activists, hackers, programmers, journalists, artists and philosophers. Spread the love.
- Invite the graphic designers and illustrators you know to contribute new ways to help people understand crypto.
- Invite everyone to share their knowledge and their skills. Individuals with little or no coding, programming, hacking or crypto skills can change cultures by promoting the idea that privacy is a fundamental right.
- Share music, beers, & chips. Bond together over eclectic music, cheeseballs, installing GPG, TrueCrypt, OTR and Tor, as well as watching movies together. We recommend Hackers, The Matrix, Bladerunner, Tron, Wargames, Sneakers, and The Net.
- Do not work too hard. Take breaks. Eat popcorn together. Create slang, phrases, memes.
- When people at CryptoParties ask for advice on "hacking the Gibson" refer them to episodes of 'My Little Pony'.
- Create fliers and advertise using slogans like: "CryptoParties: If there is hope, it lies in the proles" and "CryptoParty like it's 1984." CryptoParty all the things to avoid oppression and depression.
- Seed CryptoParties in your local communities - at nursing homes, scout groups, music festivals, universities, schools. Take CryptoParty to isolated and remote communities. Make friends in far away places and travel whenever possible. Ask people in rural farming communities if they'd like to CryptoParty.
- Share shimmering opportunities of crowd-sourced privacy: swap cheap, pre-paid SIMs, handsets and travel cards.
- Create logos in bright pink and purple, with hearts all over them. Promote CryptoParties to rebellious 13 year old girls. Declare success if rebellious 13 year old girls demand to attend your parties.
- Become friends with journalists. Invite them to your parties. Teach them crypto. Do not scare them by discussing Assassination Markets.

1 Introducing Cryptoparty

- Strew CryptoParty sigils across your city in 3am post-party raids. Make lots of stickers, paste them everywhere.
- Experiment, constantly. Do not be afraid to make mistakes. Encourage people to tinker. Assume all mistakes are meant to be made. Most people under intel agency scrutiny have electronic devices already compromised before they walk in the door. Teach people to install tools from scratch, so they can do it on a new machine, away from prying eyes.
- Assume intel agencies send representatives to CryptoParties. Acknowledge their presence at the start of your meeting, ask them to share their crypto skills. Joke about paranoia as often as possible without instilling panic. Wear tinfoil hats.
- Be excellent to each other and CryptoParty on.

1.4 Party like it's december 31st 1983

1.4.1 What is CryptoParty?

CryptoParty is a decentralized, global initiative to introduce basic tools for protecting privacy, anonymity and overall security on the Internet to the general public.

The idea was conceived in the wake of the Australian Cybercrime Legislation Amendment Bill 2011 and the reasoning is that laws like this are without substance when everybody encrypts their communication.

CryptoParties are neither commercially nor politically aligned, and free and open to attend for everyone as long as they live the following *guiding principles*:

Be excellent to each other

CryptoParties are environments where people feel welcome and safe to learn and teach no matter their background or level of expertise. All questions are relevant, all explanation shall be targeted at the person with least pre-knowledge.

This also means that any form of harassment or other behaviour that makes people uncomfortable has no place at CryptoParties. In our experience situations like these (as seldom as they occur) stem rather from social ineptitude than malice and can thus be resolved by making people aware of their behaviour and its effect on others, but in last consequence it is on the organizers of the CryptoParty to ask people to leave if they don't adhere to this very simple rule. Be excellent to each other. Awareness is key in this regard.

Do things

CryptoParties happen because people make them happen. The most amazing and unforeseen learning experiences happen because people make them happen. If you are uncertain if what you have in mind is on topic or if other people are interested as well:

Propose it anyway and see what other people have to say. If you are too shy to propose to the whole room: Ask the person standing next to you first.

On a more global scale, there is a mailing list `global@cryptoparty.is` which is open for questions and discussion of all kind, as well as country and city-specific mailing lists and other resources which can be found on <https://cryptoparty.in> .

For a guide on how to organize CryptoParties please be referred to the chapter of the same name.

1.5 Preface

This book is a collective and ongoing effort in that it is based on the two FLOSS Manuals *How to Bypass Internet Censorship* and *Basic Internet Security* and collaboratively edited on Github although other venues of collaborative editing are investigated.

Its goal is to give a comprehensive resource to people who would like to attend or organize a CryptoParty but lack the local expertise or just confidence in doing so. All chapters are designed to be self-contained.

All content in the *CryptoParty Handbook* is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0). The authors are listed in *Appendix A: Contributions*.

1.6 Why Privacy Matters

Privacy is a fundamental human right. It is recognized in many countries to be as central to individual human dignity and social values as Freedom of Association and Freedom of Speech. Simply put, privacy is the border where we draw a line between how far a society can intrude into our personal lives.

Countries differ in how they define privacy. In the UK for example, privacy laws can be traced back to the 1300s when the English monarchy created laws protecting people from eavesdroppers and peeping toms. These regulations referred to the intrusion of a person's comfort and not even the King of England could enter into a poor persons house without their permission. From this perspective, privacy is defined in terms of personal space and private property. In 1880 American lawyers, Samuel Warren and Louis Brandeis described privacy as the 'right to be left alone'. In this case, privacy is synonymous with notions of solitude and the right for a private life. In 1948, the Universal Declaration of Human Rights specifically protected territorial and communications privacy which by that became part of constitutions worldwide. The European Commission on Human Rights and the European Court of Human Rights also noted in 1978 that privacy encompasses the right to establish relationships with others and develop emotional well-being.

Today, a further facet of privacy increasingly perceived is the personal data we provide to organizations, online as well as offline. How our personal data is used and accessed drives the debate about the laws that govern our behavior and society. This in turn has knock-on effects on the public services we access and how businesses interact with us. It

1 *Introducing Cryptoparty*

even has effects on how we define ourselves. If privacy is about the borders which govern who we give permission to watch us and track aspects of our lives, then the amount and type of personal information gathered, disseminated and processed is paramount to our basic civil liberties.

An often heard argument, when questions of privacy and anonymity come up, goes along the lines of, “I only do boring stuff. Nobody will be interested in it anyway” or, “I have nothing to hide”. Both of these statements are easily defeated.

Firstly, a lot of companies are very interested in what boring things you do precisely so they have opportunity to offer “excellent” products fitting interests. In this way their advertising becomes much more efficient - they are able to tailor specifically to assumed needs and desires. Secondly you do have lots to hide. Maybe you do not express it in explicitly stated messages to friends and colleagues, but your browsing - if not protected by the techniques laid out in this book - will tell a lot about things you might rather keep secret: the ex-partner you search for using Google, illnesses you research or movies you watch are just few examples.

Another consideration is that just because you might not have something to hide at this moment, you may very well in future. Putting together all the tools and skills to protect yourself from surveillance takes practice, trust and a bit of effort. These are things you might not be able to achieve and configure right when you need them most and need not take the form of a spy movie. An obsessed, persistent stalker, for example, is enough to heavily disrupt your life. The more you follow the suggestions given in this book, the less impact attacks like this will have on you. Companies may also stalk you too, finding more and more ways to reach into your daily life as the reach of computer networking itself deepens.

Finally, a lack of anonymity and privacy does not just affect you, but all the people around you. If a third party, like your Internet Service Provider, reads your email, it is also violating the privacy of all the people in your address book. This problem starts to look even more dramatic when you look at the issues of social networking websites like Facebook. It is increasingly common to see photos uploaded and tagged without the knowledge or permission of the people affected.

While we encourage you to be active politically to maintain your right to privacy, we wrote this book in order to empower people who feel that maintaining privacy on the Internet is also a personal responsibility. We hope these chapters will help you reach a point where you can feel that you have some control over how much other people know about you. Each of us has the right to a private life, a right to explore, browse and communicate with others as one wishes, without living in fear of prying eyes.

2 Understanding Email

2.1 Basic Tips

Just as with other forms of communication on the web, some basic precautions always ought to be taken to ensure you have the best chance at protecting your privacy.

2.1.1 In brief:

- Passwords shouldn't relate to personal details and should contain a mix of a reasonable amount of letters and other characters.
- To change passwords regularly is important as they might have been stolen, cracked or exposed to others in the meantime.
- Always be sure your connection is secure when reading email on a wireless network, especially in Internet cafes.
- Temporary files (the 'cache') on the computer that you use to check your email can present some risks. Clear them often.
- Create and maintain separate email accounts for different tasks and interests.
- Encrypt any message you wouldn't feel comfortable sending on a post card.
- Be aware of the risks of having your email hosted by a company or organization.

2.1.2 Passwords

Passwords are a primary point of vulnerability in email communication. Even a secure password can be read in transit unless the connection is secure (see TLS/SSL in the glossary). In addition, just because a password is long doesn't mean it cannot be guessed by using knowledge of you and your life to determine likely words and numbers.

The general rule for creating passwords is that it should be long (8 characters might be cracked within few hours) and have a mix of letters and other characters (numbers and symbols, which means you could just choose a sentence). Combining your birthday with that of a family name is however a great example of how not to do it. This kind of information is easy to find using public resources. A popular trick is to base it on a favourite phrase and then, just to throw people off, sprinkle it with a few numbers. Best of all is to use a password generator, either on your local system or online.

Often such passwords are difficult to remember and a second point of vulnerability is opened up – physical discovery. Since there is no better means of storing a password than in your own brain, services like OnlinePasswordGenerator (<http://www.onlinepasswordgenerator.com/>) offer a great compromise by randomly generating passwords that vaguely resemble words and present you with a list to choose from.

2 Understanding Email

If you do choose to store your password outside your head, you have the choice to either write it down or use keychain software. This can be a risky decision, especially if the email account and password are on the same device like your phone or computer.

Keychain software, like KeePass, consolidates various passwords and passphrases in one place and makes them accessible through a master password or passphrase. This puts a lot of pressure on the master password. If you do decide to use a keychain software, remember to choose a secure password.

Finally, you should use a different password for different accounts. In that way, if one of them gets hijacked, your other accounts remain safe. Never use the same password for your work and private email accounts. See section **Passwords** to learn more about how to secure yourself.

2.1.3 Reading Email in Public Places

One of the great conveniences of wireless networking and ‘cloud computing’ is the ability to work anywhere. You may often want to check your email in an Internet cafe, on open networks or public location. Spies, criminals and mischievous types are known to visit these locations in order to take advantage of the rich opportunities offered for ID theft, email snooping and hijacking bank accounts.

Here we find ourselves within an often underestimated risk of someone listening in on your communications using *network packet sniffing*. It matters little if the network itself is open or password secured. If someone joins the same encrypted network, s/he can easily capture and read all *unsecured* (see chapter **Secure Connection** for *TLS* and *VPN* solutions) traffic of all of other users within the same network. A wireless key can be acquired for the cost of a cup of coffee and gives those that know how to capture and read network packets the chance to read your password while you check your email if the connection to that service is not secured.

Here a simple general rule always applies: if the cafe offers a network cable connection, use it! Finally, just as at a bank machine, make sure no one watches over your shoulder when you type in the password.

2.1.4 Cache Cunning

Here again convenience quickly paves the road to bad places. Due to the general annoyance of having to type in your password over and over again, you ask the browser or local mail client to store it for you. This is not bad in itself, but when a notebook or phone gets stolen, it enables the thief to access the owner’s email account(s). The best practice is to clear this cache every time you close your browser. All popular browsers have an option to clear this cache on exit.

One basic precaution can justify you holding onto your convenient cache: disk encryption. If your notebook is stolen and the thief reboots the machine, they’ll be met with an encrypted disk. It is also wise to have a screen lock installed on your computer or phone. If the machine is taken from you while still running your existing browsing session, it cannot be accessed.

2.1.5 Securing your communication

Whenever you write and send email in a browser or use an email program (Outlook Express, Mozilla Thunderbird, Mail.app or Mutt), you should always ensure to use encryption for the entire session. This is easily done due to the popular use of *TLS/SSL* (*Secure Socket Layer*) connections by email servers (See glossary **TLS/SSL**).

If using a browser to check your email, check to see if the mail server supports SSL sessions by looking for `https://` at the beginning of the URL. If not, be sure to turn it on in your email account settings, such as Gmail or Hotmail. This ensures that not just the login part of your email session is encrypted but also the writing and sending of emails. Furthermore check the certificate details and take *TLS pinning* into account and endorse browser extensions that warn about changing or disfunctional certificates (e.g. *Certificate Patrol*) and make use of TLS secured version of the website the default (e.g. *HTTPS everywhere*).

The email service provider you select, should provide you with the mail server details. These details can often be found in the settings option. If your email service provider does not offer you a cryptographic protocol (TLS/SSL) to encrypt your data on the network, then it is advised to stop using it. Even if your emails are not important, you might find yourself ‘locked out’ of your account one day with a changed password!

When using an email program to check your email, be sure that you are using TLS/SSL in the program options. For instance in Mozilla Thunderbird the option for securing your outgoing email is found in **Tools -> Account Settings -> Outgoing Server (SMTP)** and for incoming email in **Tools -> Account Settings -> Server Settings**. This ensures that the downloading and sending of email is encrypted, making it very difficult for someone on your network, or on any of the networks between you and the server, to read or log your email. Encrypting the email itself

Even if the line itself is encrypted using a system such as SSL, the email service provider still has full access to the email because they own and have full access to the storage device where you host your email. If you want to use a web service and be sure that your provider cannot read your messages, then you’ll need to use something like *GPG* (Appendix for **GnuPG**) with which you can encrypt the email. The header of the email however will still contain the IP (Internet address) that the email was sent from alongside other compromising details. Worth mentioning here is that the use of *GPG* in webmail is not as comfortable as with a locally installed mail client, such as *Thunderbird* or *Outlook Express*.

2.1.6 DNSSEC & DANE

certificate information can be stored in DNS records and therefore be regarded more reliable. Check the availability of *DNSSEC* and especially regarding email services *DANE* with your service providers. Here again browser extensions (e.g. *DNSSEC/TLSA Validator*) can assist to control the availability of these security measures.

2.1.7 Account Separation

Due to the convenience of services like Gmail, it is increasingly typical for people to have only one email account. This considerably centralises the potential damage done by a compromised account. More so, there is nothing to stop a disgruntled Google employee from deleting or stealing your email, let alone Google itself getting hacked. Hacks happen.

A practical strategy is to keep your personal email, well, personal. If you have a work email then create a new account if your employers haven't already done it for you. The same should go for any clubs or organisations you belong to, each with a unique password. Not only does this improve security, by reducing the risk of whole identity theft, but greatly reduces the likelihood of spam dominating your daily email.

2.1.8 A note about hosted email

Those that provide you with the service to host, send, download and read email are not encumbered by the use of TLS/SSL. As hosts, they can read and log your email in plain text. They can comply with requests by local law enforcement agencies who wish to access email. They may also study your email for patterns, keywords or signs of sentiment for or against brands, ideologies or political groups. It is important to read the EULA (End-user license agreement) of your email service provider and do some background research on their affiliations and interests before choosing what kind of email content they have access to. These concerns also apply to the hosts of your messages' recipients.

2.2 Types of Email

The use of email almost always comes in two forms:

- Email read, written and sent in the *browser* (webmail via HTTP) and stored on a providers server, and/or
- Email read, written, sent and stored using an *email program*, like e.g. Mozilla Thunderbird, Mail.App or Outlook Express by utilizing protocols like *SMTP*, *POP* and *IMAP*.

These two models might be mixed in practice, especially by using *IMAP*. Whilst the webmail solution is more convenient to use and easier to maintain for end users on different computers compared to the more powerful solution (less limits on storage, better search options and direct control over data) based on native applications.

2.2.1 Remotely hosted email ('webmail'), resourced using a web browser

Email sent using the *browser*, sometimes referred to as *webmail*, typically assumes an account with a remote email host like Google (Gmail), Microsoft (Hotmail) or Yahoo (Yahoo Mail). The business opportunities opened up by hosting other people's email

are many: contact with other services offered by the company, brand exposure and most importantly, mining your plain text email for patterns that can be used to evaluate your interests – something of great value to the advertising industry (alongside certain Governments). For the reason of datamining those companies have *no interest* in encouraging their users to use *encryption to secure privacy* and/or *signatures for integrity/authenticity* of communication.

2.2.2 Remotely hosted email, resourced using an email program or using a web browser

Email sent using an email program like Outlook, Thunderbird, Mail.App aso. can also be used with a webmail service like Gmail or your company's email service. In either case, email may still be downloaded onto your computer but is retained on the email server (e.g. Gmail). Done this way, accessing email doesn't require the browser at all, but you are still using Gmail, Hotmail as a service. The difference between storing email on your computer with an email program and having it stored remotely on an email server (like Hotmail, Gmail or your University's service) on the Internet can appear confusing at first.

Finally, email can also be sent to an email server but not stored there at all, merely volleyed onto its' destination as soon as the email reaches the email forwarding server. Google and Microsoft do not allow for this sort of setup. Rather this is typically something your university or company will provide for you. Bear in mind that this comes with the risk of the email administrator on that system still secretly copying the email as it reaches and leaves the server.

Generally, using webmail alongside downloading it using an email program is the best approach. This approach adds redundancy (local backups) alongside the option to delete all email from the remote server once downloaded. The latter option is ideal for content sensitive information where the possibility of account hijacking is high but risks total loss of email should the local machine go missing, without backups. Secondly, when using an email program, we have the option of using Email Encryption such as the popular OpenPGP implementation **GPG**, something not easily set up and used with browser-only webmail services. In any case, disk encryption on the local machine is highly advisable (Appendix **Disk Encryption**).

2.2.3 Context considerations

You may be a server administrator yourself and run your own email service. Or your email could be stored on your company or bosses' server. Finally you may be using a service provided by a corporation, like Google (Gmail) or Microsoft (Hotmail). Each comes with its own interesting mix of considerations that relates precisely to the basic fact that unless the email itself is encrypted, the administrator of the email server can still secretly copy the email the moment it reaches the server. It doesn't matter that you may be using *TLS/SSL* (Appendix **SSL**) to login and check your email as this only protects the connection between your local machine and the server.

2 Understanding Email

As always, if you know the risks and feel concerned it is wise to listen to them - don't send sensitive email using a service you don't trust. Employer/Organisation

Your employer or an organisation that you are involved with is in a very good position to take advantage of your trust and read the emails of your business email account that is stored on their email server, perhaps in an effort to learn about you, your motivations, agendas and interests. Such cases of employer->employee spying are so typical they do not bear mention. Your only measure against it is to use an email encryption solution like GPG (Appendix GPG).

2.2.4 Email & Metadata

The actual content information of mails might be preserved utilizing *OpenPGP* or *S/MIME* but the metadata - the association of persons, addresses, time and used software/services - is stored by several stakeholders. Government services might store such data as well as any company involved in transmitting them. In regards of header information Email remains a risk for communication as long as the accounts used can be connected to individuals or groups.

2.2.5 Self-administered email server

Generally speaking this is the ideal hosting configuration, but requires a higher level of technical skill. Here, in general, the risks to privacy are not only in protecting your own email against attempts at exploit (poor passwords, no SSL) but in that you have a responsibility, and perhaps a temptation, to read the emails of those you provide a service for.

2.2.6 'Free' email services

As mentioned above the risks of storing and sending your email using a service provided by a corporation are rather high if respect of your civil right to privacy is valued. The companies hosting your love letters, random expressions and diaries are always at risk of yielding to pressures from political, economic and law enforcement interests of the country to which they are legally subject. A Malaysian Gmail user, for instance, risks exposing her interests and intents to a government she did not elect, not to mention business partners of Google interested in expanding their market reach.

2.2.7 Non-profit

Several non-profit web hosts offer free email accounts to organisations that are themselves non-profit or philanthropic. Some of them even offer wikis, mailing lists, chats and social networks. A consideration for organisations working in a political field may be differences of interests between the state in which the email is hosted and the political interests of the organisation using that service. Such risks would ideally be reflected in the End User License Agreement.

2.2.8 Notes on email forwarding

Email forwarding services provide the great convenience of ‘linking’ one email account to another as the user sees fit. This of course is most commonly used when an account holder is on holiday and would like email forwarded from their work account to another used during travel or otherwise inaccessible outside the workplace. The risk with any external email forwarding service is the same as with remotely hosted emails through Gmail for instance: it can be copied and stored. Here email encryption using a system such as *GPG* (Appendix **GPG**) will ensure that if it is copied at least it cannot be read.

2.3 Fears

Who can read the email messages that I have already sent or received?

Who can read the emails I send when they travel across the Internet?

Can the people I send emails to share them with anybody?

Emails that are sent “in the clear” without any encryption (which means the vast majority of email sent and received today) can be read, logged, and indexed by any server or router along the path the message travels from sender to receiver. Assuming you use an encrypted connection (see glossary for TLS/SSL) between your devices and your email service provider (which everybody should), this means in practice that the following people can still read any given message:

1. You
2. Your email service provider
3. The operators and owners of any intermediate network connections (often ambiguous multinational conglomerates or even sovereign states)
4. The recipient’s email service provider
5. The intended recipient

Many webmail providers (like Gmail) automatically inspect all of the messages sent and received by their users for the purpose of showing targeted advertisements. While this may be a reasonable compromise for some users most of the time (free email!), it is disturbing for many that even their most private communications are inspected and indexed as part of a hidden and potentially very insightful profile maintained by a powerful corporate giant with a profit motive.

Additionally, somebody who can legally pressure the groups above could request or demand:

1. logged meta-data about email (lists of messages sent or received by any user, subject lines, recipients), in some jurisdictions even without a warrant.
2. messages sent and received by a specific user or group, with a warrant or court order in some jurisdictions.
3. a dedicated connection to siphon off *all* messages and traffic, to be analyzed and indexed off site.

2 Understanding Email

In cases where a user has a business or service relationship with their email provider, most governments will defend the privacy rights of the user against unauthorized and unwarranted reading or sharing of messages, though often it is the government itself seeking information, and frequently users agree to waive some of these rights as part of their service agreement. However, when the email provider is the user's employer or academic institution, privacy rights frequently do not apply. Depending on jurisdiction, businesses generally have the legal right to read all of the messages sent and received by their employees, even personal messages sent after hours or on vacation.

Historically, it was possible to “get away” with using clear text email because the cost and effort to store and index the growing volume of messages was too high: it was hard enough just to get messages delivered reliably. This is why many email systems do not contain mechanisms to preserve the privacy of their contents. Now the cost of monitoring has dropped much faster than the growth of internet traffic and large-scale monitoring and indexing of all messages (either on the sender or receiving side) is reasonable to expect even for the most innocuous messages and users. [CITE:corporate email archiving/spying, blue coat, Syrian monitoring, USA Utah data center, USA intercept scandals]

For more about legal protections of email messages “at rest” (technical term for messages stored on a server after having been delivered), especially regarding government access to your email messages, see:

- <https://ssd.eff.org/3rdparties/govt/stronger-protection> (USA)
- http://en.wikipedia.org/wiki/Data_Protection_Directive (EU)

Just like there are certain photos, letters, and credentials that you would not post “in the clear” on the Internet because you would not want that information to get indexed accidentally and show up in search results, you should never send email messages in the clear that you would not want an employer or disgruntled airport security officer to have easy access to.

2.3.1 Random abuse and theft by malicious hackers

What if somebody gets complete control of my email account?

I logged in from an insecure location... how do I know now if my account has been hacked?

I've done nothing wrong... what do I have to hide?

Why would anybody care about me?

Unfortunately, there are many practical, social, and economic incentives for malicious hackers to break into the accounts of random Internet individuals. The most obvious incentive is identity and financial theft, when the attacker may be trying to get access to credit card numbers, shopping site credentials, or banking information to steal money. A hacker has no way to know ahead of time which users might be better targets than others, so they just try to break into all accounts, even if the user doesn't have anything to take or is careful not to expose his information.

Less obvious are attacks to gain access to valid and trusted user accounts to collect contact email addresses from and then distribute mass spam, or to gain access to particular services tied to an email account, or to use as a “stepping stone” in sophisticated social engineering attacks. For example, once in control of your account a hacker could rapidly send emails to your associates or co-workers requesting emergency access to more secured computer systems.

A final unexpected problem affecting even low-profile email users, is the mass hijacking of accounts on large service providers, when hackers gain access to the hosting infrastructure itself and extract passwords and private information in large chunks, then sell or publish lists of login information in online markets.

2.3.2 Targeted abuse, harassment, and spying

Something I wrote infuriated a person in power... how do I protect myself?

If you find yourself the individual target of attention from powerful organizations, governments, or determined individuals, then the same techniques and principles will apply to keeping your email safe and private, but additional care must be taken to protect against hackers who might use sophisticated techniques to undermine your devices and accounts. If a hacker gains control of any of your computing devices or gets access to any of your email accounts, they will likely gain immediate access both to all of your correspondence, and to any external services linked to your email account.

Efforts to protect against such attacks can quickly escalate into a battle of wills and resources, but a few basic guidelines can go a long way. Use specific devices for specific communication tasks, and use them only for those tasks. Log out and shutdown your devices immediately when you are done using them. It is best to use open software encryption tools, web browsers, and operating systems as they can be publicly reviewed for security problems and keep up to date with security fixes.

Be wary of opening PDF files using Adobe Reader or other proprietary PDF readers. Closed source PDF readers have been known to be used to execute malign code embedded in the PDF body. If you receive a .pdf as an attachment you should first consider if you know the supposed sender and if you are expecting a document from them. Secondly, you can use PDF readers which have been tested for known vulnerabilities and do not execute code via java script.

Linux: Evince, Sumatra PDF

OS X: Preview

Windows: Evince

Use short-term anonymous throw away accounts with randomly generated passwords whenever possible.

2.3.3 When Encryption Goes Wrong

What happens if I lose my “keys”? Do I lose my email?

Rigorous GPG encryption of email is not without its own problems.

2 Understanding Email

If you store your email encrypted and lose all copies of your private key, you will be absolutely unable to read the old stored emails, and if you do not have a copy of your revocation certificate for the private key it could be difficult to prove that any new key you generate is truly the valid one, at least until the original private key expires.

If you sign a message with your private key, you will have great difficulty convincing anybody that you did not sign if the recipient of the message ever reveals the message and signature publicly. The term for this is *non-repudiation*: any message you send signed is excellent evidence in court. Relatedly, if your private key is ever compromised, it could be used to read all encrypted messages ever sent to you using your public key: the messages may be safe when they are in transit and just when they are received, but any copies are a liability and a gamble that the private key will never be revealed. In particular, even if you destroy every message just after reading it, anybody who snooped the message on the wire would keep a copy and attempt to decrypt it later if they obtained the private key.

The solution is to use a messaging protocol that provides *perfect forward secrecy* by generating a new unique session key for every conversation or exchange of messages in a random way such that the session keys could not be re-generated after the fact even if the private keys were known. The OTR chat protocol provides perfect forward secrecy (http://en.wikipedia.org/wiki/Perfect_forward_secrecy) for real time instant messaging, and the SSH protocol provides it for remote shell connections, but there is no equivalent system for email at this time.

It can be difficult to balance the convenience of mobile access to your private keys with the fact that mobile devices are much more likely to be lost, stolen, or inspected and exploited than stationary machines. An emergency or unexpected time of need might be exactly the moment when you would most want to send a confidential message or a signed message to verify your identity, but these are also the moments when you might be without access to your private keys if your mobile device was seized or not loaded with all your keys.

2.4 Secure Connections

2.4.1 Can other people read along when I check my email?

As discussed in the Chapter **Basic Tips**, whether you use webmail or an email program you should always be sure to use encryption for the entire session, from login to logout. This will keep anyone from spying on your communication with your email provider. Thankfully, this is easily done due to the popular use of *TLS/SSL* connections on email servers (See appendix **TLS/SSL**).

A TLS/SSL connection in the browser, when using webmail, will appear with **https** in the URL instead of the standard **http**, like so:

https://gigglemail.com

If your webmail host does not provide a TLS/SSL service then you should consider discontinuing use of that account; even if your emails themselves are not especially private or important, your account can very easily be hacked by “sniffing” your password! If it is

not enabled already be sure to turn it on in your account options. At the time of writing, Google's Gmail and Hotmail / Microsoft Live both automatically switch your browser to using a secure connection.

If you are using an email program like Thunderbird, Mail.app or Outlook, be sure to check that you are using TLS/SSL in the options of the program. See the chapter **Setting Up Secure Connections** in the section **Email Security**.

2.4.2 Notes

It's important to note that the administrators at providers like Hotmail or Google, that host, receive or forward your email can read your email even if you are using secure connections. It is also worth noting that the cryptographic keys protecting a TLS/SSL connection can be deliberately disclosed by site operators, or copied without their permission, breaching the confidentiality of that connection. It is also possible for a Certificate Authority to be corrupted or compromised so that it creates false certificates for keys held by eavesdroppers, making it much easier for a Man In The Middle Attack on connections using TLS/SSL (See Glossary for "Man in the Middle Attack"). An example of compromised E-mail providers is discussed here, implicating America's NSA and several email providers: <http://cryptome.info/0001/nsa-ssl-email.htm>

We also note here that a *Virtual Private Network* also a good way of securing your connections when sending and reading email but requires using a VPN client on your local machine connecting to a server. See the chapter **Virtual Private Networking** in the **Browsing** section.

2.5 Secure Emails

It is possible to send and receive secure email using standard current email programs by adding a few add-ons. The essential function of these add-ons is to make the message body (but not the To:, From:, CC: and Subject: fields) unreadable by any 3rd party that intercepts or otherwise gains access to your email or that of your conversation partner. This process is known as encryption.

Secure email is generally done using a technique called *Public-Key Cryptography*. Public-Key Cryptography is a clever technique that uses two code keys to send a message. Each user has a *public key*, which can only be used to encrypt a message but not to decrypt it. The public keys are quite safe to pass around without worrying that somebody might discover them. The *private keys* are kept secret by the person who receives the message and can be used to decode the messages that are encoded with the matching public key.

In practice, that means if Rosa wants to send Heinz a secure message, she only needs his public key which encodes the text. Upon receiving the email, Heinz then uses his private key to decrypt the message. If he wants to respond, he will need to use Rosa's public key to encrypt the response, and so on.

2.5.1 What software can I use to encrypt my email?

The most popular setup for public-key cryptography is to use *Gnu Privacy Guard (GPG)* to create and manage keys and an add-on to integrate it with standard email software. Using GPG will give you the option of encrypting sensitive mail and decoding incoming mail that has been encrypted but it will not force you to use it all the time. In years past, it was quite difficult to install and set up email encryption but recent advances have made this process relatively simple.

See section **Email Encryption** for working with GPG in the scope of your operating system and email program.

If you use a *webmail* service and wish to encrypt your email this is more difficult. You can use a GPG program on your computer to encrypt the text using your public key or you can use an add-on, like Lock The Text (<http://lockthetext.sourceforge.net/>). If you want to keep your messages private, we suggest using a dedicated email program like Thunderbird instead of webmail.

3 Understanding Browsing

3.1 Basic Tips

3.1.1 In Brief:

- When you visit a website you give away information about yourself to the site owner, unless precautions are taken.
- Your browsing on the Internet may be tracked by the sites you visit and partners of those sites. Use anti-tracking software.
- Visiting a website on the Internet is never a direct connection. Many computers, owned by many different people are involved. Use a secure connection to ensure your browsing can not be recorded.
- What you search for is of great interest to search providers. Use search anonymising software to protect your privacy.
- It is wiser to trust Open Source browsers like Mozilla Firefox as they can be more readily security audited.

3.1.2 Your browser talks about you behind your back

All browsers communicate information to the web server serving you a web page. This information includes name and version of the browser, referral information (a link on another site, for instance) and the operating system used.

Websites often use this information to customise your browsing experience, suggesting downloads for your operating system and formatting the web page to better fit your browser. Naturally however, this presents an issue and regards the user's own anonymity as this information becomes part of a larger body of data that can be used to identify you individually.

Stopping the chatter of your browser is not easily done. You can, however, falsify some of the information sent to web servers while you browse by altering data contained in the *User Agent*, the browser's identity. There is a very useful plugin for Firefox, for instance, called *User Agent Switcher* that allows you to set the browser identity to another profile selected from a drop down list of options.

3.1.3 Web sites can track you as you browse

Small files, called *cookies*, are often written onto your computer by web sites. Cookies present certain conveniences, like caching login data, session information and other data that makes your browsing experience smoother. These small pieces of data however

3 Understanding Browsing

present a significant risk to your right to anonymity on the web: they can be used to identify you if you return to a site and also to track you as you move from site to site. Coupled with the User-Agent, they present a powerful and covert means of remotely identifying your person.

The ideal solution to this problem is deny all website attempts to write cookies onto your system but this can greatly reduce the quality of your experience on the web.

See the section **Tracking** for guides as to how to stop web servers tracking you.

3.1.4 Searching online can give away information about you

When we search online using services like Bing or Google our right to privacy is already at risk, vastly more so than asking a person at an Information Desk in an airport, for instance.

Combined with the use of cookies and User Agent data this information can be used to build an evolving portrait of you over time. Advertisers consider this information very valuable, use it to make assumptions about your interests and market you products in a targeted fashion.

While some customers may sing the praises of targeted advertising and others may not care, the risks are often misunderstood. Firstly, the information collected about you may be requested by a government, even a government you did not elect (Google, for instance, is an American company and so must comply with American judicial processes and political interests). Secondly there is the risk that merely searching for information can be misconstrued as intent or political endorsement. For instance an artist studying the aesthetics of different forms of Religious Extremism might find him or herself in danger of being associated with support for the organisations studied. Finally there is the risk that this hidden profile of you may be sold on to insurance agents, provided to potential employers or other customers of the company whose search service you are using.

Even once you've ensured your cookies are cleared, your *User Agent* has been changed (see above and chapter **Tracking**) you are still giving away one crucial bit of information: the Internet Address you are connecting from (see chapter **What Happens When You Browse**). To avoid this you can use an anonymising service like Tor (see chapter **Anonymity**). If you are a Firefox user be sure to install the excellent *Google Sharing* add-on, an anonymiser for Google search. Even if you don't consciously use Google, a vast number of web sites use a customised Google Search bar as a means of exploring their content.

With the above said, there are no reasons to trust Google, Yahoo or Bing. We recommend switching to a search service that takes your right to privacy seriously: DuckDuckGo (<http://duckduckgo.com/>).

3.1.5 More eyes than you can see

The Internet is a big place and is not one network but a greater network of many smaller interconnected networks. So it follows that when you request a page from a server on the

Internet your request must traverse many machines before it reaches the server hosting the page. This journey is known as a *route* and typically includes at least 10 machines along the path. As packets move from machine to machine they are necessarily copied into memory, rewritten and passed on.

Each of the machines along a network route belongs to someone, normally a company or organisation and may be in entirely different countries. While there are efforts to standardise communication laws across countries, the situation is currently one of significant jurisdictional variation. So, while there may not be a law requiring the logging of your web browsing in your country, such laws may be in place elsewhere along your packet's route.

The only means of protecting the traffic along your route from being recorded or tampered with is using *end to end encryption* like that provided by TLS/Secure Socket Layer (See chapter **Encryption**) or a Virtual Private Network (See chapter **VPN**).

3.1.6 Your right to be unknown

Beyond the desire to minimise privacy leakage to specific service providers, you should consider obscuring the Internet Address you are connecting from more generally (see chapter **What Happens When You Browse**). The desire to achieve such anonymity spurred the creation of the *Tor Project*.

Tor uses an ever evolving network of nodes to route your connection to a site in a way that cannot be traced back to you. It is a very robust means of ensuring your Internet address cannot be logged by a remote server. See the chapter **Anonymity** for more information about how this works and how to get started with Tor.

3.2 Fears

3.2.1 Social Networking - what are the dangers?

The phenomenon of Internet based Social Networking has changed not just how people use the Internet but its very shape. Large data centers around the world, particularly in the US, have been built to cater to the sudden and vast desire for people to upload content about themselves, their interests and their lives in order to participate in Social Networking.

Social Networking as we know it with FaceBook, Twitter (and earlier MySpace) are certainly far from 'free'. Rather, these are businesses that seek to develop upon, and then exploit, a very basic anxiety: the fear of social irrelevance. As social animals we can't bear the idea of missing out and so many find themselves placing their most intimate expressions onto a businessman's hard-disk, buried deep in a data center in another country - one they will never be allowed to visit.

Despite this many would argue that the social warmth and personal validation acquired through engagement with Social Networks well out-weighs the potential loss of privacy. Such a statement however is only valid when the *full* extent of the risks are known.

The risks of Social Networking on a person's basic right to privacy are defined by:

3 Understanding Browsing

- The scope and intimacy of the user's individual contributions.
- A user posting frequently and including many personal details constructs a body of information of greater use for targeted marketing.
- The preparedness of the user to take social risks.
- A user making social connections uncritically is at greater risk from predators and social engineering attacks.
- The economic interests and partners of the organisation providing the service.
- Commissioned studies from clients, data mining, sentiment analysis.
- Political/legal demands exerted by the State against the organisation in the jurisdiction(s) in which it is resident.
- Court orders for data on a particular user (whether civilian or foreigner).
- Surveillance agendas by law enforcement or partners of the organisation.
- Sentiment analysis: projections of political intent.

With these things in mind it is possible to chart a sliding scale between projects like Diaspora and Facebook: the former promises some level of organisational transparency, a commitment to privacy and a general openness, whereas Facebook proves to be an opaque company economically able to gamble with the privacy of their users and manage civil lawsuits in the interests of looking after their clients. As such there is more likelihood of your interactions with a large Social Network service affecting how an Insurance company or potential employer considers you than a smaller, more transparent company.

3.2.2 Who can steal my identity?

This question depends on the context you are working within as you browse. A weak and universal password presents a danger of multiple services from Social Networking, Banking, WebMail etc being account hijacked. A strong and universal password on a wireless network shared with others (whether open or encrypted) is just as vulnerable. The general rule is to ensure you have a strong password (see section on **Passwords**).

Wireless networks

Here we find ourselves amidst an often underestimated risk of someone listening in on your communications using *network packet sniffing*. It matters little if the network itself is open or password secured. If someone uses the same encrypted network, he can easily capture and read all unsecured traffic of other users within the same network. A wireless key can be acquired for the cost of a cup of coffee and gives those that know how to capture and read network packets the chance to read your password while you check your email.

A simple rule always applies: if the cafe offers a network cable connection, use it! Finally, just as at a bank machine, make sure no one watches over your shoulder when you type in the password.

The browser cache

Due to the general annoyance of having to type in your password repeatedly, you allow the browser or local mail client to store it for you. This is not bad in itself, but when a laptop or phone gets stolen, this enables the thief to access the owner's email account(s). The best practice is to clear this cache every time you close your browser. All popular browsers have an option to clear this cache on exit.

One precaution can justify you holding onto your convenient cache: disk encryption. If your laptop is stolen and the thief reboots the machine, they'll be met with an encrypted disk. It is also wise to have a screen lock installed on your computer or phone. If the machine is taken from you while still running your existing user session, it cannot be accessed.

Securing your line

Whenever you log into any service you should always ensure to use encryption for the entire session. This is easily done due to the popular use of *TLS/SSL (Secure Socket Layer)*.

Check to see the service you're using (whether Email, Social Networking or online-banking) supports TLS/SSL sessions by looking for `https://` at the beginning of the URL. If not, be sure to turn it on in any settings provided by the service. To better understand how browsing the World Wide Web works, see the chapter **What Happens When I Browse?**

3.2.3 Can I get in trouble for Googling weird stuff?

Google and other search companies may comply with court orders and warrants targeting certain individuals. A web site using a customised Google Search field to find content on their site may be forced to log and supply all search queries to organisations within their local jurisdiction. Academics, artists and researchers are particularly at risk of being misunderstood, assumed to have motivations just by virtue of their apparent interests.

3.2.4 Who is keeping a record of my browsing and am I allowed to hide from them?

It is absolutely within your basic human rights, and commonly constitutionally protected, to visit web sites anonymously. Just as you're allowed to visit a public library, skim through books and put them back on the shelf without someone noting the pages and titles of your interest, you are free to browse anonymously on the Internet.

3.2.5 How to not reveal my Identity?

See the chapter on **Anonymity**.

3.2.6 How to avoid being tracked?

See the chapter on **Tracking**.

3.3 What happens when you browse

Browsing the web is communicating. You might not send as much text in terms of number of words, but it is always the browser which initiates and maintains the communication by requesting the bits and pieces which are woven into what is eventually displayed on your screen.

Browsers like Mozilla Firefox, Google Chrome, Opera, Safari & Internet Explorer all work in a similar manner. When we type a URL (e.g. “http://happybunnies.com”) in the address bar, the browser requests the website (which is just a special kind of text) from a remote server and then transforms it into colored blocks, text and images to be displayed in the browser window. To see the text the way the browser sees it, one just has to click on the **View --> Page source** menu entry in the browser. What comes up is the same webpage but in HTML – a language mainly concerned with content, context and links to other resources (CSS and JavaScript) which govern the way these contents are displayed and behave.

When the browser tries to open a webpage – and assuming there are no proxies involved – the first thing it does is to check its own cache. If there is no past memories of such website, it tries to resolve the name into an address it can actually use. It is an internet program, so it needs an Internet Protocol address (IP address or just IP). To get this address it asks a DNS Server (kind of a telephone book for internet programs) which is installed in the router of your internet access by default. The IP address is a numerical label assigned to every device in the (global) network, like the address of a house in the postal system – and as the address of your home, you should be very careful to whom you hand out the IP address you are browsing from (by default this is: to everyone). Once the IP address has been received, the browser opens a TCP (just a communication protocol) connection to the destination host and starts sending packages to a port at this address, typically no. 80 (ports are like doors to the servers, there are many but usually only a few are open), unless another path is specified. These packages travel through a number of servers on the internet (up to a couple of dozens depending on where the target address is located). The server then looks for the requested page and, if found, delivers it using the HTTP protocol. (To prevent others from reading or altering the data, TLS/SSL can be used to below HTTP to secure the connection)

When the HTTP response arrives, the browser can close the TCP connection or reuse it for subsequent requests. The response can be one of many things, from some sort of redirection or a classic Internal Server Error (500). Provided the response proceeds as expected the browser will store the page in a cache for further use, decode it (uncompress it

if compressed, rendered if video codec, etc) and display/play it according to instructions.

Now, the process can be illustrated in a little conversation between browser (B) and server (S):

B: "Hallo."

S: "Hey!"

B: "May I get that page with the happy bunnies, please?"

S: "Well, here you are."

B: "Oh, maybe you could also give me a big version of that picture of that bunny baby cuddling a teddy bear."

S: "Sure, why not."

[...]

B: "That's all for now. Thank you. Bye."

Note that there are lots of activities happening parallel to this TCP/IP exchange. Depending on how you have configured its options, your browser might be adding the page to browser history, saving cookies, checking for plugins, checking for RSS updates and communicating with a variety of servers, all while you're doing something else.

3.3.1 A topography of you: footprints

Most important: you will leave footprints. Some of them will be left on your own computer – a collection of cache data, browsing history and naughty little files with elephantine memory called cookies. They are all very convenient; speed up your browser's performance, reduce your data download or remember your passwords and preferences from Social Networks. They also snitch on your browsing habits and compile a record of everywhere you go and everything you do there. This should bother you if you are using a public computer station at a library, work at a cybercafe, or share your apartment with a nosey partner!

Even if you configure your browser to not keep a history record, reject cookies and delete cached files (or allocate zero MB of space for the cache), you would still leave breadcrumbs all over the Internet. Your IP address is recorded by default everywhere, by everyone and the packets sent are monitored by an increasing number of entities - commercial, governmental or criminal, along with some creeps and potential stalkers.

Democratic governments everywhere are redesigning regulations to require Internet providers to keep a copy of everything so they can have later access to it. In the USA, section 215 of the American PATRIOT act '*prohibits an individual or organization from revealing that it has given records to the federal government, following an investigation*'. That means that the company you pay every month as a customer to provide you with Internet access can be ordered to turn over your browsing and email records without your knowledge.

Most of the time, though, surveillance is not a 1984 affair. Google collects your searches along with your browser identification (*user agent*), your IP and a whole bunch of data that can eventually lead to your doorstep, but the ultimate aim is usually not political repression but market research. Advertisers don't fuss about advertising space any more, they just want to know everything about you. They want to know your dietary and

3 Understanding Browsing

medication habits, how many children you have and where you take them on holidays; how you make your money, how much you earn and how you like to spend it. Even more: they want to know how you *feel* about stuff. They want to know if your friends respect those feelings enough so that you can convince them to change their consumption habits. This is not a conspiracy, but rather the nature of Information Age capitalism. To paraphrase a famous observation of the current situation, the best minds of our generation are thinking about how to make people click ads.⁴

Some people think ads can be ignored or that having advertisers cater for our specific needs is a win-win situation, because at least they are spammed with things they may actually want. Even if that was the case (it isn't): should we trust Google with such intimate details of our life? Even if we trust Google to 'do no evil', it can still be bought by someone we do not trust; benevolent Larry Page and Sergey Brin could be overruled by their own Board, or their data base be sequestered by a fascistic government. One of their 30,000 employees worldwide could cut loose and run with our data. Their servers can be hacked. And in the end, they are just interested in their customers, *the companies paying for advertising*. We are just the product being sold.

Moreover; in the Social Networks our browsing habits are generating a Permanent Record, a collection of data so vast that the information that Facebook keeps about a given user alone can fill 880 pages. Nobody will be surprised to learn that Facebook's purpose is not to make us happy – again: if you are not paying for it, you're not the customer, you're the product. But even if you don't care about their commercial goals, consider this: the platform has publicly admitted hackers break into hundreds of thousands of Facebook accounts every day.

For a taste of what lurks behind the curtains of the websites you visit, install a plugin/add-on called *Ghostery* to your browser. It's like an x-ray-machine which reveals all the surveillance technology which might be (and often is) embedded in a web page, normally invisible to the user. In the same line, *Do Not Track Plus* and *Trackerblock* will give you further control over online tracking, through cookie blocking, persistent opt-out cookies, etc. Our following chapter **Tracking** will equip you with expertise in such topics.

Even in between your computer and the router, your packages can easily be intercepted by anyone using the same wireless network in the casual environment of a cafe. It is a jungle out there, but still we choose passwords like "password" and "123456", perform economic transactions and buy tickets on public wireless networks and click on links from unsolicited emails. It is not only our right to preserve our privacy but also our responsibility to defend that right against the intrusions of governments, corporations and anyone who attempts to dispossess us. If we do not exercise those rights today, we deserve whatever happens tomorrow.

1. If you are a Unix user, you can use the `tcpdump` command in the bash and view real time dns traffic. It's loads of fun! (and disturbing) ^
2. See list of TCP and UDP port numbers (http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)
3. If this exchange is happening under an HTTPS connection, the process is much

more complicated and also much safer, but you will find out more about that in a most fascinating chapter called Encryption. ^

4. This Tech Bubble Is Different (http://www.businessweek.com/magazine/content/11_17/b4225060960537.htm), Ashlee Vance (Businessweek magazine) ^

3.4 Accounts and Security

When you browse, you may be logged into various services, sometimes at the same time. It may be a company website, your email or a social networking site. Our accounts are important to us because highly sensitive information about us and others is stored on machines elsewhere on the Internet.

Keeping your accounts secure requires more than just a strong password (see section **Passwords**) and a secure communication link with the server via TLS/SSL (see chapter **Secure Connection**). Unless specified otherwise, most browsers will store your login data in tiny files called cookies, reducing the need for you re-type your password when you reconnect to those sites. This means that someone with access to your computer or phone may be able to access your accounts without having to steal your password or do sophisticated snooping.

As smart phones have become more popular there has been a dramatic rise in account hijacking with stolen phones. Laptops theft presents a similar risk. If you do choose to have the browser save your passwords then you have a few options to protect yourself:

- Use a screen lock. If you have a phone and prefer an unlock pattern system get in the habit of wiping the screen so an attacker can not guess the pattern from finger smears. On a Laptop, you should set your screensaver to require a password as well as a password on start-up.
- Encrypt your hard disk. TrueCrypt is an open and secure disk encryption system for Windows 7/Vista/XP, Mac OS X and Linux. OSX and most Linux distributions provide the option for disk encryption on install.
- Android Developers: do not enable USB debugging on your phone by default. This allows an attacker using the Android *adb shell* on a computer to access your phone's hard disk without unlocking the phone.

3.4.1 Can malicious web sites take over my accounts?

Those special cookies that contain your login data are a primary point of vulnerability. One particularly popular technique for stealing login data is called click-jacking, where the user is tricked into clicking on a seemingly innocuous link, executing a script that takes advantage of the fact you are logged in. The login data can then be stolen, giving the remote attacker access to your account. While this is a very complicated technique, it has proven effective on several occasions. Both Twitter and Facebook have seen cases of login sessions being stolen using these techniques.

It's important to develop a habit for thinking before you click on links to sites while logged into your accounts. One technique is to use another browser entirely that is not

3 Understanding Browsing

logged into your accounts as a tool for testing the safety of a link. Always confirm the address (URL) in the link to make sure it is spelled correctly. It may be a site with a name very similar to one you already trust. Note that links using URL shorteners (like <http://is.gd> and <http://bit.ly>) present a risk as you cannot see the actual link you are requesting data from.

If using Firefox on your device, use the add-on NoScript as it mitigates many of the *Cross Site Scripting* techniques that allow for your cookie to be hijacked but it will disable many fancy features on some web sites.

3.5 Tracking

When you browse the web tiny digital traces of your presence are left behind. Many web sites harmlessly use this data to compile statistics and see how many people are looking at their site and which pages are popular, but some sites go further and use various techniques to track individual users, even going as far as trying to identify them personally. It doesn't stop there however. Some firms store data in your web browser which can be used to track you on other web sites. This information can be compiled and passed on to other organizations without your knowledge or permission.

This all sounds ominous but really who cares if some big company knows about a few web sites that we have looked at? Big web sites compile and use this data for "behavioral advertising" where ads are tailored to fit your interests exactly. That's why after looking at say, the Wikipedia entry for Majorca, one may suddenly start seeing lots of ads for packaged vacations and party hats. This may seem innocent enough, but after doing a search for "Herpes Treatments" or "Fetish Communities" and suddenly seeing listings for relevant products, one may start to feel that the web is getting a bit too familiar.

Such information is also of interest to other parties, like your insurance company. If they know you have been looking at skydiving sites or forums for congenital diseases, your premiums may mysteriously start going up. Potential employers or landlords may turn you down based on their concerns about your web interests. In extreme instances, the police or tax authorities may develop an interest without you ever having committed a crime, simply based on suspicious surfing.

3.5.1 How do they track us?

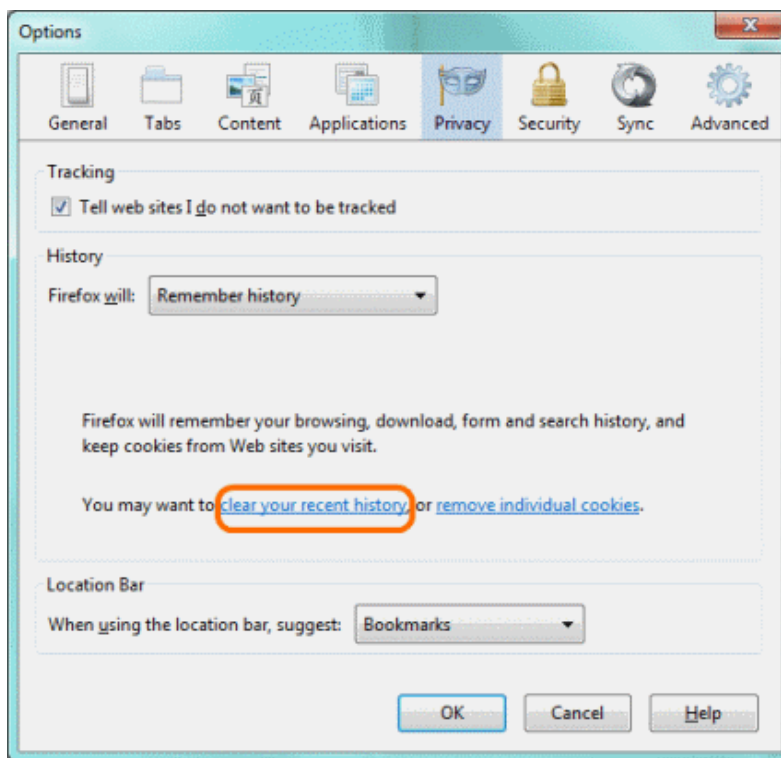
Every time you load a web page, the server software on the web site generates a record of the page viewed in a log file. This is not always a bad thing. When you log in to a website, there is a need for a way to establish your identity and keep track of who you are in order to save your preferences, or present you with customized information. It does this by passing a small file to your browser and storing a corresponding reference on the web server. This file is called a *cookie*. It sounds tasty but the problem is that this information stays on your computer even after leaving the web site and may phone home to tell the owner of the cookie about other web sites you are visiting. Some major sites, like Facebook and Google have been caught using them to keep track of your browsing even after you have logged out.

Supercookies / Evercookie / Zombie Cookies?

3.5.2 How can I prevent tracking?

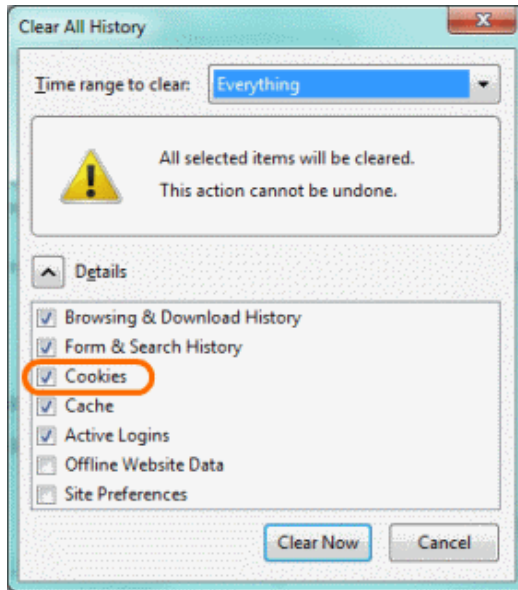
The simplest and most direct way to deal with tracking is to delete the cookie files in your browser:

In **Firefox**: 1. Click the **Firefox menu**. 2. Click **Options**. 3. Click **Privacy**. 4. Click **Clear your recent history**.



5. Make sure **Time range** to clear is set to **Everything**. 6. Tick **Cookies**.

3 Understanding Browsing



7. Click **Clear now**.

In **Chrome**: 1. Click the **Chrome** menu. 2. Click **Tools**. 3. Click **Clear browsing data**. 4. Make sure **Obliterate the following items from** is set to **The beginning of time**. 5. Tick **Delete cookies and other site and plug-in data**. 6. Click **Clear browsing data**.

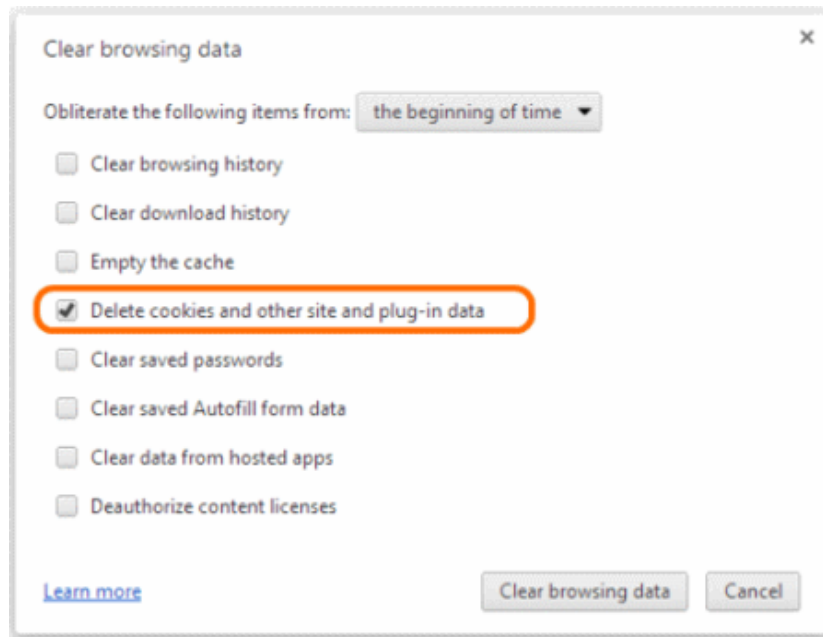


Figure 3.1: Delete Chrome Cookies

In **Internet Explorer**: 1. Click the **Tools** button (shaped like a gear). 2. Click **Safety**. 3. Click **Delete Browsing History**. 4. Tick **Cookies**. 5. Click **Delete**.

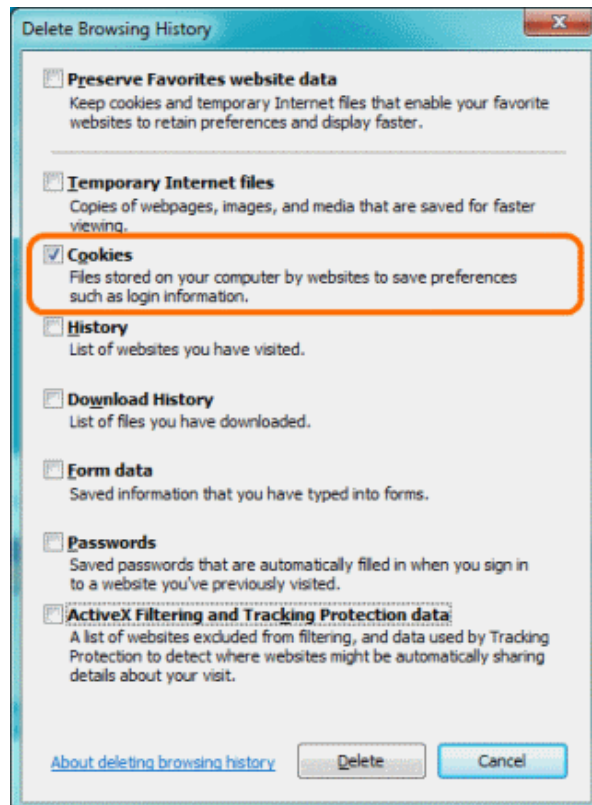
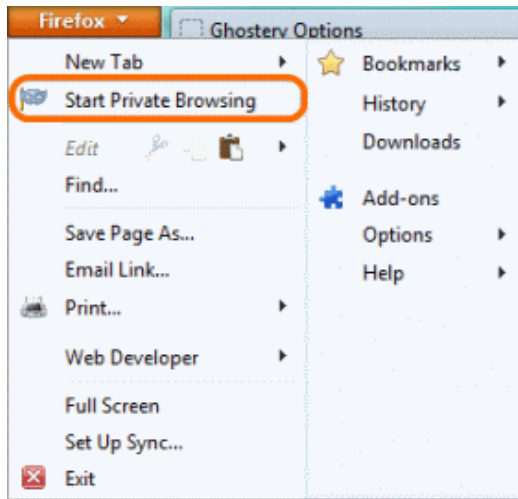


Figure 3.2: Delete IE Cookies

3 Understanding Browsing

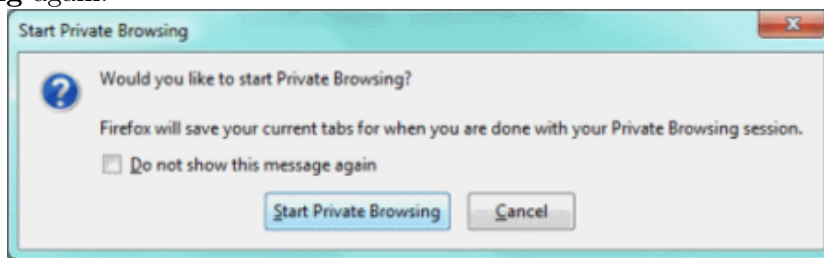
The limitation to this approach is that you will receive new cookies as soon as you return to these sites or go to any other pages with tracking components. The other disadvantage is that you will lose all of your current login sessions for any open tabs, forcing you to type in usernames and passwords again. A more convenient option, supported by current browsers is private browsing or incognito mode. This opens a temporary browser window that does not save the history of pages viewed, passwords, downloaded files or cookies. Upon closing the private browsing window, all of this information is deleted. You can enable private browsing:

In **Firefox**: 1. Click the **Firefox menu**. 2. Click **Start Private Browsing**.



3. If prompted, click **Start Private Browsing**

again.



4. The **Firefox menu**

button turns purple, showing that private browsing is on.

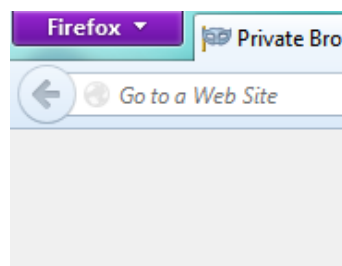
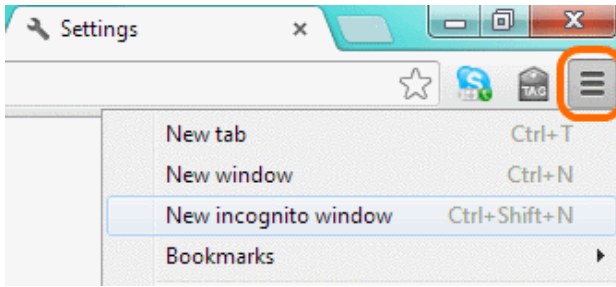


Figure 3.3: Firefox Private Browsing

In **Chrome**: 1. Click the **Chrome menu**. 2. Click **New incognito window**.



3. The **spy icon** in the top-left of the browser window shows that private browsing is on.

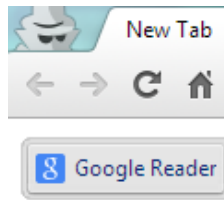
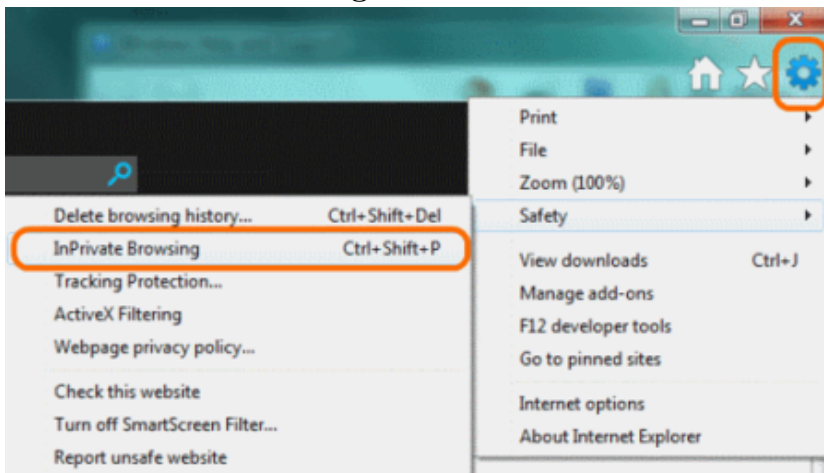


Figure 3.4: Chrome Private Browsing

In **Internet Explorer**: 1. Click the **Tools** menu, shaped like a gear. 2. Click **Safety**. 3. Click **InPrivate Browsing**.



4. The **InPrivate** logo appears in the top-left of your browser window, showing that private browsing is on.

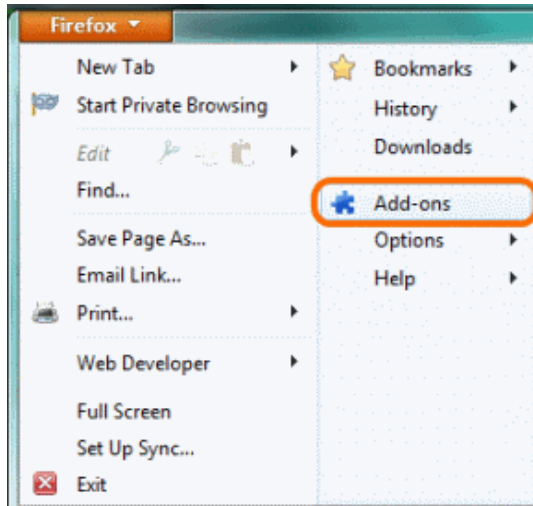


Figure 3.5: IE Private Browsing

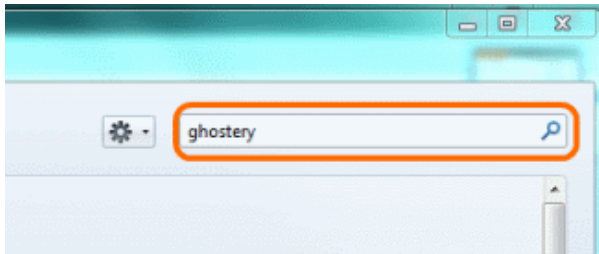
3 Understanding Browsing

This solution also has its limitations. We cannot save bookmarks, remember passwords, or take advantage of much of the convenience offered by modern browsers. Thankfully, there are several plugins specially designed to address the problems of tracking. The most extensive, in terms of features and flexibility, is Ghostery. The plugin allows you to block categories or individual services that track users. Here's how you install Ghostery:

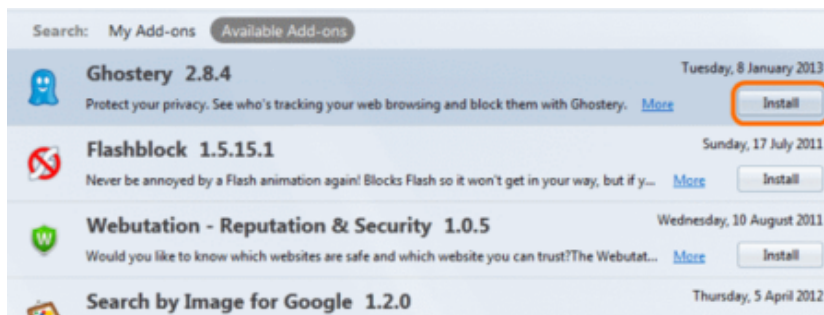
1. In Firefox, click the **Firefox** menu and select **Add-ons**.



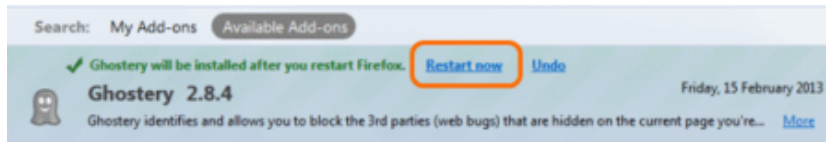
2. In the **Search** box, type "ghostery", then click the **Search** icon or press **Enter**.



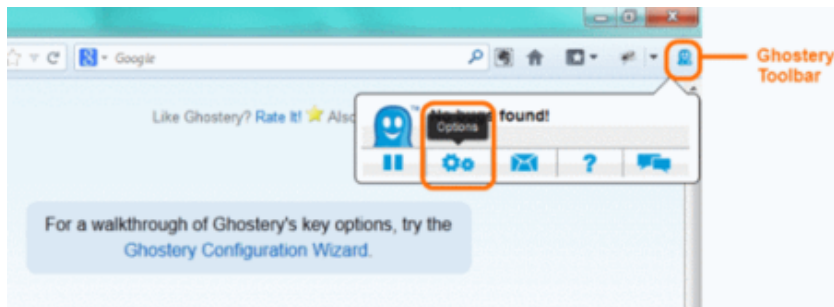
3. Find Ghostery in the list of Add-ons, and click **Install**.



4. Restart your browser by clicking **Restart Now**.



5. Click the **Ghostery toolbar** and select **Options**. Do the walkthrough and/or play with Ghostery's settings, if you want.



6. Visit a web page and have a look at its trackers.

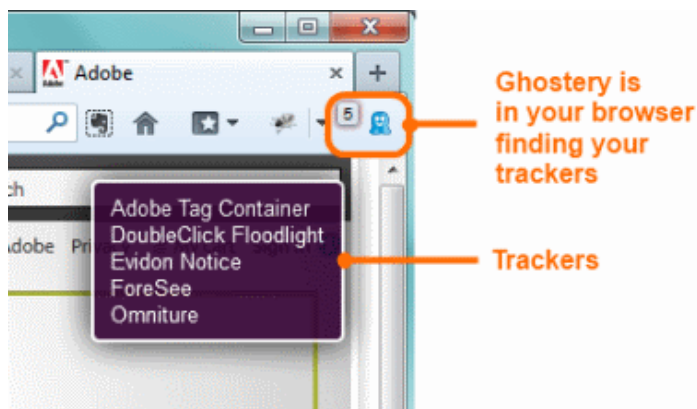


Figure 3.6: Ghostery

Another option is to install an ad-blocking plugin like AdBlockPlus. This will automatically block many of the tracking cookies sent by advertising companies but not those used by Google, Facebook and other web analytics companies. [expand on this maybe, explain “web analytics”]

How can I see who is tracking me?

The easiest way to see who is tracking you is to use the Ghostery plugin. There is a small icon on the upper right or lower right corner of your browser window that will tell you which services are tracking you on particular web sites.

{Suggestion: Add Abine.com's Do Not Track add-on. I suggest using both Ghosterly and DNT, as occasionally they block a different cookie. Abine also has Privacy Suite, recently developed which can give a proxy telephone and proxy email, similar to 10 Minute Mail or Guerrilla Mail for fill- in emails for forms.}

3.5.3 A word of warning

If you block trackers, you will have a higher level of privacy when surfing the net. However, government agencies, bosses, hackers and unscrupulous network administrators will still be able to intercept your traffic and see what you are looking at. If you want to secure your connections you will need to read the chapter on encryption. Your identity may also be visible to other people on the internet. If you want to thoroughly protect your identity while browsing, you will need to take steps toward online anonymity which is explained in another section of this book.

3.6 Anonymity

3.6.1 Intro

Article 2 of the Universal Declaration of Human Rights states:

“Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.“

One way of enforcing this basic right in hostile environments is by means of anonymity, where attempts to connect an active agent to a specific person are blocked.

Acting anonymously is also a great way to help others with a high need for protection – the bigger the herd of sheep, the harder it is to target a specific one. An easy way to do so is by using Tor, a technique which routes internet traffic between users of a special software, thus making it untraceable to any specific IP address or person without having control over the whole network (and nobody has that yet in the case of the internet). A highly functional means to protect ones own identity is by using anonymous proxy servers and Virtual Private Networks (VPN).

3.6.2 Proxy

“An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable. It is a proxy [server] computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user’s behalf, protecting personal information by hiding the client computer’s identifying information.” (<http://en.wikipedia.org/wiki/Anonymizer>)

The main purpose behind using a proxy is to hide or to change Internet address (IP address) assigned to user's computer. There can be a few reasons for needing to do so, for example:

- To anonymize access to particular server(s) and/or to obfuscate traces left in the log files of a web-server. For instance a user might need/want to access sensitive materials online (special materials, research topics or else) without triggering authorities attention.
- To break through firewalls of corporations or repressive regimes. A corporation/government can limit or completely restrict Internet access for a particular IP address or a range of IP addresses. Hiding behind a proxy will help to trick these filters and access otherwise forbidden sites.
- To watch online video and streams banned in your country due to legal issues.
- To access websites and/or materials available only for IP addresses belonging to a specific country. For example, a user wants to watch a BBC video stream (UK-only) while not residing in the UK.
- To access the Internet from a partially banned/blocked IP address. Public IP addresses can often have "bad reputation" (bandwidth abuse, scam or unsolicited email distribution) and be blocked by some web-sites and servers.

While a usual scenario would be to use proxy for accessing the Web (HTTP), practically Internet protocol can be proxied - i.e. sent via a remote server. Unlike a router, proxy server is not directly forwarding remote user requests but rather mediates those requests and echos responses back to remote user's computer.

Proxy (unless setup as "transparent") does not allow direct communication to the Internet thus applications such as browsers, chat-clients or download applications need to be made aware of the proxy server (see **Safer Browsing/Proxy settings** chapter)

3.6.3 Tor

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android. (<https://www.torproject.org>)

Tor is a system intended to enable online anonymity, composed of client software and a network of servers which can hide information about users' locations and other factors which might identify them. Imagine a message being wrapped in several layers of protection: every server needs to take off one layer, thereby immediately deleting the sender information of the previous server.

Use of this system makes it more difficult to trace Internet traffic to the user, including visits to Web sites, online posts, instant messages, and other communication forms. It is intended to protect users' personal freedom, privacy, and ability to conduct confidential

3 Understanding Browsing

business, by keeping their internet activities from being monitored. The software is open-source and the network is free of charge to use.

Tor cannot and does not attempt to protect against monitoring the traffic entering and exiting the network. While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called end-to-end correlation). *End-to-End Correlation* is a way of matching an online identity with a real person.

A recent case of this involved the FBI wanting to prove that the man Jeremy Hammon was behind an alias known to be responsible for several Anonymous attacks. Sitting outside his house, the FBI were monitoring his wireless traffic alongside a chat channel the alias was known to visit. When Jeremy went online in his apartment, inspection of the wireless packets revealed he was using Tor at the same moment the suspected alias associated with him came online in the surveilled chat channel. This was enough to incriminate Jeremy and he was arrested.

See section **Safer Browsing/Using Tor** for setup instructions.

3.7 VPN

The way your data makes it to the desired server and back to your laptop computer or a mobile device is not as straightforward as it might first seem. Say, you are connected to a wireless network at home and opening a wikipedia.org page. The path your request (data) takes will consist of multiple middle points or “hops” - in network-architect terminology. At each of these hops (which are likely to be more than 5) your data can be scooped, copied and potentially modified.

- Your wireless network (your data can be sniffed from the air)
- Your ISP (in most countries they are obliged to keep detailed logs of user activity)
- Internet Exchange Point (IXP) somewhere on another continent (usually more secure than any other *hop*)
- ISP of the hosting company that hosts the site (is probably keeping logs)
- Internal network to which the server is connected
- And multiple hops between...

Any person with physical access to the computers or the networks which are on the way from you to the remote server, intentionally or not, can collect and reveal the data that's passing from you to the remote server and back. This is especially true for so called 'last mile' situations - the few last leaps that an internet connection makes to reach a user. That includes domestic and public wireless or wired networks, telephone and mobile networks, networks in libraries, homes, schools, hotels. Your ISP can not be considered a safe, or 'data-neutral' instance either - in many countries state agencies do not even require a warrant to access your data, and there is always the risk of intrusion by paid attackers working for a deep-pocketed adversaries.

VPN - a Virtual Private Network - is a solution for this 'last-mile' leakage. VPN is a technology that allows the creation of a virtual network on top of an existing infrastructure. Such a VPN network operates using the same protocols and standards as the

underlying physical network. Programs and OS use it transparently, as if it was a separate network connection, yet its topology or the way how network nodes (you, the VPN server and, potentially, other members or services available on VPN) are interconnected in relation to the physical space is entirely redefined.

Imagine that instead of having to trust your data to every single middle-man (your local network, ISP, the state) you have a choice to pass it via a server of a VPN provider whom you trust (after a recommendation or research) - from which your data will start its journey to the remote location. VPN allows you to recreate your local and geo-political context all together - from the moment your data leaves your computer and gets into the VPN network it is fully secured with TLS/SSL type encryption. And as such it will appear as pure random noise to any node who might be spying after you. It is as if your data was traveling inside a titanium-alloy pipe, unbreakable on all the way from your laptop to the VPN server. Of course one could argue that eventually, when your data is outside the safe harbour of VPN it becomes just as vulnerable as it was - but this is only partially true. Once your data exits the VPN server it is far away from you - way beyond the reach of some creeps sniffing on the local wireless network, your venal ISP or a local government obsessed with anti-terrorism laws. A serious VPN provider would have their servers installed at a high-security Internet exchange location, rendering any physical human access, tapping or logging a difficult task.

“Today everything you do on the Internet is monitored and we want to change that. With our fast VPN service you get totally anonymous on the Internet. It’s also possible to surf censored web sites, that your school, ISP, work or country are blocking. [DarkVPN] will not only help people to surf anonymously, it also helps people in countries like China to be able to surf censored web pages. Which is your democratic right. DarknetVPN gives all VPN users an anonymous IP address. All electronic tracks will end up with us. We do not save any log files in order to achieve maximum anonymity. With us you always surfing anonymously, secure and encrypted.”
(<http://www.darknetvpn.com/about.php>)

Another interesting and often underrated features of VPN is encoded in its name - besides being **V**irtual and **P**rivate it is also a **N**etwork. VPN allows one not only to connect via the VPN server to the rest of the world but also to communicate to other members of the same VPN network without ever having to leave the safety of encrypted space. Through this functionality Virtual Private Network becomes something like a *DarkNet* (in a broader sense of the definition) - a network isolated from the Internet and inaccessible to “others”. Since a connection to VPN server, and thus the private network it facilitates, require a key or a *certificate*, only “invited” users are allowed. There is no chance that Internet stranger would gain access to what’s on a VPN without enrolling as a user or stealing someones keys. While not referred to as such, any corporate Intranet type of network is a DarkNet too.

“A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data

3 *Understanding Browsing*

across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network.”(http://en.wikipedia.org/wiki/Virtual_private_network)

Many commercial VPN providers stress the anonymity that their service provides. Quoting Ipredator.org page (a VPN service started by the people behind The Pirate Bay project):

“You’ll exchange the IP address you get from your ISP for an anonymous IP address. You get a safe/encrypted connection between your computer and the Internet”. (<https://www.ipredator.se>)

Indeed, when you access the Internet via a VPN connection it does appear as if the connection is originating from the IP address of IPredator servers.

4 Publishing And Distribution

4.1 Publishing Anonymously

Whether you are an activist operating under a totalitarian regime, an employee determined to expose some wrongdoings in your company or a vengeful writer composing a bitchy portrait of your ex-wife, you need to protect your identity. If you are not collaborating with others, the focus lies on anonymity and not encryption or privacy.

If the message is urgent and the stakes are high, one easy way to just get it out quickly is going to an internet cafe one usually does not frequent, create accounts specifically set up for the task, deliver the data and discard those accounts right after that. If you are in a hurry, consider MintEmail (<http://www.mintemail.com/>) or FilzMail (<http://www.filzmail.com/>), where your address will expire from 3 to 24 hours respectively. Do not do anything else while you're there; don't check your Gmail account, do not have a quick one on Facebook and clear all cache, cookies and history and close the browser before you leave.

If you keep these basic rules, the worst – though highly improbable – thing that could happen would be that the offered computer is compromised and logging keystrokes, revealing passwords or even your face, in case an attached webcam is remotely operated. Don't do this at work or in a place where you are a registered member or a regular visitor, like a club or a library.

If you want to maintain a constant stream of communication and maybe even establish an audience, this method quickly becomes quite cumbersome, and you might also run out of unused internet cafes. In this case you can use a machine you own, but, if you cannot dedicate one especially to this purpose, boot your computer with a different operating system (OS). This can be easily done by using a USB stick to boot a live operating system like Tails (<https://tails.boum.org/>), which comes with Tor enabled by default and includes state-of-the-art cryptographic tools. In any case, use Tor to disguise your IP.

Turn off all cookies, history and cache options and never use the same profile or the same browser for other activities. Not only would that add data to your topography as a user in the Net, but it also opens a very wide window for mistakes. If you want extra support, install *Do Not Track Plus* and *Trackerblock* or *Ghostery* in your browser add-ons menu.

Use passwords for different accounts and choose proper passwords or even passphrases (more about that in the basic tips section). Protect your entire system with a general password, change it often and do not share it with anyone, *especially* not your lover. Install a keystroke logger to see if someone sneaks into your email, especially your lover. Set up your preferences everywhere to log out of every service and platform after 5

minutes of non-use. Keep your superhero identity to yourself.

If you can maintain such level of discipline, you should even be capable of using your own internet connection. But consider this: not using a dedicated system makes it incredibly difficult to keep all the different identities separated in a safe way, and the feeling of safety often leads to carelessness. Keep a healthy level of neurosis.

Today there are many publishing possibilities, from cost-free blogging sites (Blogspot, Tumblr, WordPress, Identi.ca) to PasteBins (see glossary) and some specifically catered to anonymous users like BlogACause. Global Voices Advocacy recommends using WordPress through the Tor network. Keep a sane level of cynicism; they all act in commercial interests that you use for ‘free’ and so cannot be trusted at all, especially in that they may be bound to the demands of a legal jurisdiction that is not your own. All providers are, when it comes down to it, traitors.

If registration with these services requires a working email address, create one dedicated solely to this purpose. Avoid Gmail, Yahoo, Hotmail and other big commercial platforms with a history of turning over their users and go for an specialized service like Hushmail (<https://www.hushmail.com/>). For more on anonymous email, please find the chapter Anonymous email in the previous section.

4.1.1 Several Don'ts

Don't register a domain. There are services that will protect your identity from a simple who is query, like Anonymous Speech or Silent Register, but they will know who you are through your payment data. Unless you have the chance to purchase one in BitCoins, limit yourself to one of the domains offered by your blogging platform like `yourblogname.blogspot.com` and choose a setting outside your native country. Also, find a name that doesn't give you away easily. If you have problems with that, use a blog name generator online.

Don't open a social network account associated to your blog. If you must, keep the level of hygiene that you keep for blogging and never ever login while using your regular browser. If you have a public social network life, avoid it all together. You will eventually make a mistake.

Don't upload video, photo or audio files without using an editor to modify or erase all the meta data (photos contain information up to the GPS coordinates of the location the photo was taken at) that standard digital cameras, SmartPhones, recorders and other devices add by default. The *Metadata Anonymisation Toolkit* or *ExifTool* might help you with that.

Don't leave a history. Add X-Robots-Tag to your http headers to stop the searching spiders from indexing your website. That should include repositories like the Wayback Machine from `archive.org`. If you don't know how to do this, search along the lines of “Robots Text File Generator”.

Don't leave comments. If you must, maintain the levels of hygiene that you use for blogging and always logout when you're done and for god sakes do not troll around. Hell hath no fury like a blogger scorned.

Don't expect it to last. If you hit the pot and become a blogging sensation (like

Belle de Jour, the British PhD candidate who became a sensation and sold a book and mused two TV shows about her double life as a high escort) there will be a legion of journalists, tax auditors and obsessive fans scrutinizing your every move. You are only human: they will get to you.

Don't linger. If you realize you have already made any mistakes but nobody has caught you yet, do close all your accounts, cover your tracks and start a totally new identity. The Internet has infinite memory: one strike, and you're out of the closet.

4.2 Anonymous Email

Every data packet traveling through the Internet contains information about its sender and its recipient. This applies to email as well as any other network communication. There are several ways to reduce identifying information but no way to remove it completely.

4.2.1 Sending From Throw-away Email Accounts

One option is to use a throw-away email account. This is an account set up at a service like Gmail or Hotmail, used once or twice for anonymous exchange. When signing up for the account, you will need to provide fake information about your name and location. After using the account for a short amount of time, say 24 hours, you should never log in again. If you need to communicate further, then create a new account.

It is very important to keep in mind that these services keep logs of the IP addresses of those using them. If you are sending highly sensitive information, you will need to combine a throw away email account with Tor in order keep your IP address hidden.

If you are not expecting a reply, then an anonymous remailer like AnonEmail or Silentsender may be a useful solution. A remailer is a server that receives messages with instructions on where to send the data and acts as a relay, forwarding it from a generic address without revealing the identity of the original sender. This works best when combined with an email provider like Hushmail or RiseUp who are specially set up for secure email connections.

Both of these methods are useful, but only if you always remember that the intermediary himself knows where the original message came from and can read the messages as they come in. Despite their claims to protect your identity, these services often have user agreements that indicate their right "to disclose to third parties certain registration data about you" or they are suspected to be compromised by secret services. The only way to safely use this technique is to not trust these services at all, and apply extra security measures: send via Tor using a throw-away email address.

If you only need to receive email, services like Mailinator and MintEmail give you an email address that destroys itself after a few hours. When signing up for any account, you should provide fake information about your name and location and protect yourself by using Tor.

4.2.2 Be Careful about what you say!

The content of your message can give away your identity. If you mention details about your life, your geography, social relations or personal appearance, people may be able to determine who is sending the message. Even word choice and style of writing can be used to guess who might be behind anonymous emails.

You should not use the same user name for different accounts or use a name that you are already linked to like a childhood nickname or a favorite book character. You should never use your secret email for normal personal communication. If someone knows your secrets, do not communicate with that person using this email address. If your life depends on it, change your secret email address often as well as between providers.

Finally, once you have your whole email set up to protect your identity, vanity is your worst enemy. You need to avoid being distinct. Don't try to be clever, flamboyant or unique. Even the way you break your paragraphs is valuable data for identification, especially these days when every school essay and blog post you have written is available in the Internet. Powerful organizations can actually use these texts to build up a database that can "fingerprint" writing.

4.3 File Sharing

The term *File Sharing* refers to the practice of sharing files on a network, often with widest possible distribution in mind. Unfortunately in recent years the term has come to be popularly associated with the distribution of content registered under certain copyright licenses that disallow the distribution of copies (eg. supposed criminal activity). Regardless of this new association, file sharing remains a vital tool for many world wide: from academic groups to scientific networks and open source software communities.

In this book we wish to help you learn to privately distribute files, with other consenting people, without the content of that exchange known to others or the transaction stopped by an external party. Your basic right to anonymity and to not be spied upon protects that. Suspicions that those things *might* have been stolen and are not yours to give does not undermine that same and original right to privacy.

The history of the internet is littered with attacks of different types on publication and distribution nodes, conducted by different means (court order, Distributed Denial of Service attacks). What such events have demonstrated is that if one wants information to be persistently available and robust against attack, it is a mistake to rely upon a single node which can be neutralised.

This has recently been demonstrated by the takedown of the direct download service Megaupload, whose disappearance led to the loss of massive amounts of its users' data, much of it extraneous even to the alleged copyright infringements which formed the pretext for its closure. In similar vein ISPs will often take down web sites containing disputed material merely because it is cheaper for them to do so than to go to court and have a judge decide. Such policies leave the door open to groundless bullying by all manner of companies, organisations and individuals ready and willing to make aggressive use of legal letters. Both direct download services and ISPs are examples of centralised

structures which cannot be relied upon both because they are a single point of failure for attack, and because their commercial interests are not aligned with those of their users.

Spreading files through distribution, decentralising the data, is the best way to defend against such attacks. In the following section two realms of filesharing are profiled. The first are standard p2p technologies whose technical design is determined by the efficiency of the networks in enabling speed of distribution and discovery of content through associated search mechanisms. The second focuses on I2P as an example of a so-called darknet, its design prioritises security and anonymity over other criteria offering a robust, if less resource efficient, path to persistent availability.

The means of sharing files mentioned below are just some examples of the many P2P technologies that were developed since 1999. BitTorrent and Soulseek have very different approaches, both however were designed for easy usability by a wide public and have significant user communities. I2P is of more recent development and has a small user base.

BitTorrent has become the most popular P2P file-sharing system. The controversy that surrounds it nowadays ironically seems to help the community grow, while police, lobbied by powerful copyright holders seize torrent-tracker server hardware and pursue their operators, sometimes to the point of jailing them as in the case of The Pirate Bay.

Soulseek - while it has never been the most popular file-sharing platform, neither did it ever have the ambition. Soulseek focuses on the exchange of music between enthusiasts, underground producers, fans and researchers. The system and the community around it is completely isolated from the Web: Soulseek files can't be linked to. They are kept exclusively on the hard-disks of Soulseek users. The content of the network fully depends on how many members are connected and what they share. Files are transferred only between two users at a time and nobody but those two users are involved. Because of this 'introverted' character - and the specificity of its content - Soulseek has stayed out of sight of legislation and non-pro-copy copyright advocates.

I2P is one of several systems developed to resist censorship (others include FreeNet and Tor) and has a much smaller user community, it is highlighted here because of its inclusion of Bit Torrent functionality within its basic installation. These systems can also be used to provide hidden services, amongst others, enabling you to publish web pages within their environments.

4.3.1 BitTorrent

BitTorrent is a peer-to-peer (P2P) protocol that facilitates distribution of data stored across multiple nodes/participants of the network. There are no central servers or hubs, each node is capable of exchanging data with any other node, sometimes hundreds of them simultaneously. The fact that data is exchanged in parts between numerous nodes allows for great download speeds for popular content on BitTorrent networks, making it quickly the de facto P2P file-sharing platform.

If you are using BitTorrent to circulate material of ambiguous legality, you should know that enforcement agents typically collect information on allegedly infringing peers by participating in torrent swarms, observing and documenting the behaviour of other

peers. The large number of users creates a difficulty for the enforcement system simply at the level of scaling up - there simply are not the resources to pursue every user. Any court case will require actual evidence of data transfer between your client and another (and usually evidence of you uploading), it is enough that you provide even part of the file, not the file in its entirety, for a prosecution to have legs. But if you prefer to lean towards greater caution, you should use a VPN to route your BitTorrent traffic, as detailed in the **Using VPN** chapter.

Leeching (downloading) of a file from BitTorrent network begins with a *torrent file* or *magnet link*. A torrent file is a small file containing information on the larger files you want to download. The torrent file tells your torrent client the names of the files being shared, a URL for the *tracker* and a *hash* code, which is a unique code representing, and derived from, the underlying file - kind of like an ID or catalog number. The client can use that hash to find others seeding (uploading) those files, so you can download from their computers and check the authenticity of the chunks as they arrive.

A *Magnet Link* does away with the need for a torrent file and is essentially a hyperlink containing a description for that torrent, which your torrent client can immediately use to start finding people sharing the file you are willing to download. Magnet links don't require a tracker, instead they rely on *Distributed Hash Table (DHT)* - which you can read more about in the Glossary - and *Peer Exchange*. Magnet links do not refer to a file by its location (e.g. by IP addresses of people who have the file, or URL) but rather defines search parameters by which this file can be found. When a magnet link is loaded, the torrent client initiates an availability search which is broadcast to other nodes and is basically a shout-out "who's got anything matching this hash?!". Torrent client then connects to the nodes which responded to the shout-out and begins to download the file.

BitTorrent uses encryption to prevent providers and other man-in-the-middle from blocking and sniffing your traffic based on the content you exchange. Since BitTorrent swarms (flocks of seeders and leechers) are free for everyone to join it is possible for anyone to join a swarm and gather information about all connected peers. Using magnet links will not prevent you from being seen in a swarm; any of the nodes sharing the same file must communicate between each-other and thus, if just one of the nodes in your swarm is rogue, it will be able to see your IP address. It will also be able to determine if you are seeding the data by sending your node a download request.

One important aspect of using BitTorrent is worth a special mention. Every chunk of data that you receive (leech) is being instantly shared (seeded) with other BitTorrent users. Thus, a process of downloading transforms into a process of (involuntary) publishing, using a legal term - *making available* of that data, before the download is even complete. While BitTorrent is often used to re-distribute freely available and legitimate software, movies, music and other materials, its "making available" capacity created a lot of controversy and led to endless legal battles between copyright holders and facilitators of BitTorrent platforms. At the moment of writing this text, the co-founder of *The Pirate Bay* Gottfrid Svartholm is being detained by Swedish police after an international warrant was issued against him.

For these reasons, and a public relations campaign by copyright holders, use of BitTorrent platforms has become practically analogous to piracy. And while the meaning

of terms such as piracy, copyright and ownership in digital context is yet to be settled, many ordinary BitTorrent users have been already prosecuted on the basis of breaking copyright laws.

Most torrent clients allow you to block IP addresses of known copyright trolls using blacklists. Instead of using public torrents one can also join closed trackers or use BitTorrent over VPN or Tor.

In situations when you feel that you should be worried about your BitTorrent traffic and it's anonymity go through the following check-list:

- Check if your torrent client supports peer-blacklists.
- Check if the peer-blacklist definitions are updated on a daily basis.
- Make sure your client supports all recent protocols - DHT, PEX and Magnet links.
- Choose a torrent client that supports encrypted peers and enable it.
- Upgrade or change your torrent client if any of the above mentioned options is not available.
- Use VPN connection to disguise your BitTorrent traffic from your ISP. Make sure your VPN provider allows P2P traffic. See more tips and recommendations in Using VPN chapter.
- Do not leech and seed stuff you don't know much about.
- Be suspicious of high ratings and overly-positive comments regarding particular torrent link.

4.3.2 SoulSeek

As a peer to peer (P2P) file sharing program, the content available is determined by the users of the Soulseek client, and what files they choose to share. The network has historically had a diverse mix of music, including underground and independent artists, unreleased music, such as demos and mix-tapes, bootlegs, etc. It is entirely financed by donations, with no advertising or user fees.

“Soulseek does not endorse nor condone the sharing of copyrighted materials. You should only share and download files which you are legally allowed to, or have otherwise received permission to, share.” (<http://www.soulseekqt.net>)

Soulseek network depends on a pair of central servers. One server supports the original client and network, and the other supporting the newer network. While these central servers are key to coordinating searches and hosting chat rooms, they do not actually play a part in the transfer of files between users, which takes place directly between the users concerned.

Users can search for items; the results returned being a list of files whose names match the search term used. Searches may be explicit or may use wildcards/patterns or terms to be excluded. A feature specific to the Soulseek search engine is the inclusion of the folder names and file paths in the search list. This allows users to search by folder name.

4 Publishing And Distribution

The list of search results shows details, such as the full name and path of the file, its size, the user who is hosting the file, together with that users' average transfer rate, and, in the case of mp3 files, brief details about the encoded track itself, such as bit rate, length, etc. The resulting search list may then be sorted in a variety of ways and individual files (or folders) chosen for download.

Unlike BitTorrent, Soulseek does not support multi-source downloading or "swarming" like other post-Napster clients, and must fetch a requested file from a single source.

While the Soulseek software is free, a donation scheme exists to support the programming effort and cost of maintaining the servers. In return for donations, users are granted the privilege of being able to jump ahead of non-donating users in a queue when downloading files (but only if the files are not shared over a local area network). The Soulseek protocol search algorithms are not published, as those algorithms run on the server. However several Open Source implementations of server and client software exist for Linux, OS X and Windows.

Regarding privacy and copyright issues Soulseek stand quite far away from BitTorrent too. Soulseek has been taken to court only once, in 2008, but even that did not go anywhere. There are no indications of Soulseek users ever being brought to court or accused of illegal distribution of copyrighted materials or any other 'digital-millennium' crimes.

If you want to use the Soulseek network with some degree of real anonymity, you will need to use it over a VPN.

4.3.3 I2P

I2P began as a fork from the Freenet project, originally conceived as a method for censorship-resistant publishing and distribution. From their website:

The I2P project was formed in 2003 to support the efforts of those trying to build a more free society by offering them an uncensorable, anonymous, and secure communication system. I2P is a development effort producing a low latency, fully distributed, autonomous, scalable, anonymous, resilient, and secure network. The goal is to operate successfully in hostile environments - even when an organization with substantial financial or political resources attacks it. All aspects of the network are open source and available without cost, as this should both assure the people using it that the software does what it claims, as well as enable others to contribute and improve upon it to defeat aggressive attempts to stifle free speech. (<http://www.i2p2.de/>)

For a guide to installing the software and configuring your browser see section on Secure Filesharing - Installing I2P. Once complete, on launch you will be brought to a console page containing links to popular sites and services. In addition to the usual webpages (referred to as eePsites) there are a range of applications services available ranging from the blogging tool Syndie to a built in BitTorrent client which functions through a web interface.

5 Secure Calls And Sms

5.1 Secure Calls

Phone calls made over the normal telecommunications system have some forms of protection from third party interception, i.e. GSM mobile phones calls are encrypted. GSM calls are not encrypted end-to-end however and telephone providers are increasingly forced to give governments and law enforcement organisations access to your calls. In addition to this the encryption used in GSM has been cracked and now anyone with enough interest and capital can buy the equipment to intercept calls. A GSM Interceptor (<http://en.intercept.ws/catalog/2087.html>) is an off the shelf device to record mobile phone conversations when in the vicinity of the call. Centralised or proprietary systems like Skype also encrypt calls but have built in backdoors for secret services and governments and are at the behest of their owner (in Skype's case Microsoft). Additionally, there are a whole classification of devices called IMSI catchers which can further gather information about mobile phones, including the content of your communication.

However, there are a variety of tools you can use to secure your phone using end-to-end encryption.

5.1.1 iOS - Installing Signal

From the makers of TextSecure is a free and open source tool named Signal. <https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8> Signal uses similar same encryption methods as SilentCircle but provides their service with free and using open source tools. Additionally, the GUI is extremely easy to use. Signal will transparently detect if you are calling a fellow Signal user and ask if you wish to make a "secure call" (with Signal) or "insecure call" (without end-to-end encryption).

5.1.2 Android - Installing RedPhone

Also from the makers of Signal, there is a free and open source tool named Redphone. <https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone&hl=en> Again, RedPhone uses the similar encryption methods as SilentCircle but provides their service with free and using open source tools. Again, the GUI will transparently detect if you are calling a fellow Signal or RedPhone user and ask if you wish to make a "secure call" (with RedPhone) or "insecure call" (without end-to-end encryption). Unfortunately, RedPhone requires the Google Play framework so it will not work on phones without it (stock Cyanogenmod or similar ROMs).

5.2 Secure Messaging

SMS are short messages sent between mobile phones. The text is sent without encryption and can be read and stored by mobile phone providers and other parties with access to the network infrastructure to which you're connected. To protect your messages from interception you need to use end-to-end encryption on your text messages.

5.2.1 Android

- **TextSecure** - WhisperSystems provide an SMS encryption system for Android called TextSecure, based on public key cryptography which ensures that messages are encrypted on the wire and are also stored in an encrypted database on the device, however to ensure encryption on the wire, both parties must be using the application. It is Open Source and available through the Play Store

The encryption technology behind it (named `//axolotl//`) extends the OTR protocol so that messages can be encrypted and send even if not all of the communicating parties are online.

6 Basic Email Security

6.1 Start Using Thunderbird



Figure 6.1: Thunderbird

In upcoming sections, we will be using Mozilla’s Thunderbird e-mail program to show you how to configure your e-mail client for maximum security. Similar to Mozilla’s Firefox browser, Thunderbird has many security advantages over its counterparts like Apple Mail and Outlook.

Thunderbird is a so-called “mail user agent” (MUA). This is different from web-based e-mail services like Google’s Gmail. You must install the Thunderbird application on your computer. Thunderbird has a nice interface and features that enable you to manage multiple mailboxes, organize messages into folders, and search through mails easily.

Thunderbird can be configured to work with your existing e-mail account, whether that account is through your Internet Service Provider (such as Comcast) or through an web-based email provider (such as Gmail).

Using Thunderbird has many advantages over using web-based e-mail interfaces. These will be discussed in the following chapter. To summarize, though, Thunderbird enables much greater privacy and security than web-based e-mail services.

This section provides information on how to install Thunderbird on Windows, Mac OS X, and Ubuntu.

6.1.1 Installing Thunderbird on Windows

Installing Thunderbird involves two steps: first, download the software and then run the installation program.

1. Use your web browser to visit the Thunderbird download page at <http://www.mozillamessaging.com/en-US/thunderbird/>. This page detects your computer’s operating system and language, and recommends the best version of Thunderbird for you to use.

If you want to use Thunderbird in a different language or with a different operating system, click the *Other Systems and Languages* link on the right side of the page and select the version that you need.



Figure 6.2: Thunderbird Install

2. Click the download button to save the installation program to your computer.

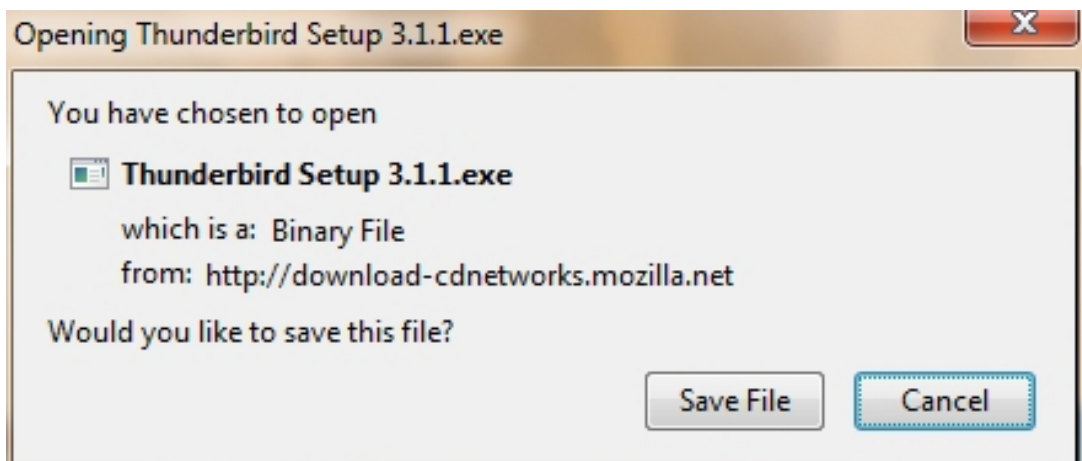


Figure 6.3: Thunderbird Install

Click the **Save** button to save the Thunderbird Setup file to your computer.

3. Close all applications running on your computer.
4. Find the setup file on your computer (it's usually in the Downloads folder or on your desktop) and then double-click it to start the installation. The first thing that the installer does is display the **Welcome to the Mozilla Thunderbird Setup Wizard** screen.



Figure 6.4: Thunderbird Install

Click the **Next** button to start the installation. If you want to cancel it, click the **Cancel** button.

5. The next thing that you see is the **Setup Type** screen. For most users the Standard setup option is good enough for their needs. The Custom setup option is recommended for experienced users only. Note that Thunderbird installs itself as your default mail application. If you do not want this, clear the checkbox labeled **Use Thunderbird as my default mail application**.

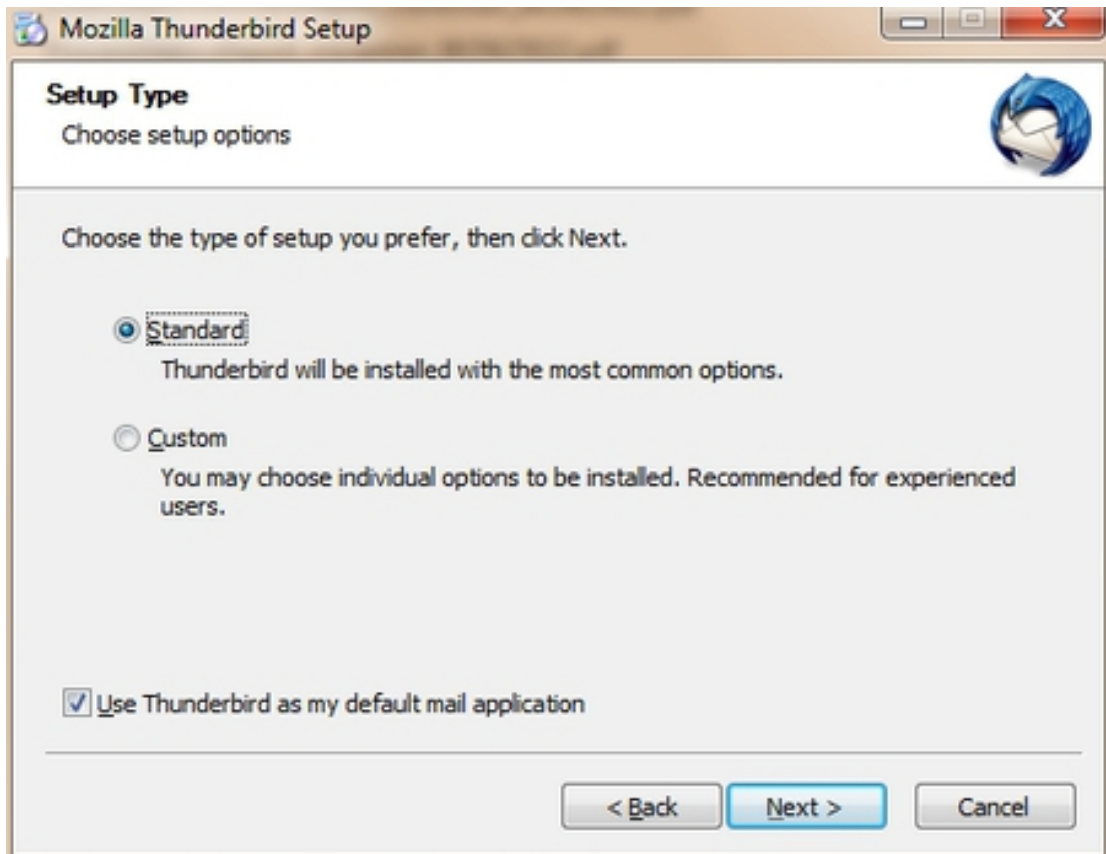


Figure 6.5: Thunderbird Install

Click the **Next** button to continue the installation.

6. After Thunderbird has been installed, click the **Finish** button to close the setup wizard.

If the **Launch Mozilla Thunderbird** now checkbox is selected, Thunderbird starts after it has been installed.



Figure 6.6: Thunderbird Install

6.1.2 Installing Thunderbird on Ubuntu

There are two different procedures for installing Thunderbird on Ubuntu: one for version 10.04 or later, and one for earlier versions of Ubuntu. We describe both below.

Thunderbird will not run without the following libraries or packages installed on your computer:

- GTK+ 2.10 or higher
- GLib 2.12 or higher
- Pango 1.14 or higher
- X.Org 1.0 or higher

Mozilla recommends that a Linux system also has the following libraries or packages installed:

- NetworkManager 0.7 or higher
- DBus 1.0 or higher
- HAL 0.5.8 or higher
- GNOME 2.16 or higher

6.1.3 Installing Thunderbird on Ubuntu 12.04 or newer

If you're using Ubuntu 12.04 or newer, the easiest way to install Thunderbird is through the Ubuntu Software Center.

1. Type Software in the Untiy search window.



Figure 6.7: Thunderbird Install

2. Click on 'Ubuntu Software Center'

3. Type “Thunderbird” in the search box and press the Enter on your keyboard. The Ubuntu Software Center finds Thunderbird in its list of available software.
4. Click the **Install** button. If Thunderbird needs any additional libraries, the Ubuntu Software Center alerts you and installs them along with Thunderbird.

You can find the shortcut to start Thunderbird in the Internet option under the Applications menu:

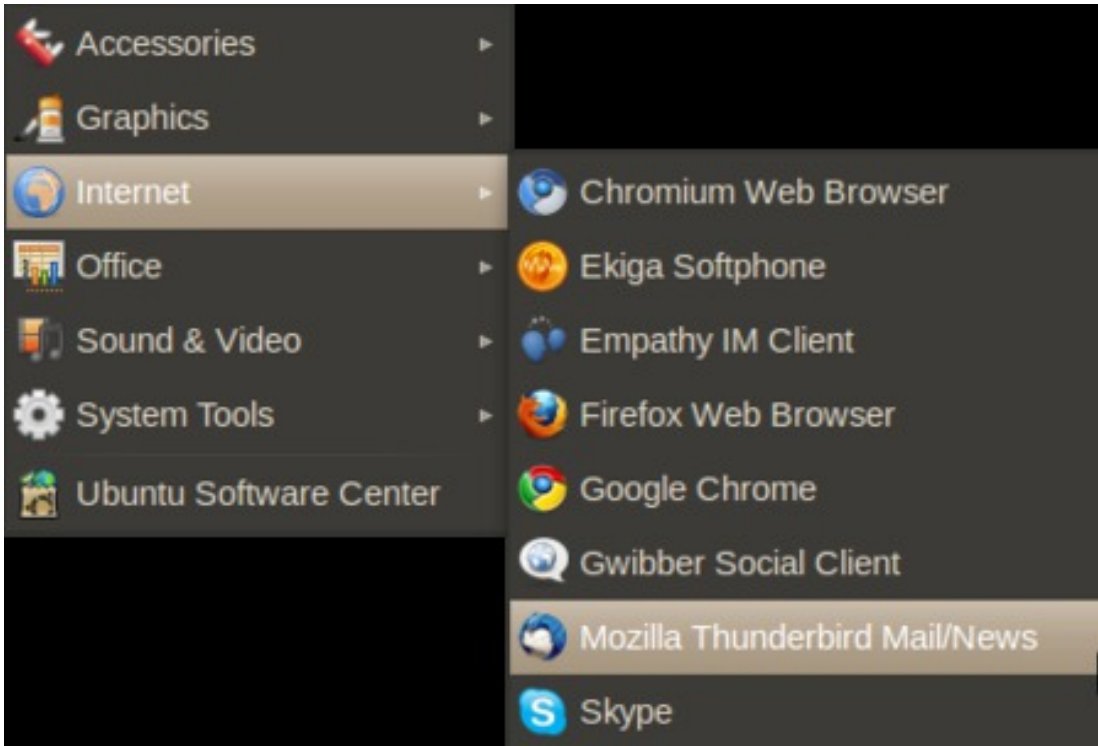


Figure 6.8: Thunderbird Install

6.1.4 Installing Thunderbird on Mac OS X

To install Thunderbird on your Mac, follow these steps:

1. Use your web browser to visit the Thunderbird download page at <http://www.mozillamessaging.com/en-US/thunderbird/>. This page detects your computer’s operating system and language, and it recommends the best version of Thunderbird for you to use.
2. Download the Thunderbird disk image. When the download is complete, the disk image may automatically open and mount a new volume called *Thunderbird*.



Figure 6.9: Thunderbird Install

If the volume did not mount automatically, open the Download folder and double-click the disk image to mount it. A Finder window appears:

3. Drag the Thunderbird icon into your Applications folder. You've installed Thunderbird!
4. Optionally, drag the Thunderbird icon from the Applications folder into the Dock. Choosing the Thunderbird icon from the Dock lets you quickly open Thunderbird from there.

Note: When you run Thunderbird for the first time, newer versions of Mac OS X (10.5 or later) will warn you that the application Thunderbird.app was downloaded from the Internet.

If you downloaded Thunderbird from the Mozilla site, click the **Open** button.



Figure 6.10: Thunderbird Install



Figure 6.11: Thunderbird Install



Figure 6.12: Thunderbird Install

6.1.5 Starting Thunderbird for the first time

After you have installed Thunderbird for the first time you will be guided through the configuration of your mail account. These settings are defined by your e-mail provider (your Internet Service Provider or web-based e-mail service provider). The next chapter describes how to set up your account and configure it for maximum security.

6.2 Setting up secure connections

There is a right (secure) way to configure your connection to your provider's mail servers and a wrong (insecure) way. The most fundamental aspect of e-mail security is the type of connection that you make to your e-mail provider's mail server.

Whenever possible, you should connect using the **SSL** (Secure Socket Layer) and **TLS** (Transport Layer Security) protocols. (**STARTTLS**, which is another option available when configuring an account, is a variation of SSL / TLS.) These protocols prevent your own system (beyond Thunderbird) and any points between your system and the mail server from intercepting and obtaining your password. SSL / TLS also prevent eavesdroppers from reading the content of your messages.

These protocols, however, only secure the connection between your computer and the mail server. They do not secure the information channel all the way to the message recipient. Once the mail servers forward the message for delivery, the message may be intercepted and read by points in between the mail server and the recipient.

This is where **PGP** (Pretty Good Privacy) comes in, which is described in the next chapter.

The first step in establishing e-mail security is a secure connection between your system and the mail servers. This chapter describes how to set up your e-mail account the right way.

6.2.1 Configuration requirements

When you configure an account, Thunderbird attempts to determine (from the email account and the account details that you provide) the connection parameters to your email provider. While Thunderbird knows the connection parameters for many email providers, it does not know them all. If the parameters are not known to Thunderbird, you will need to provide the following information to configure your account:

- **Your username**
- **Your password**
- **Incoming server:** name (such as `imap.example.com`), protocol (POP or IMAP), port (by default, 110), and security protocol
- **Outgoing server:** name (such as `smtp.example.com`), port (by default, 25), and security protocol

You should have received this information from your hosting provider. Alternatively, you can usually find this information on the support pages on the website of your hosting provider. In our example we will be using the Gmail server configuration. You can use Thunderbird with your Gmail account. To do so, you must change a configuration setting in your account. If you are not using a Gmail account, skip the next section.

6.2.2 Preparing a Gmail account for use with Thunderbird

Log in to your Gmail account in your browser. Select **Settings** from options in the top right, then go to the tab **Forwarding and POP/IMAP**. Click **Enable IMAP** and then **Save Changes**.

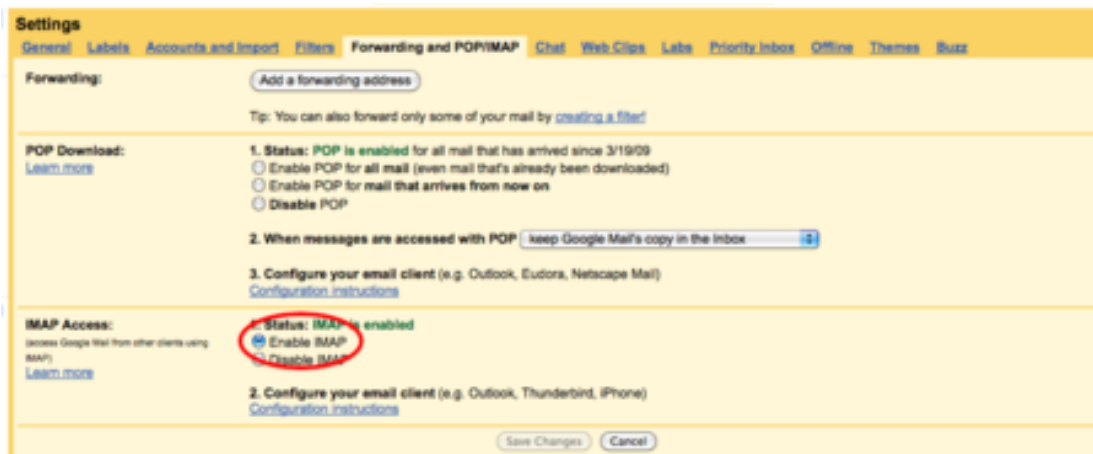


Figure 6.13: Gmail enable IMAP

6.2.3 Configuring Thunderbird to use SSL/TLS

When you start up Thunderbird for the first time, you will enter a step-by-step configuration procedure for setting up your first account. (You can invoke the account setup interface any time by selecting **File | New | Mail Account**). On the first screen, you will be asked for your name, your email-address and your password. The value you enter for your name does not have to be your real name. It will be shown to the recipient of your messages. Enter the information and click **Continue**.

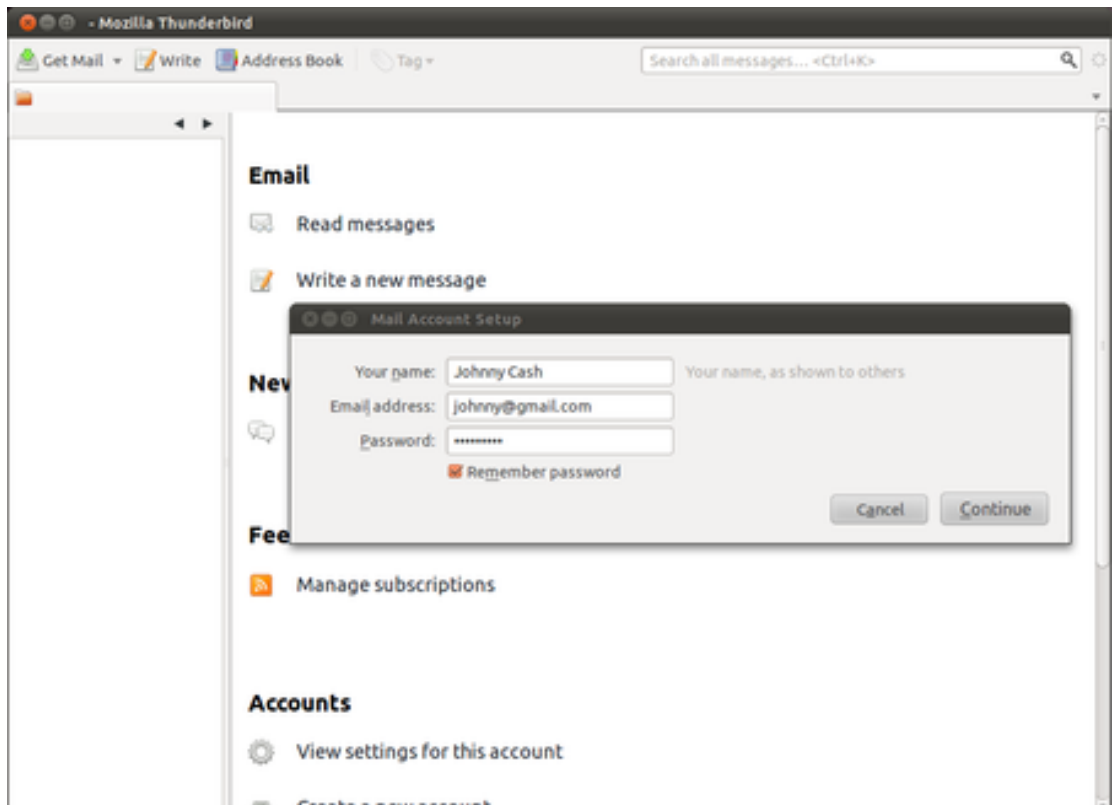


Figure 6.14: Thunderbird Configure

On the next screen, Thunderbird will attempt to determine the server names based on your email address. This may take some time, and will only work if Thunderbird knows the settings for the mail servers for your email provider. In either case you will be presented with a window where you can modify the settings. In the example below, Thunderbird has detected the settings automatically. You can see the protocol at the right side of the server names. This should be either **SSL/TLS** or **STARTTLS**. *Otherwise your connection is insecure and you should attempt manual setup.*

When you are finished, click **Create account**. If Thunderbird could not determine your server settings, click on **Manual setup** to configure the server names yourself.

6.2 Setting up secure connections

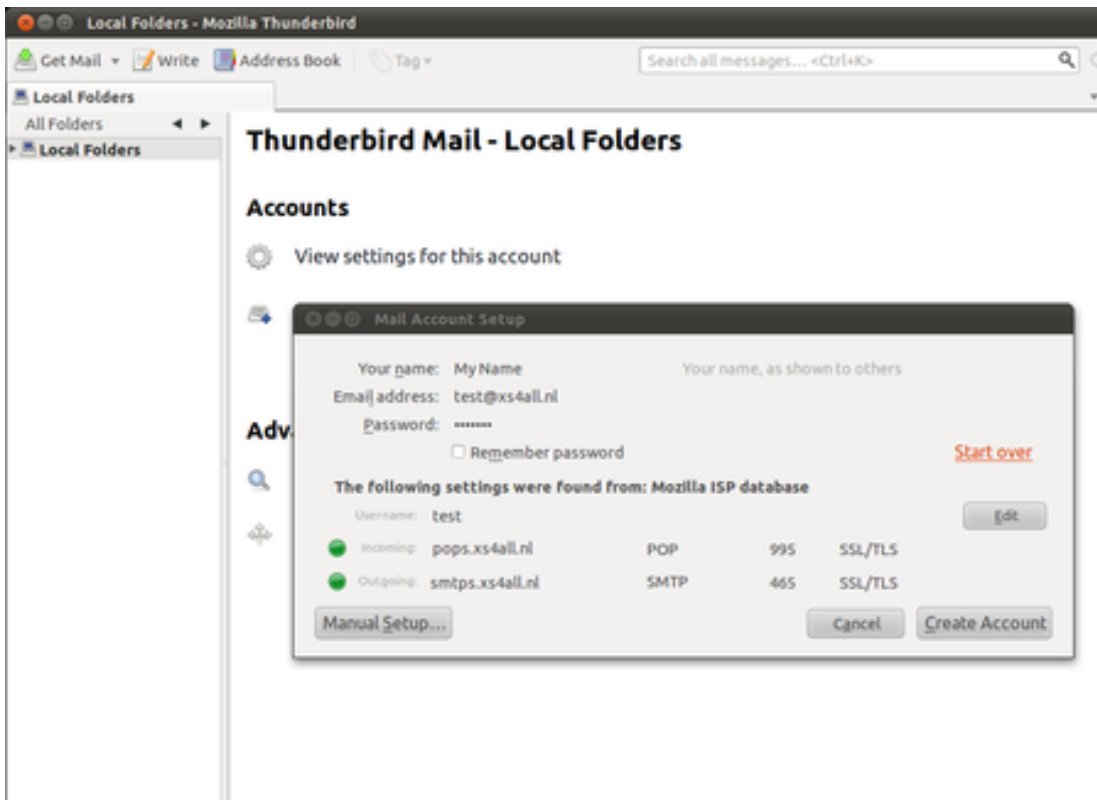


Figure 6.15: Thunderbird Install

6.2.4 Manual setup

Use the Account Settings interface to manually configure accounts in Thunderbird. The Account Settings dialog will automatically open if you select **Manual setup** in the configuration wizard. In this case we are only interested in the incoming and outgoing mail server names, and the protocol we use to connect with them. As you can see in the examples below, we enter the Gmail server names and we force them to use **TLS/SSL**, a secure method to connect to the servers.

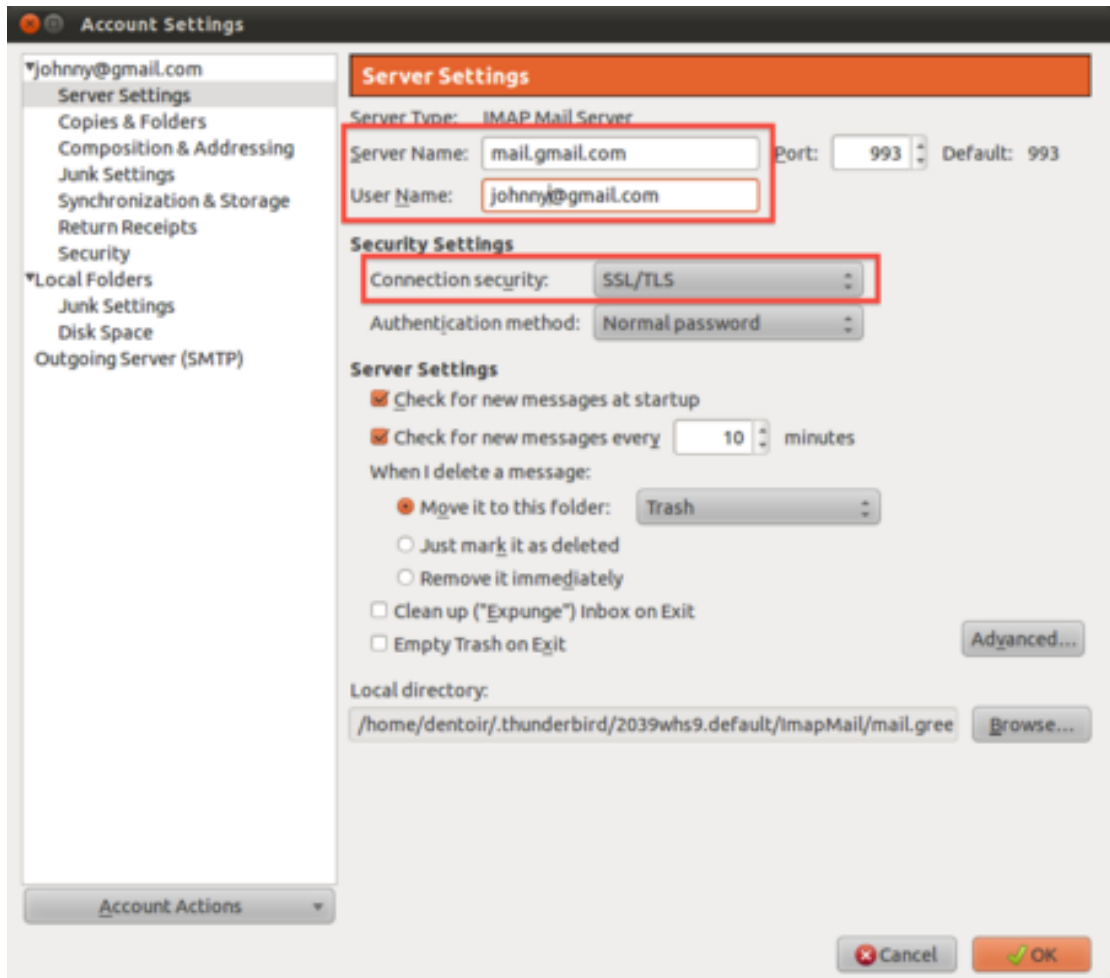


Figure 6.16: Thunderbird Install

Under ‘Server Settings’, we will find only the incoming (**IMAP**) server and its settings for that specific account.

After **Server Name** enter the name of the IMAP server, in this case `mail.gmail.com`.

As you can see we have selected ‘SSL/TLS’ under the connection security setting. This enforces encryption. Do not be scared by the authentication method **Normal**

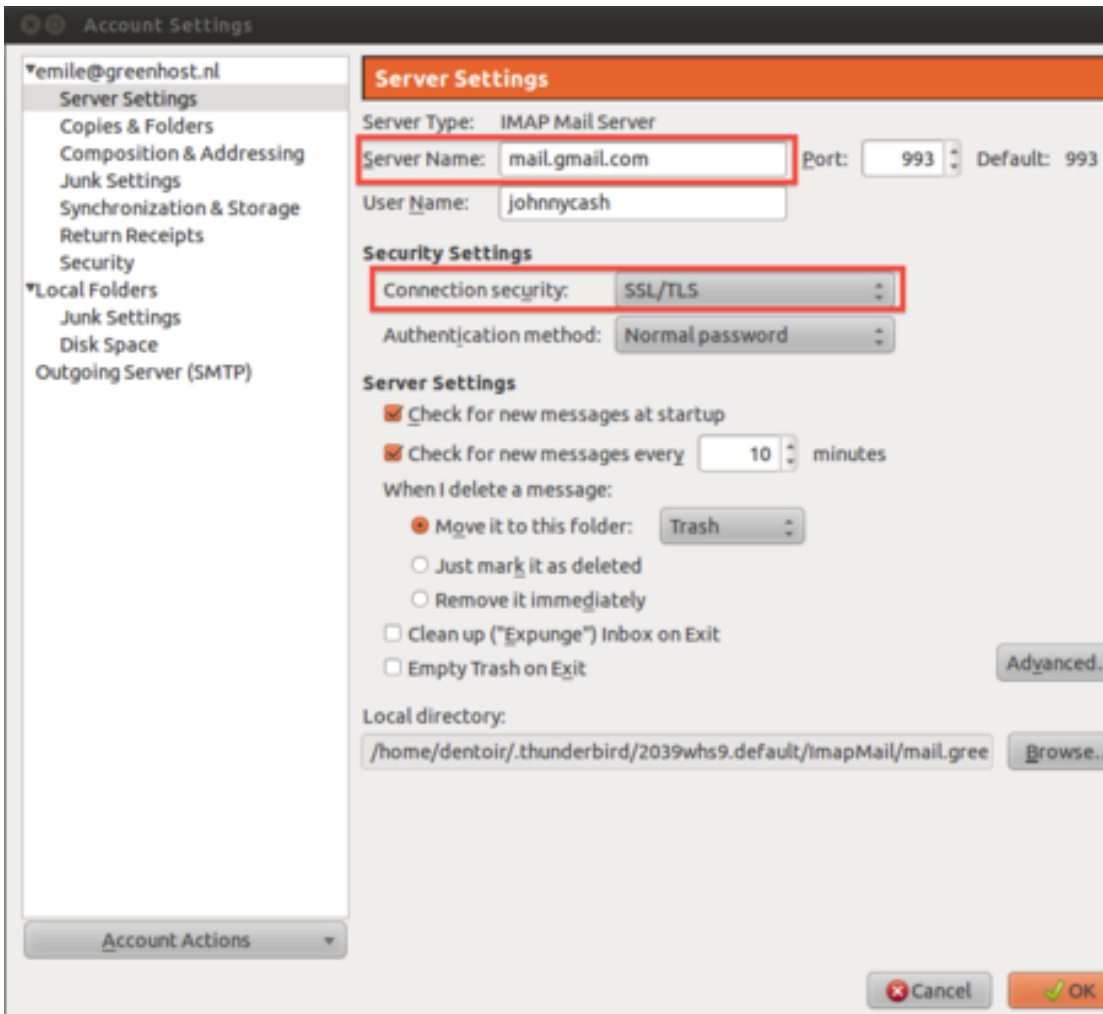


Figure 6.17: Thunderbird Install

password. The password will be automatically encrypted due to our secured connections to the server.

Finally, configure the outgoing server for the account. Click on **Outgoing Server (SMTP)** in the left panel.

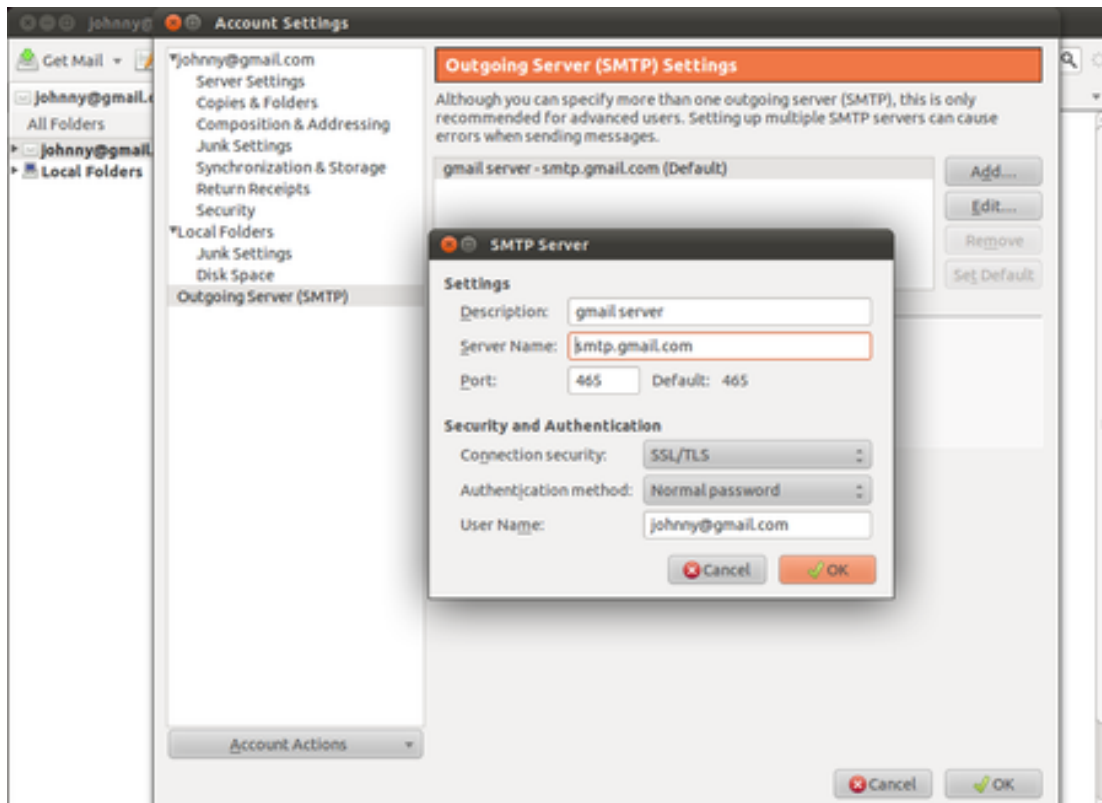


Figure 6.18: Thunderbird Install

Again, we have selected **SSL/TLS** under **Connection security**. The port will default to 465 and this should generally not have to be changed.

6.2.5 Finishing the setup, different encryption methods

Test your Thunderbird setup by trying to send and receive mails. Some email hosting providers may not support the SSL/TLS protocol, which is the preferred choice. You will get an error message saying the authentication protocol is not supported by the server. You may then switch to using STARTTLS instead. In the above two screens, select 'STARTTLS' under 'Connection security'. If this method also fails, contact your email hosting provider and ask them if they provide another way to securely connect to their servers. If they do not allow you to securely connect to their servers, then you should complain and seriously consider switching to a different provider.

6.2.6 Returning to the configuration screens

At any time you can reconfigure your email accounts by going to the Thunderbird menu bar and clicking **Edit | Account Settings** (Linux), **Tools | Account Settings** (Windows and Mac OS X).

6.3 Some Additional Security Settings

Thunderbird provides additional security measures to protect you from junk mail, identity theft, viruses (with the help of your anti-virus software, of course), intellectual property theft, and malicious web sites.

We will look at the following Thunderbird security features. First a little background on why you need to consider some of these measures:

- **Adaptive junk mail controls.** Adaptive junk mail controls allow you to train Thunderbird to identify junk email (SPAM) and remove it from your inbox. You can also mark messages as junk mail manually if your email provider's system misses the junk mail and lets it go through.
- **Integration with anti-virus software.** If your anti-virus software supports Thunderbird, you can use that software to quarantine messages that contain viruses or other malicious content. If you're wondering what anti-virus software works with Thunderbird, you can find a list here: http://kb.mozillazine.org/Antivirus_software.
- **Master password.** For your convenience, you can have Thunderbird remember each of your individual passwords of your e-mail accounts. You can specify a master password that you enter each time you start Thunderbird. This will enable Thunderbird to open all your email accounts with your saved passwords.
- **Restrictions on cookies.** Some blogs and websites attempt to send cookies (a piece of text that stores information from Web sites on your computer) with their RSS feeds. These cookies are often used by content providers to provide targeted advertising. Thunderbird rejects cookies by default, but you can configure Thunderbird to accept some or all cookies.

In the Security Preferences section of Thunderbird's Options/Preferences dialog box you can set up the preferences for these features.

- In Windows and Mac OS X, go to the 'Tools' menu and click 'Options'.
- On Ubuntu or other versions of Linux, go to the 'Edit' menu and click 'Preferences'.

6.3.1 Junk mail settings

1. In the Preferences/Options dialog box, click 'Security' and then click the 'Junk' tab.

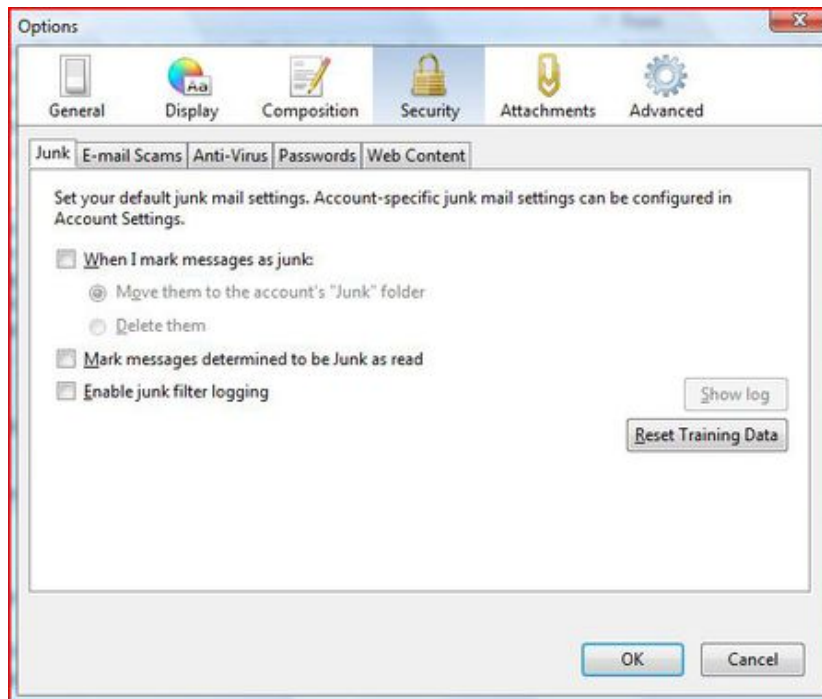


Figure 6.19: Thunderbird Security

2. Do the following:
 - To tell Thunderbird that it should handle messages marked as junk, select the check box labelled 'When I mark message as junk'.
 - To have Thunderbird move these messages to a junk folder, select the 'Move them to account's 'Junk' folder' radio button.
 - To have Thunderbird delete junk mail upon receiving it, select the 'Delete them' radio button.
3. Thunderbird will mark junk message as read if you select the check box labeled 'Mark messages determined to be Junk as read'.
4. If you want to keep a log of junk mail received, select the 'Enable junk filter logging' check box.
5. Click the 'OK' button to close the 'Options/Preferences' dialog box.

6.3.2 Scam detection and warning system

1. In the Preferences/Options dialog box, click 'Security' and then click the 'E-mail Scams' tab.
2. To have Thunderbird warn you about possible email scams, select the check box

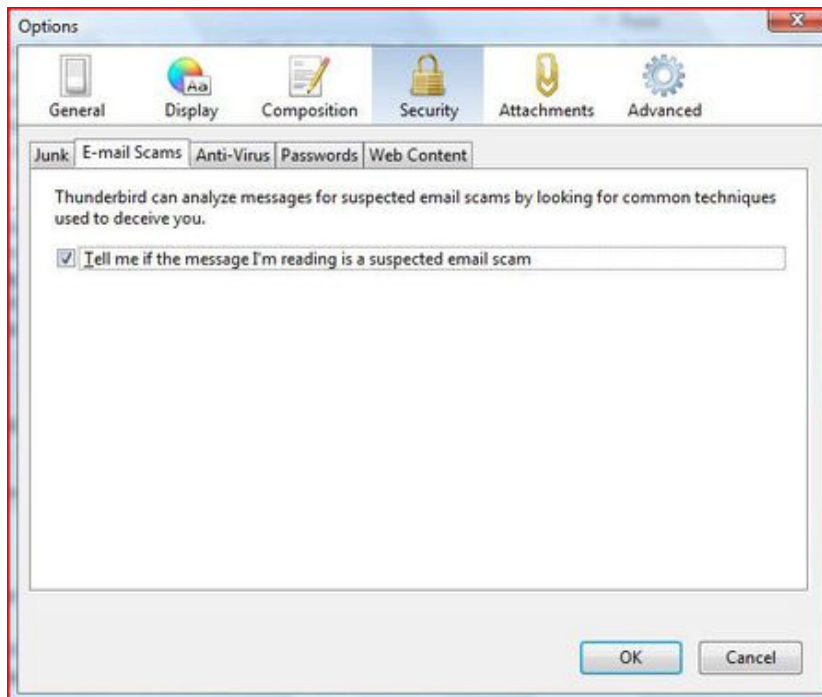


Figure 6.20: Thunderbird Security

labelled 'Tell me if the message I'm read is a suspected email scam'. To turn off this feature, deselect this check box.

3. Click the 'OK' button to close the 'Options/Preferences' dialog box.

6.3.3 Anti-virus integration

1. In the Preferences/Options dialog box, click 'Security' and then click the 'Anti-Virus' tab.
2. To turn on anti-virus integration, select the check box labeled 'Allow anti-virus clients to quarantine individual incoming messages'. To turn off this feature, deselect this check box.
3. Click the 'OK' button to close the 'Options/Preferences' dialog box.

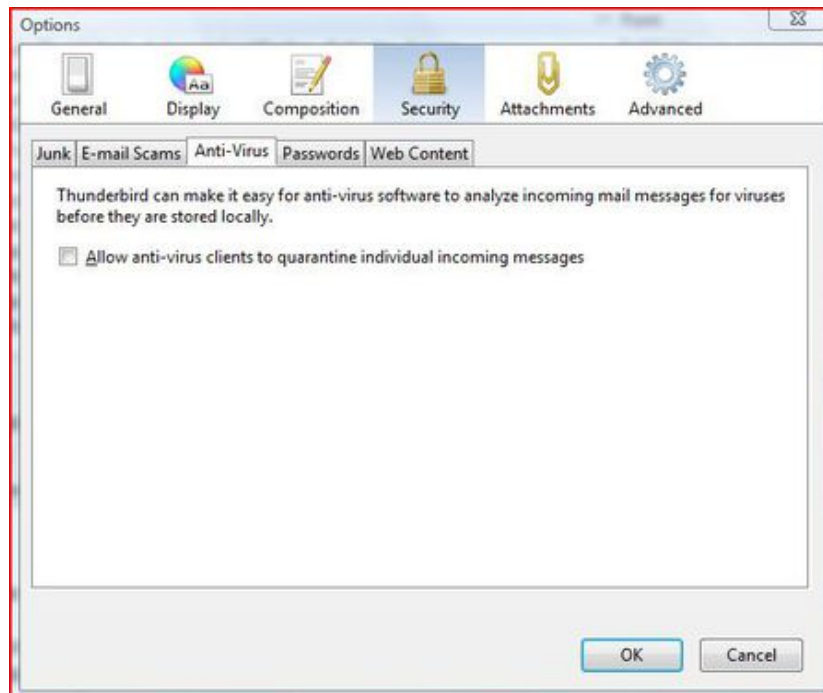


Figure 6.21: Thunderbird Security

6.3.4 Set a master password

1. In the Preferences/Options dialog box, click 'Security' and then click the 'Passwords' tab.
2. Select the check box labeled 'Use a master password'.
3. Enter your password into the 'Enter new password' and 'Re-enter password' fields.
4. Click the 'OK' button to close the Change Master Password dialog box.
5. If you want to see the passwords that you have saved in Thunderbird, click the 'Saved Passwords' button. This will open the 'Saved Passwords' dialog box.
6. To see the passwords, click the 'Show Passwords' button.
7. Click the 'Close' button to close 'Saved Passwords' dialog box.
8. Click the 'OK' button to close the 'Options/Preferences' dialog box.

6.3 Some Additional Security Settings

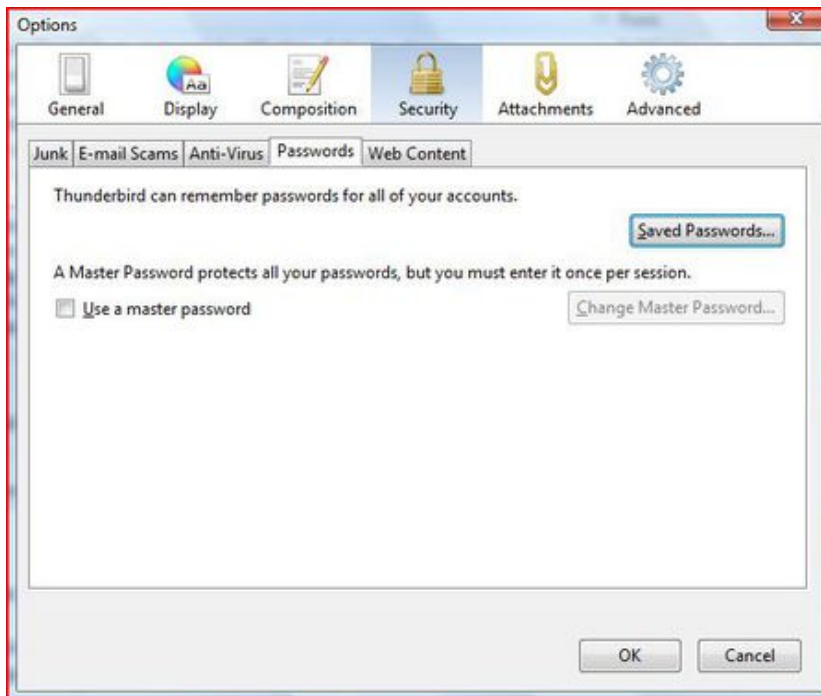


Figure 6.22: Thunderbird Security



Figure 6.23: Thunderbird Security

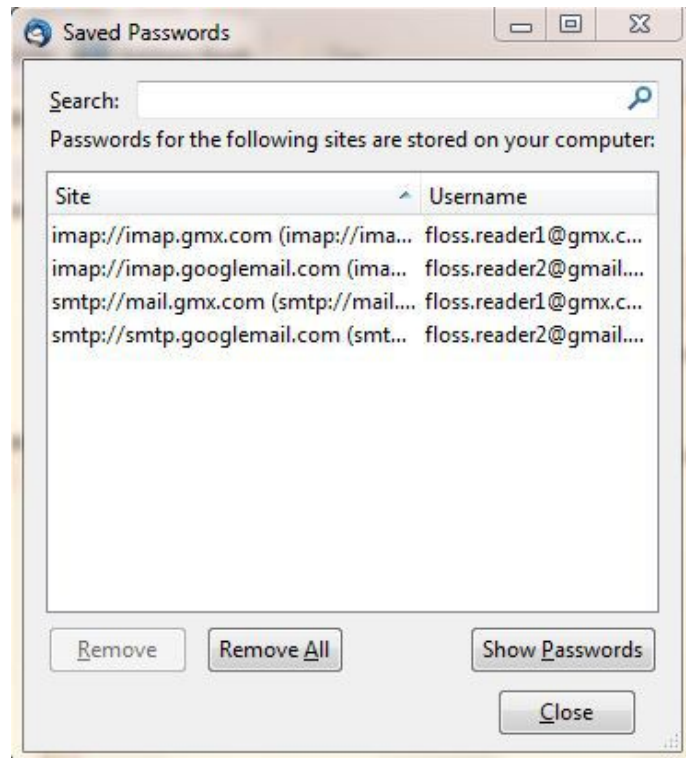


Figure 6.24: Thunderbird Security

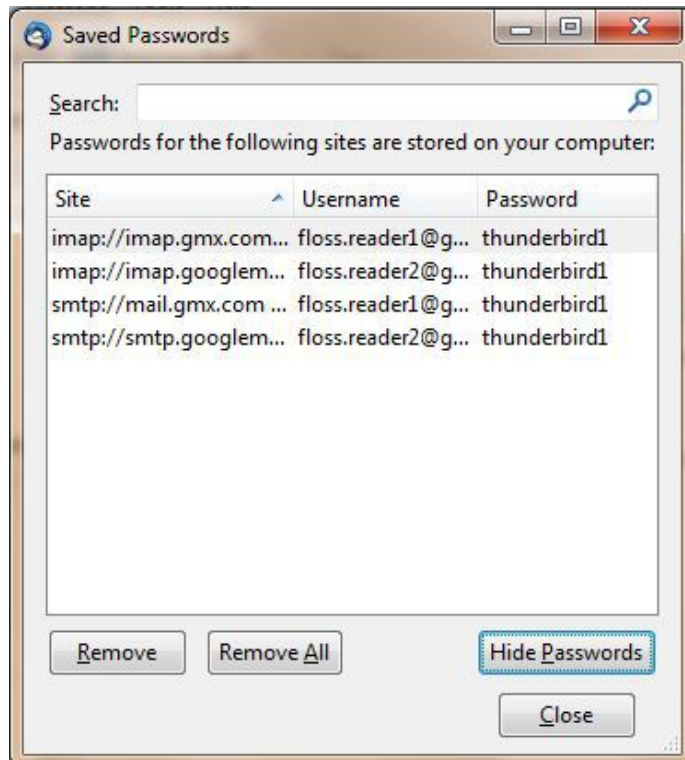


Figure 6.25: Thunderbird Security

6.3.5 Adaptive junk mail controls

You need to first open Account Settings window. Note that settings configured in the Account Settings window apply only to the account that you select in the Folders pane. You must configure local folders separately.

1. In the Folders pane right-click on an account name and select 'Settings'.

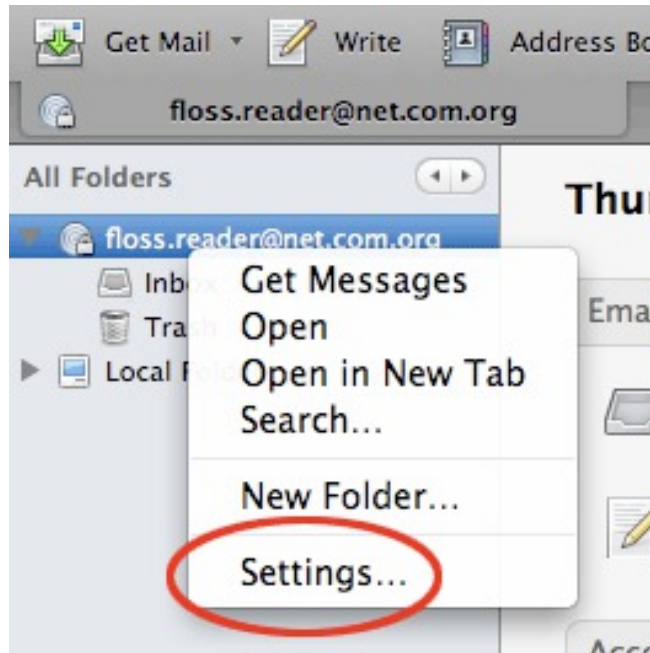


Figure 6.26: Thunderbird Security

2. In Windows or Mac go to the 'Tools' menu and select 'Account Settings'. In Linux, go to the 'Edit menu' and select 'Account Settings'.
3. To set adaptive junk mail controls for a specific account, pick an account and click 'Junk Settings'.
4. To turn on the controls, select the check box labeled 'Enable adaptive junk mail controls for this account'. To turn them off, deselect this check box.
5. If you want the controls to ignore mail from senders in your Address Book, select the check boxes next to any of the listed address books.
6. To use a mail filter such as SpamAssassin or SpamPal, select the check box labelled 'Trust junk mail headers sent by:' and pick a filter from the menu.
7. Select the check box labeled 'Move new junk messages to' if you want to move junk mail to a specified folder. Then select the destination folder to be either at your email provider or a local folder on your computer.

6.3 Some Additional Security Settings

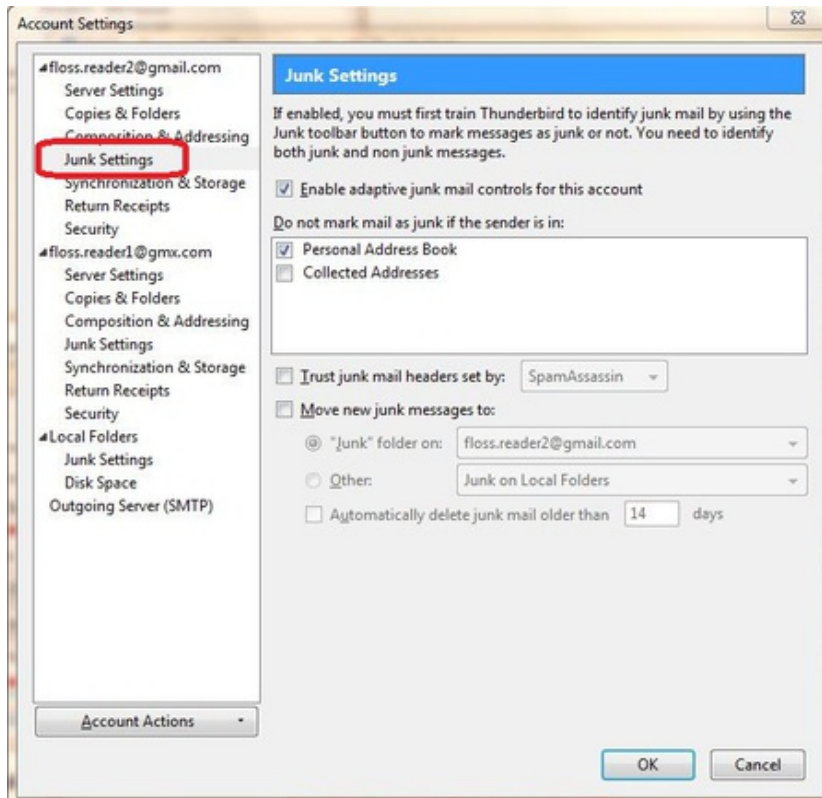


Figure 6.27: Thunderbird Security

6 *Basic Email Security*

8. Select the 'Automatically delete junk mail other 14 days' check box to have Thunderbird regularly remove junk mail. To change the time period for this process, enter a different number (in days) in the text box.
9. Click 'OK' to save your changes.

7 Email Encryption

7.1 Introducing mail encryption (PGP)



Figure 7.1: PGP

This chapter will introduce you to some basic concepts behind mail encryption. It is important to read to get some feeling of how mail encryption actually works and what its caveats and limitations are. **PGP** (Pretty Good Privacy) is the protocol we shall use for e-mail encryption. This protocol allows us to digitally sign and encrypt mail messages. It works on an end-to-end basis: messages will be encrypted on your own computer and will only be decrypted by the recipient of the message. There is no possibility for a ‘man-in-the-middle’ to decipher the contents of your encrypted message. This *excludes* the subject lines and the ‘from’ and ‘to’ addresses, which unfortunately are not encrypted in this protocol.

After having introduced these basic concepts, the next chapters will give you a hands-on guide to install the necessary tools on your operating system and get encryption up and running. We will focus on using Enigmail which is an extension for Thunderbird that helps you manage PGP encryption for your email. The installation process for Enigmail / PGP is different for Mac OSX, Windows and Ubuntu so please see the appropriate chapters in this section for instructions.

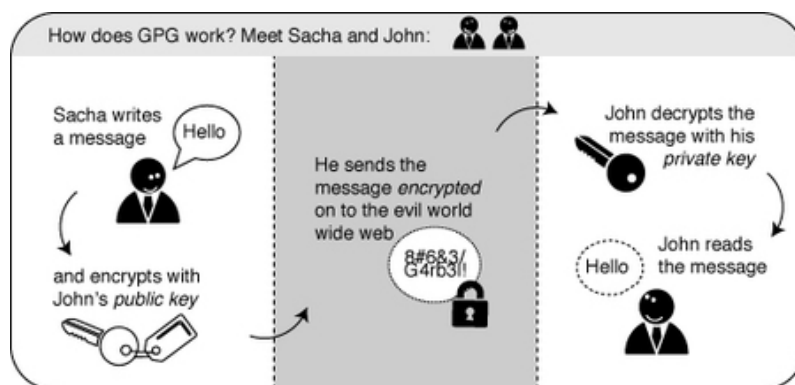


Figure 7.2: GPG Schema

7.1.1 Using a key-pair to encrypt your mail

A crucial concept in mail encryption is the usage of so-called *key-pairs*. A key-pair is just two separate files sitting on your harddisk or USB stick. Whenever you want to encrypt mails for a certain mail-account, you will need to have these files available to yourself in some form. If they are sitting at home on your computer, you will not be able to decrypt mail at the office. Putting them on a USB stick should provide a solution to this problem.

A key-pair consists of the two different keys: a public key and a secret key.

The public key: you can give this key to other people, so they can send you encrypted mails. This file does not have to be kept secret.

The secret key: this basically is your secret file to decrypt emails people send to you. It should *never* be given to someone else.

7.1.2 Sending encrypted mails to other people: you need their public key

I have five colleagues at work and I want to send encrypted mails to them. I need to have public keys for each of their addresses. They can send me these keys using ordinary mail, or they can give them to me in person, or put them on a USB stick, or they can have their keys on a website. It doesn't matter, as long as I can trust those keys really belong to the person I want to correspond with. My software puts the keys on my 'keyring', so my mail application knows how to send them encrypted mails.

7.1.3 Receiving encrypted mails from other people: they need my public key

For my five (or thirty) colleagues to be able to send *me* encrypted mails, the process goes the other way around. I need to distribute my public key to each of them.

7.1.4 Conclusion: encryption requires public key distribution!

All the people in a network of friends or colleagues wanting to send each other encrypted emails, need to distribute their public keys to each other, while keeping their secret keys a closely guarded secret. The software described in this chapter will help you do this key management.

7.2 Installing PGP on Windows

To complicate matters a little - PGP is the protocol used for encrypting e-mail by various softwares. To get PGP to work with Thunderbird we need to install GPG - a free software implementation of PGP *and* Enigmail - an extension of Thunderbird that allows you to use GPG... Confused?! Don't worry about it, all you have to know is how to encrypt your email with PGP and you need to install *both* GPG and Enigmail. Here is how to do it...

7.2.1 Installing PGP (GPG) on Microsoft Windows

The GNU Privacy Guard (GnuPG) is software which is required to send PGP encrypted or signed emails. It is necessary to install this software before being able to do any encryption.

Head to the website of the Gpg4win project. Go to <http://gpg4win.org/>
On the left side of the website, you will find a 'Download' link. Click on it.



Figure 7.3: GPG Windows

This will take you to a page where you can download the Gpg4Win. Click on the button which offers you the latest stable version (not beta) of Gpg4Win.



Figure 7.4: GPG Windows

This will download you an .exe file. Depending on your browser, you may have to double-click on this downloaded file (named something like `gpg4win-2.1.0.exe`) before something happens. Windows will ask you if you are sure you want to install this program. Answer yes.

Then complete the installation by agreeing to the license, choosing appropriate language and accepting the default options by clicking 'Next', unless you have a particular reason not to.

The installer will ask you where to put the application on your computer. The default setting should be fine but make a note of it as we may need this later. Click on 'Next' when you agree.

7.2.2 Installing with the Enigmail extension

After you have successfully installed the **PGP** software as we described above you are now ready to install the **Enigmail** add-on.

Enigmail is a Thunderbird add-on that lets you protect the privacy of your email conversations. Enigmail is simply an interface that lets you use PGP encryption from

7 Email Encryption

within Thunderbird.

Enigmail is based on public-key cryptography. In this method, each individual must generate her/his own personal key pair. The first key is known as the private key. It is protected by a password or passphrase, guarded and never shared with anyone.

The second key is known as the public key. This key can be shared with any of your correspondents. Once you have a correspondent's public key you can begin sending encrypted e-mails to this person. Only she will be able to decrypt and read your emails, because she is the only person who has access to the matching private key.

Similarly, if you send a copy of your own public key to your e-mail contacts and keep the matching private key secret, only you will be able to read encrypted messages from those contacts.

Enigmail also lets you attach digital signatures to your messages. The recipient of your message who has a genuine copy of your public key will be able to verify that the e-mail comes from you, and that its content was not tampered with on the way. Similarly, if you have a correspondent's public key, you can verify the digital signatures on her messages.

7.2.3 Installation steps

To begin installing Enigmail, perform the following steps:

1. Open **Thunderbird**, then **Select Tools > Add-ons** to activate the *Add-ons* window; the Add-ons window will appear with the default *Get Add-ons* pane enabled.
2. Enter enigmail in the search bar, like below, and click on the search icon.

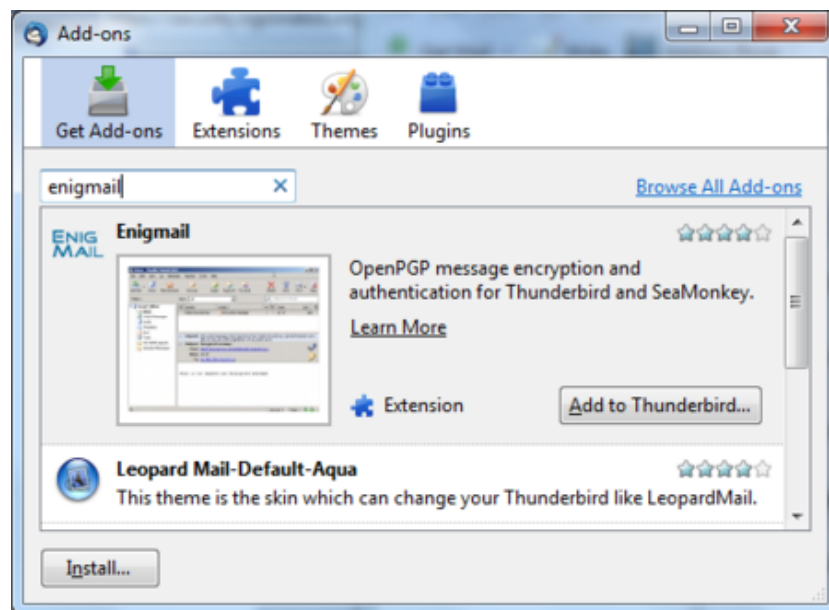


Figure 7.5: Enigmail Install

3. Simply click on the 'Add to Thunderbird' button to start the installation.
4. Thunderbird will ask you if you are certain you want to install this add-on. We trust this application so we should click on the 'Install now' button.

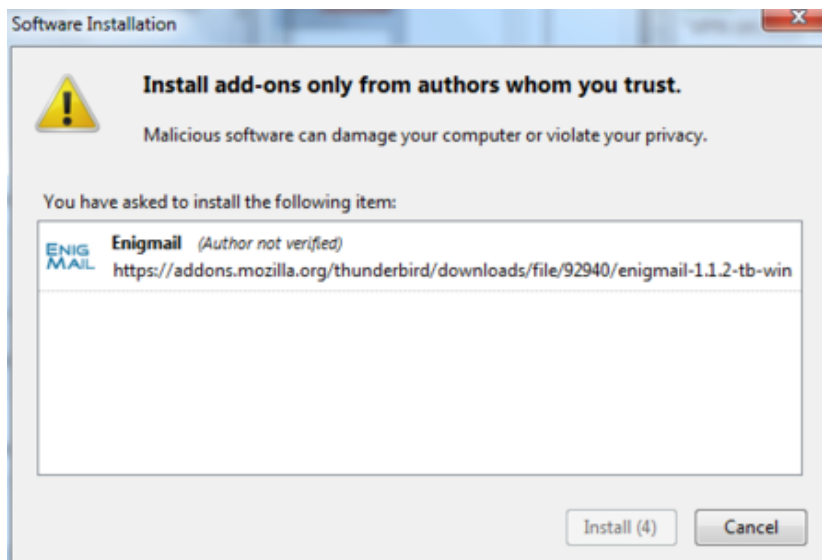


Figure 7.6: Enigmail Install

5. After some time the installation should be completed and the following window should appear. Please click on the 'Restart Thunderbird' button.

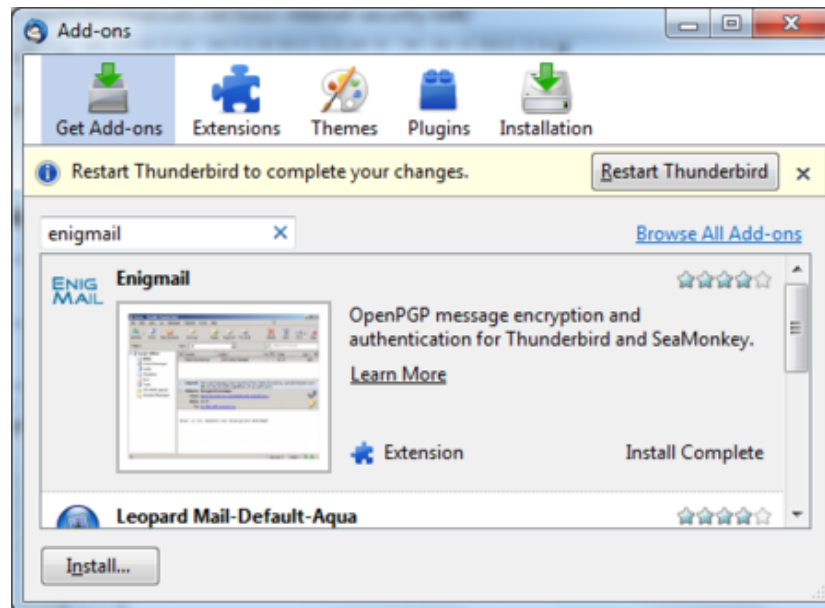


Figure 7.7: Enigmail Install

7.3 Installing PGP on OSX

The GNU Privacy Guard (GnuPG) is software which enables you to send PGP encrypted or signed emails. It is necessary to install this software before being able to do any encryption. This chapter covers the installation steps required to install GnuPG on Mac OSX.

7.3.1 Getting started

For this chapter we assume you have the latest version of:

- OSX installed (10.6.7)
- Thunderbird (3.1.10)

Note on OSX Mail: It is possible to use PGP with the build-in mail program of OSX. But we do not recommend this because this option relies on a hack of the program which is neither open or supported by its developer and breaks with every update of the mail program. So unless you really have no other option we advice you to switch to Mozilla Thunderbird as your default mail program if you want to use PGP.

7.3.2 Downloading and installing the Software

1. For OSX there is a bundle available which will install everything you need in one installation. You can get it by directing your browser to <http://www.gpgtools.org/> and clicking on the big blue disk with "Download GPGTools Installer" written under

it. It will redirect you to another page on <http://www.gpgtools.org/installer/index.html> where you can actually download the software.

(nb. We are using the latest version Firefox for this manual, so the screens might look a little bit different if you are using a different browser)

2. Download the software by choosing ‘Save File’ and clicking ‘OK’ in the dialogue.
3. Navigate to the folder where you normally store your downloads (Mostly the desktop or the downloads folder surprisingly) en double click the ‘.DMG’ file to open the virtual disk containing the installer.
4. Open the installer by double-clicking on the icon.
5. The program will check your computer to see if it can run on the computer.

(Note, if you’re Mac is bought before 2006 it will not have an intel processor required to run this software and the installation will fail. Sadly it is beyond the scope of this manual to also take into account computers over five year old)

You will be guided by the program through the next steps like accepting the license agreement. But stop pressing all the OK’s and Agrees as soon as you come to the ‘Installation Type’ screen:

6. Clicking ‘Customize’ will open this screen where you several options of programs and software to install. You can click on each one of them to get a little bit of information on what is is, what it does and why you might need it.

As said in the intro; we advise against using Apple Mail in combination with PGP. Therefore you won’t be needing ‘GPGMail’, as this enables PGP on Apple Mail, and you can uncheck it.

‘**Enigmail**’ on the other hand is very important as it is the component that will enable Thunderbird to use PGP. In the screen shot here it is greyed out as the installer wasn’t able to identify my installation of Thunderbird. Since this seems to be a bug. You can also install Enigmail from within Thunderbird as is explained in another chapter.

If the option is not greyed out in your installation, you should tick it.

After you checked all the components you want to install click ‘Install’ to proceed. The installer will ask you for your password and after you enter that the installation will run and complete; Hooray!

7 Email Encryption



Figure 7.8: GPG Install

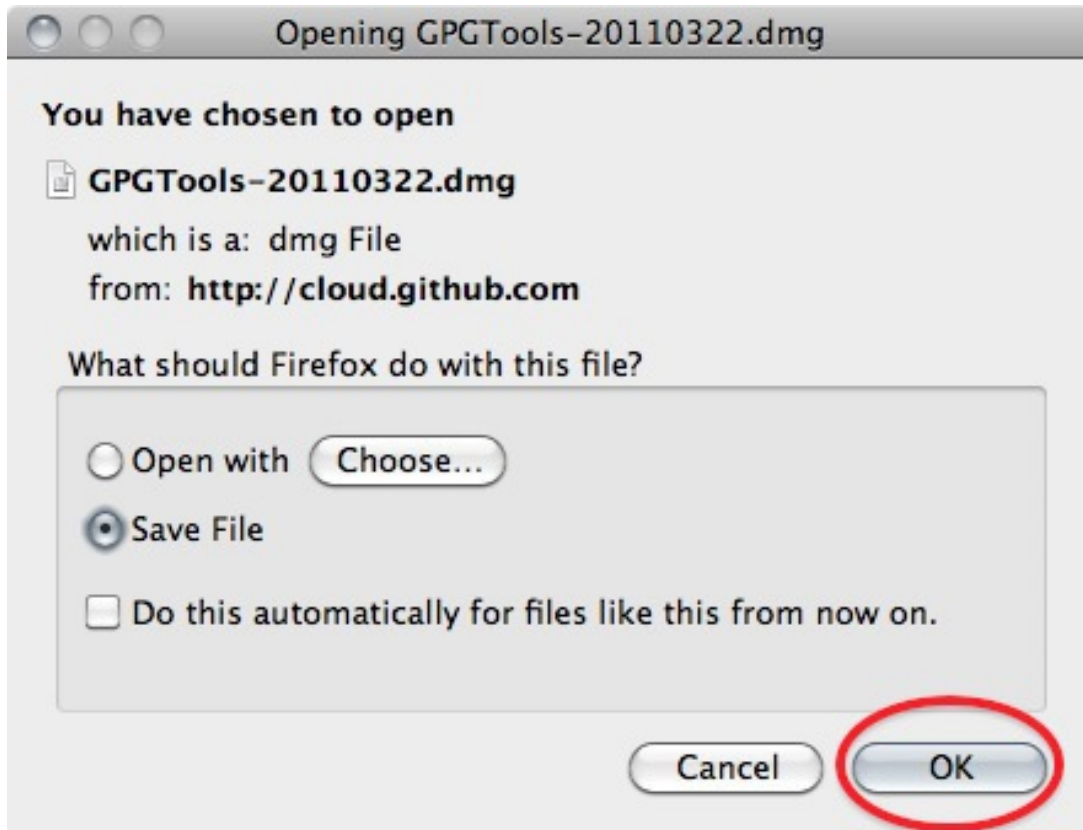


Figure 7.9: GPG Install

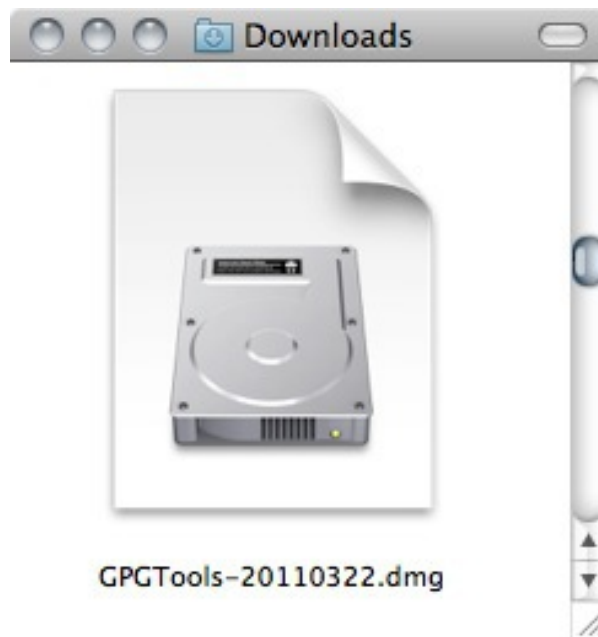


Figure 7.10: GPG Install



Figure 7.11: GPG Install



Figure 7.12: GPG Install



Figure 7.13: GPG Install

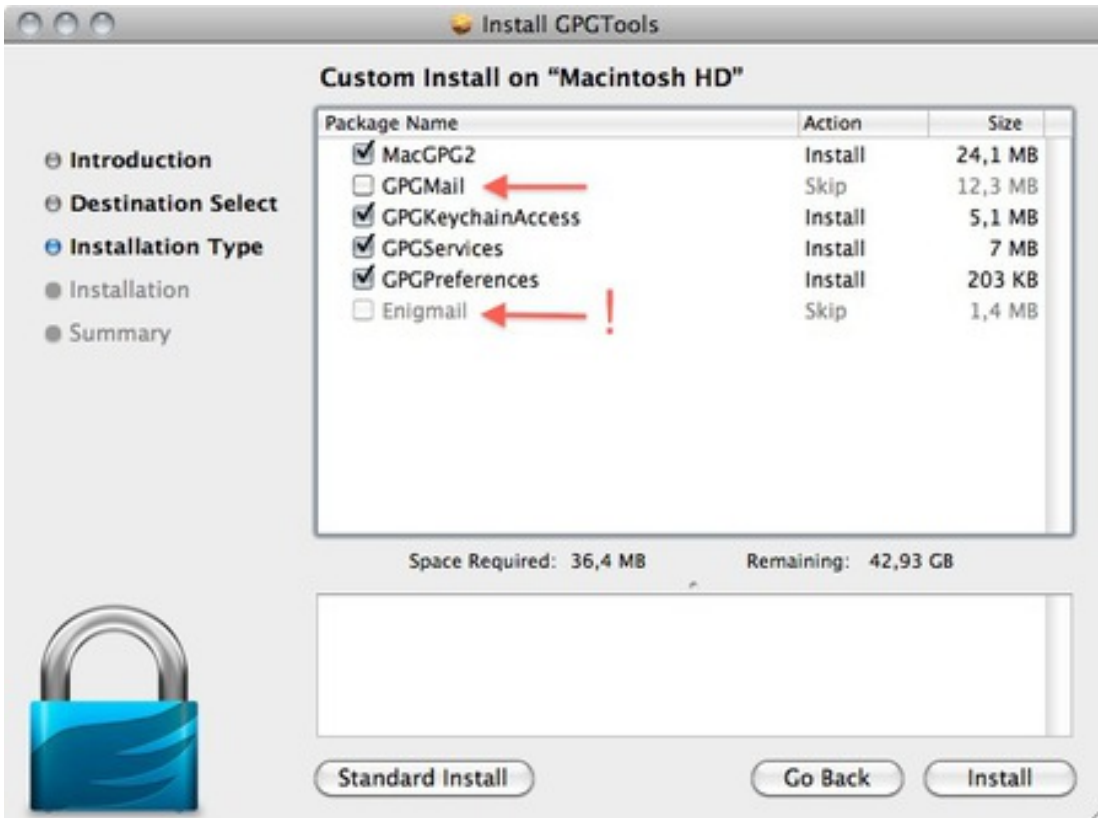


Figure 7.14: GPG Install



Figure 7.15: GPG Install

7.3.3 Installing up Engimail

1. Open **Thunderbird**, then **Select Tools > Add-ons** to activate the *Add-ons* window; the Add-ons window will appear with the default *Get Add-ons* pane enabled.

In the Add-On window, you can search for ‘Enigmail’ and install the extension by clicking ‘Add to Thunderbird ...’

2. After you open the Add-On window, you can search for ‘Enigmail’ and install the extension by clicking ‘Add to Thunderbird ...’
3. Click on ‘Install Now’ to download and install the extension.

Be aware that you will have to restart Thunderbird to use the functionality of this extension!

Now that you have successfully downloaded and installed Enigmail and PGP you can go on to the Chapter that deals with setting up the software for use.

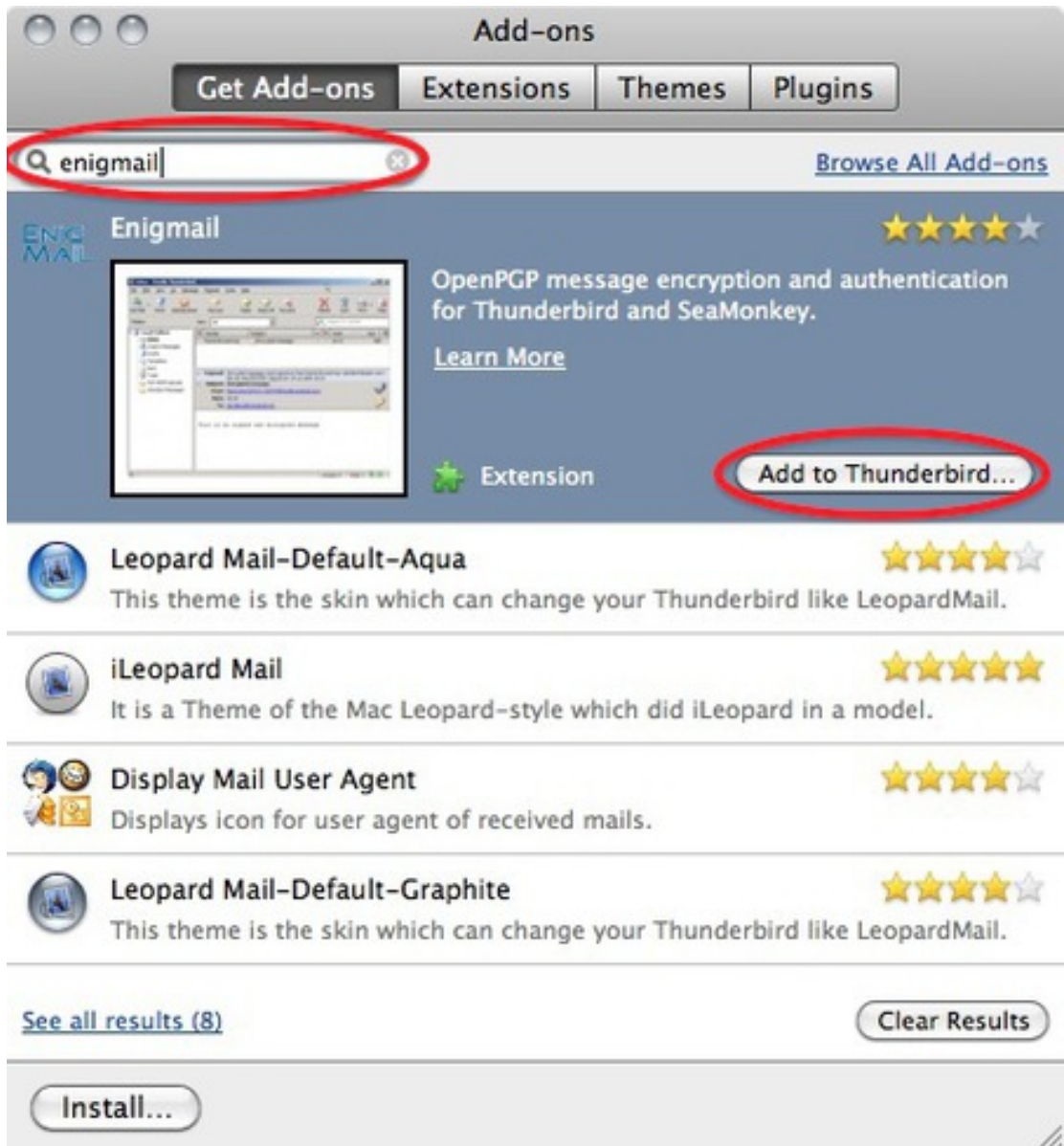


Figure 7.16: GPG Install

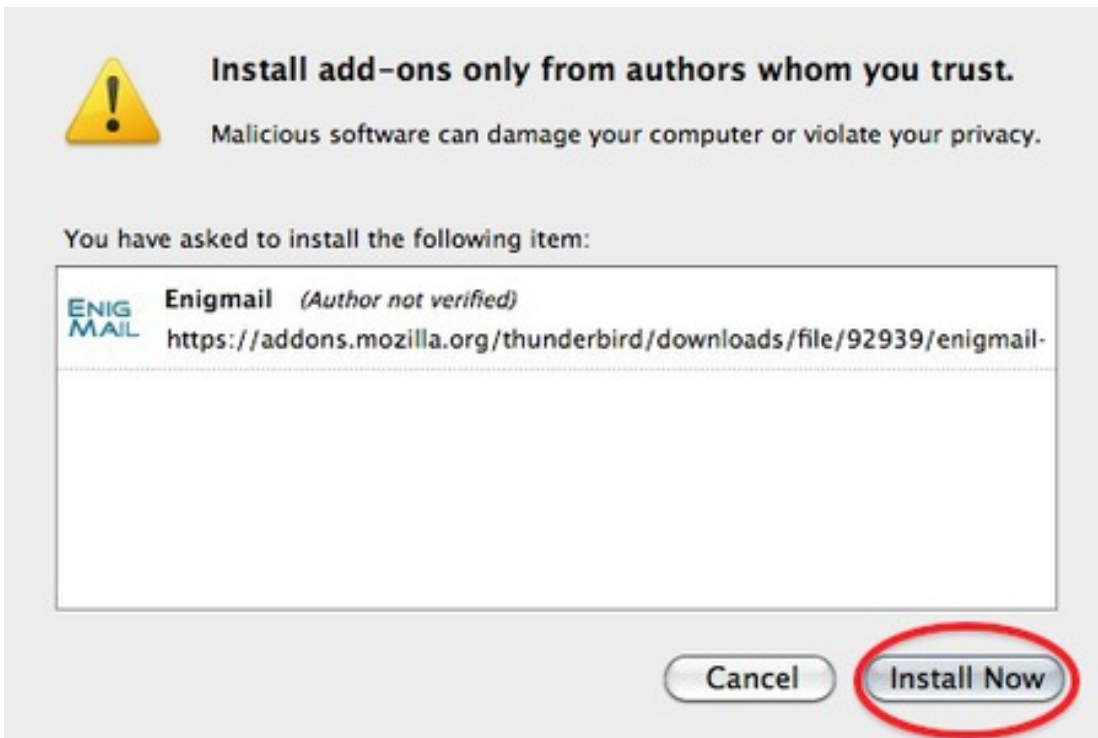


Figure 7.17: GPG Install

7.4 Installing PGP on Ubuntu

We will use the Ubuntu Software Centre for installing PGP (Enigmail and accessories). First open the Ubuntu Software Center through the Unity menu by typing 'software' into the Unity search area



Figure 7.18: PGP Install

Click on the 'Ubuntu Software Center'.

Type into the search field 'Enigmail' and search results should be returned automatically:

Highlight the Enigmail item (it should be highlighted by default) and click 'Install' and you will be asked to authenticate the installation process.

Enter your password and click 'Authenticate'. The installation process will begin.

When the process is completed you get very little feedback from Ubuntu. The progress bar at the top left disappears. The 'In Progress' text on the right also disappears. Enigmail should now be installed.



Figure 7.19: PGP Install

7.5 Installing GPG on Android

With the growing usage of mobile phones for e-mail, it's interesting to be able to use GPG also on your mobile. This way you can still read the messages sent to you in GPG on your phone and not only on your computer.

Install the *Android Privacy Guard (APG)* and *K-9 Mail* applications to your Android device from the Google Play Store or another trusted source.

1. Generate a new private key that uses DSA-Elgamal with your PC's GPG installation (You can only create keys with up to 1024bit key length on Android itself).
2. Copy the private key to your Android device.
3. Import the private key to APG. You may wish to have APG automatically delete the plaintext copy of your private key from your Android device's filesystem.
4. Set-up your e-mail accounts in *K-9 Mail*.
5. In the settings for each account, under *Cryptography*, make sure that K-9 Mail knows to use APG. You can also find options here to make K-9 Mail automatically sign your messages and/or encrypt them if APG can find a public key for the recipient(s).
6. Try it out.

7.5.1 APG

This is a small tool which makes GPG encryption possible on the phone. You can use APG to manage your private and public keys. The options in the application are quite

7 Email Encryption

straightforward if you are a little knowledgeable of GPG in general.

Management of keys is not very well implemented yet. The best way is to manually copy all your public keys to the SD card in the APG folder. Then it's easy to import your keys. After you've imported your public and private keys, GPG encrypting, signing and decrypting will be available for other applications as long as these applications have integrated encryption/GPG.

7.5.2 GPG enabled e-mail on Android: K-9 Mail

The default mail application does not support GPG. Luckily there is an excellent alternative: K-9 Mail. This application is based on the original Android mail application but with some improvements. The application can use APG as its GPG provider. Setting up K-9 Mail is straightforward and similar to setting up mail in the Android default mail application. In the settings menu there is an option to enable "Cryptology" for GPG mail signing.

If you want to access your GPG mails on your phone this application is a must have.

Please note, due to some small bugs in K-9 Mail and/or APG, it's very advisable to disable HTML mail and use only Plain text. HTML mails are not encrypted nicely and are often not readable.

7.6 Creating your PGP keys

Enigmail comes with a nice wizard to help you create a public/private key pair (see the chapter introducing PGP for an explanation). You can start the wizard at any time within Thunderbird by selecting **OpenPGP > Setup Wizard** from the menu on top.

1. This is what the wizard looks like. Please read the text on every window carefully. It provides useful information and helps you setup PGP to your personal preferences. In the first screen, click on Next to start the configuration.
2. The wizard asks you whether you want to sign all your outgoing mail messages. Signing all your messages is a good choice. If you choose not to, you can still manually decide to sign a message when you are composing it. Click on the 'Next' button after you have made a decision.
3. On the following screen, the wizard asks you whether you want to encrypt *all* your outgoing mail messages. Unlike signing of mails, encryption requires the recipient to have PGP software installed. You should probably answer 'no' to this question, so that you will send normal (unencrypted) mail by default. After you have made your decision, click on the 'Next' button.

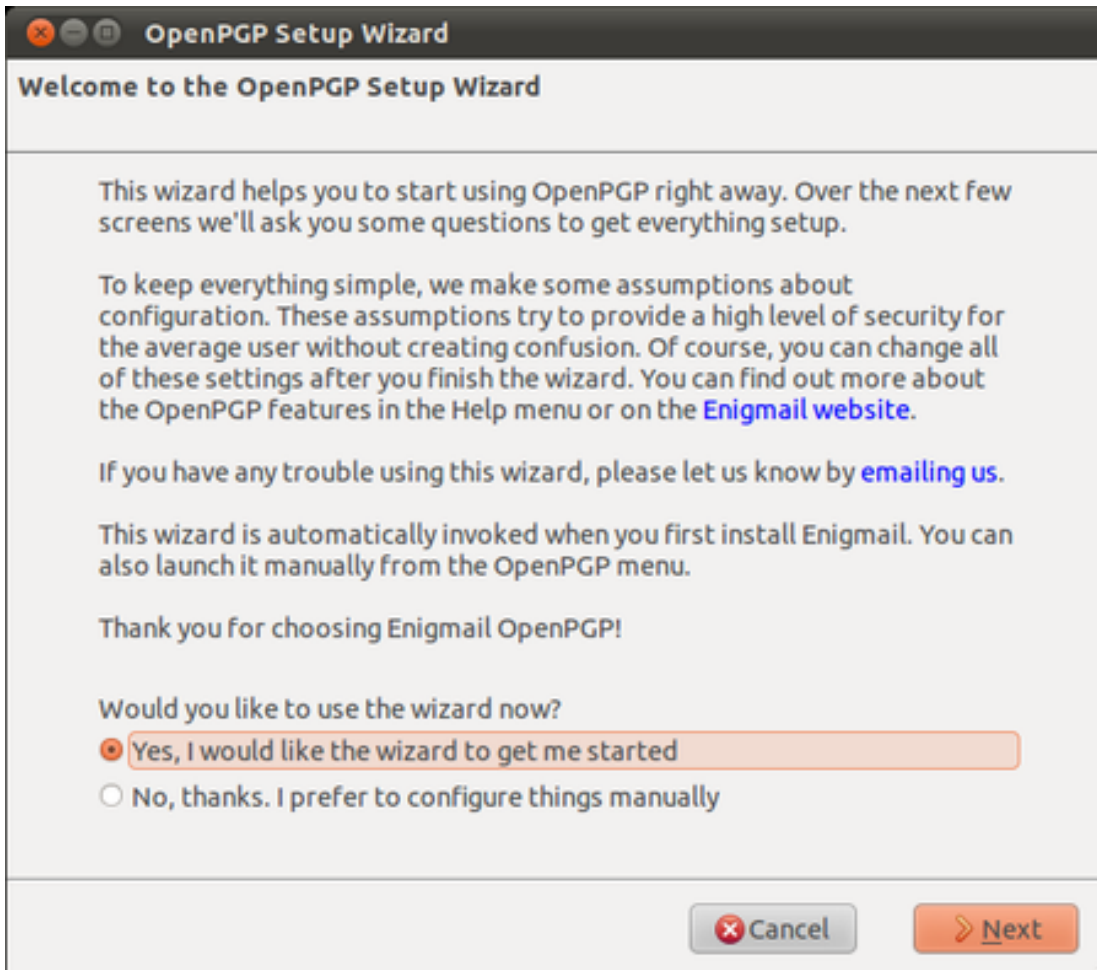


Figure 7.20: GPG Keys



Figure 7.21: GPG Keys



Figure 7.22: GPG Keys

7 Email Encryption

4. On the following screen the wizard asks if it can change some of your mail formatting settings to better work with PGP. It is a good choice to answer ‘Yes’ here. This will mean that by default, mail will be composed in plain text rather than HTML. Click on the ‘Next’ button after you have made your decision.

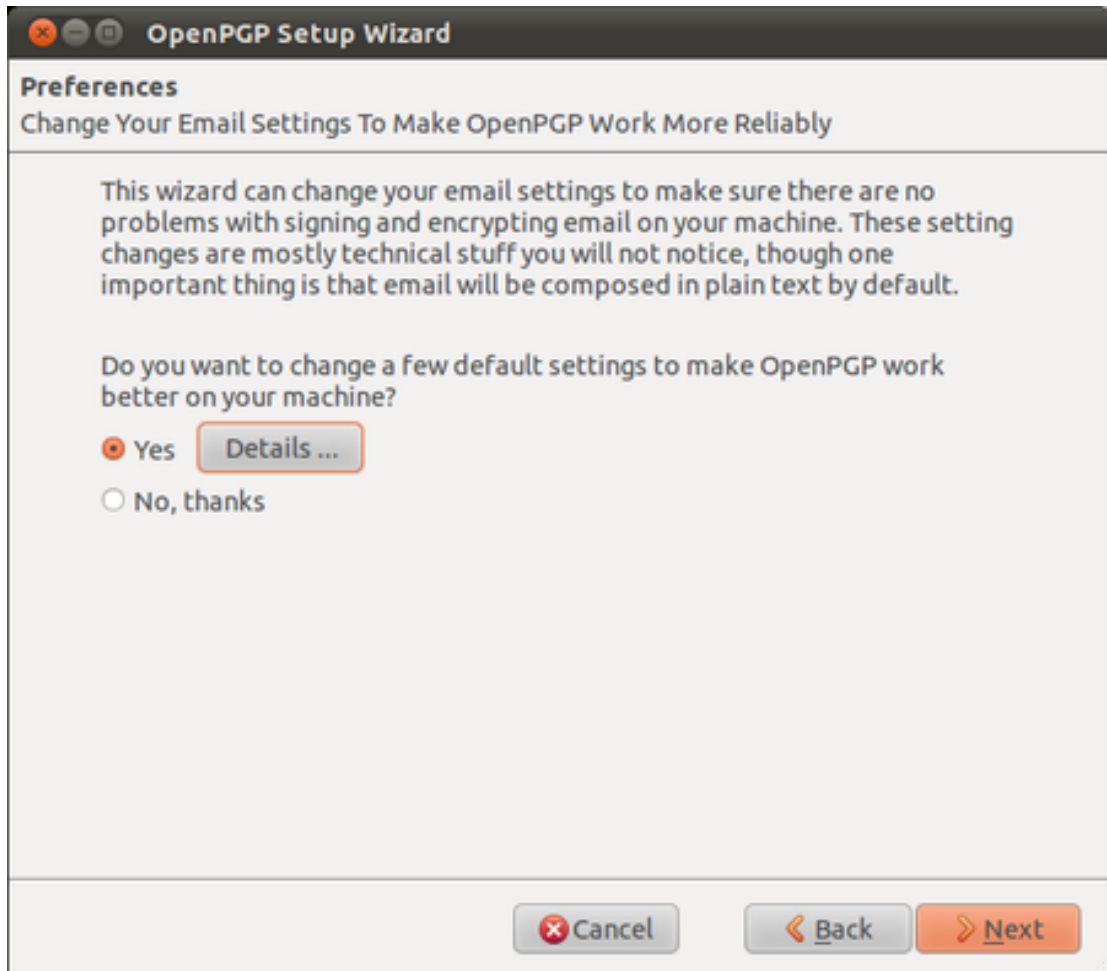


Figure 7.23: GPG Keys

5. In the following screen, select one of your mail accounts; the default is selected for you if you only have one. In the ‘Passphrase’ text box you must enter a password. This is a *new* password which is used to protect your private key. It is **very important** to remember this password, because you cannot read your own encrypted emails if you forget it. Make it a **strong** password, ideally 20 characters or longer. Please see the chapter on passwords for help on creating unique, long and easy to remember passwords. After you have selected your account and created a passphrase, click on the ‘Next’ button.



Figure 7.24: GPG Keys

7 Email Encryption

6. In the following screen the wizard summarizes the actions it will take to enable PGP encryption for your account. If you are satisfied, click the 'Next' button.

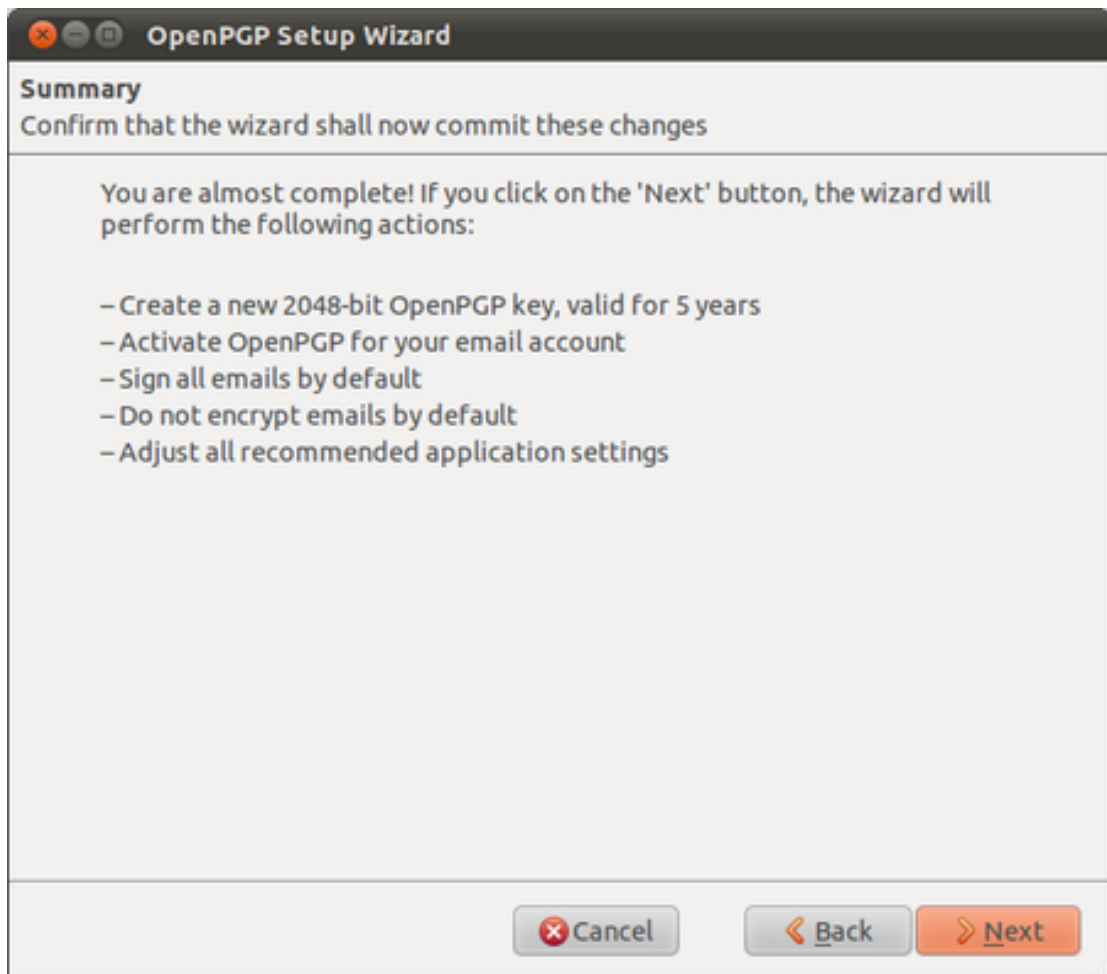


Figure 7.25: GPG Keys

7. Your keys will be created by the wizard, which will take some time. When completed, click on the 'Next' button.
8. You now have your own PGP key-pair. The wizard will ask you if you also want to create a 'Revocation certificate'. This is a file which can be used to inform everyone if your private key is compromised, for example if your laptop is stolen. Think of it as a 'kill switch' for your PGP identity. You may also wish to revoke the key simply because you have generated a new one, and the old one is obsolete.

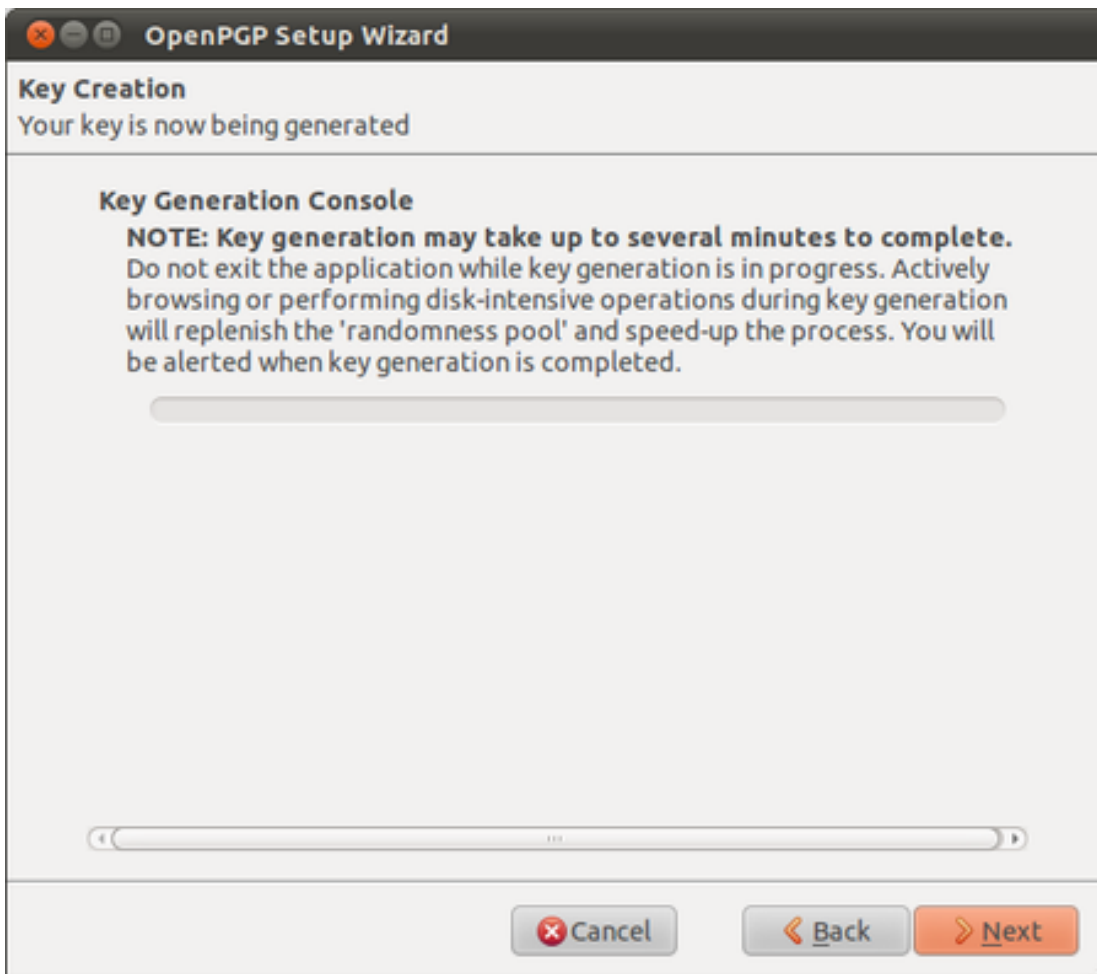


Figure 7.26: GPG Keys

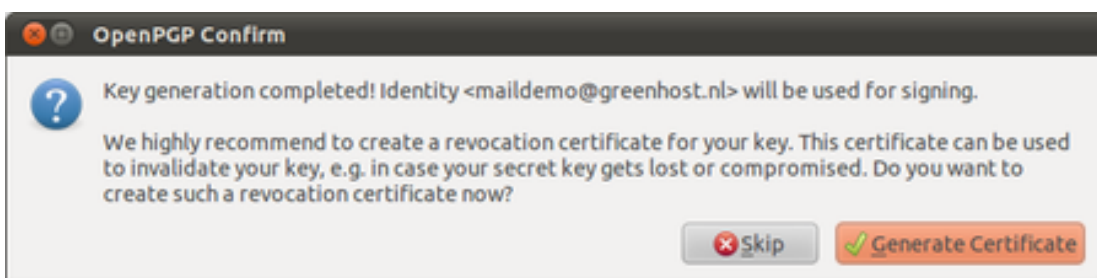


Figure 7.27: GPG Keys

7 Email Encryption

9. If you decided to generate a revocation certificate, the wizard will ask you where the file should be saved. The dialog will look different depending on which operating system you use. It is a good idea to rename the file to something sensible like `my_revocation_certificate`. Click on 'Save' when you you have decided on a location.

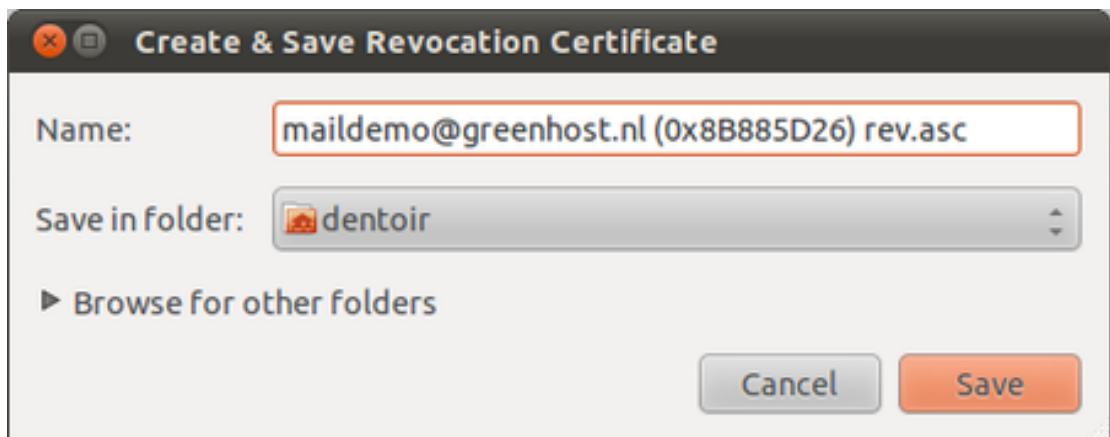


Figure 7.28: GPG Keys

10. If you decided to generate a revocation certificate, the wizard informs you it has been successfully stored. You may want to print it out or burn it to a CD and keep it in a safe place.

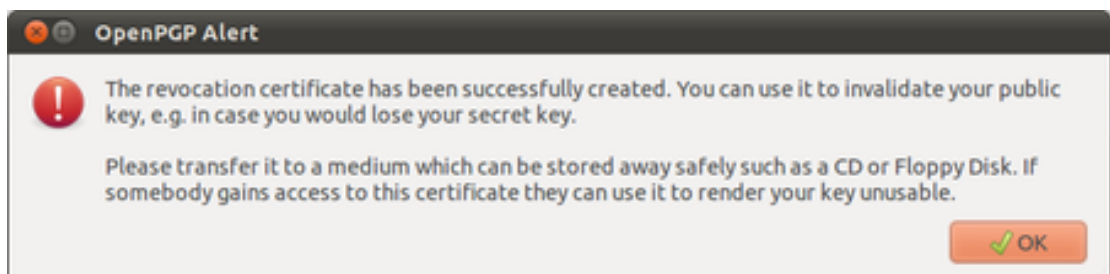


Figure 7.29: GPG Keys

11. The wizard will inform you it has completed.

Congratulations, you now have a fully PGP-configured mail client. In the next chapter we will explain how to manage your keys, sign messages and do encryption. Thunderbird can help you do a lot of these things automatically.

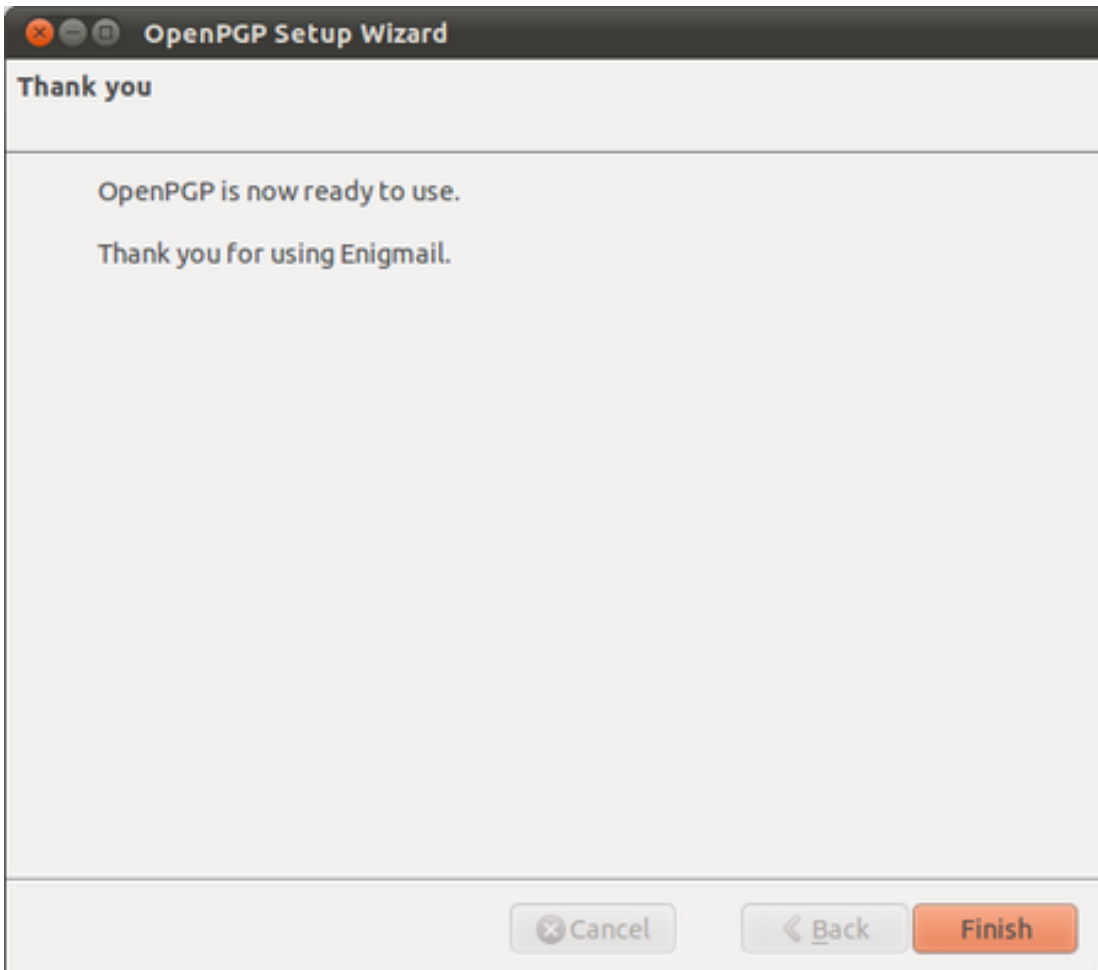


Figure 7.30: GPG Keys

7.7 Daily PGP usage

In the previous chapters we have explained how to set up a secure mail environment using Thunderbird, GPG and Enigmail. We assume you have installed the software and have successfully followed the wizard instructions to generate an encryption key-pair as described in the previous chapter. This chapter will describe how to use your secured Thunderbird in daily life to protect your e-mail communication. In particular we will focus on:

1. Encrypting attachments
2. Entering your pass-phrase
3. Receiving encrypted e-mail
4. Sending and receiving public keys
5. Receiving public keys and adding them to your key ring
6. Using public key servers
7. Signing e-mails to an individual
8. Sending encrypted e-mails to an individual
9. Automating encryption to certain recipients
10. Verifying incoming e-mails
11. Revoking your GPG key pair
12. What to do when you have lost your secret key, or forgot your passphrase
13. What to do when your secret key has been stolen, or compromised
14. Backing up your keys

First we shall explain two dialog windows that will inevitably appear after you start using Thunderbird to encrypt your emails.

7.7.1 Encrypting attachments

The dialog window below will pop-up whenever you are sending an encrypted email with attachments for the first time. Thunderbird asks a technical question on how to encrypt attachments to your mail. The second (default) option is the best choice, because it combines security with the highest compatibility. You should also select the ‘Use the selected method for all future attachments’ option. Then click ‘OK’ and your mail should be sent with no further delay.

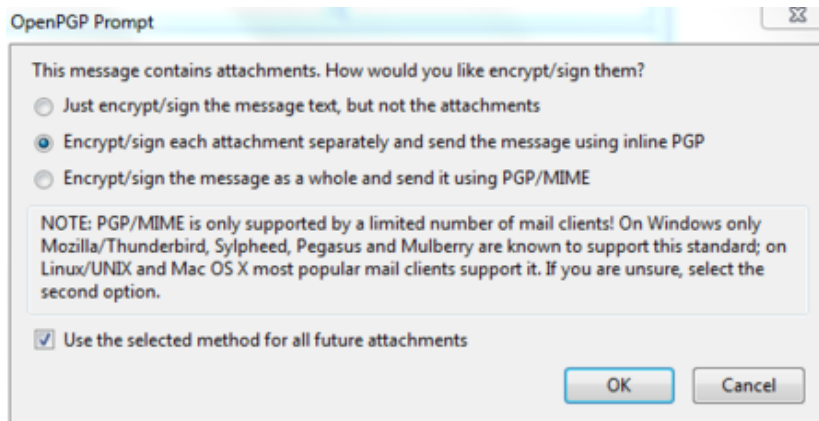


Figure 7.31: Daily GPG Usage

7.7.2 Entering your pass-phrase

For security reasons, the pass-phrase to your secret key is stored temporarily in memory. Every now and then the dialog window below will pop-up. Thunderbird asks you for the pass-phrase to your secret key. This should be different from your normal email password. It was the pass-phrase you have entered when creating your key-pair in the previous chapter. Enter the pass-phrase in the text-box and click on 'OK'

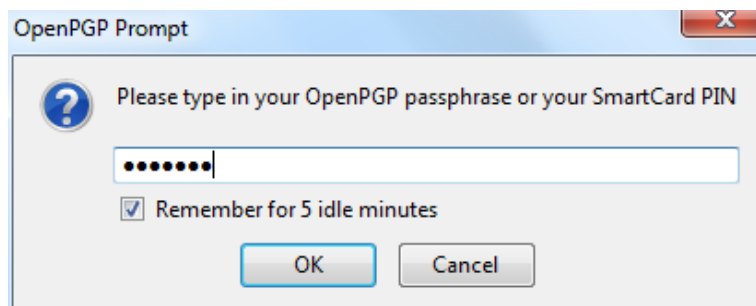


Figure 7.32: Daily GPG Usage

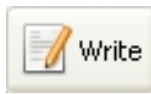
7.7.3 Receiving encrypted e-mails


The decryption of e-mails is handled automatically by Enigmail, the only action that may be needed on your behalf is to enter the pass-phrase to your secret key. However, in order to have any kind of encrypted correspondence with somebody, you will first need to exchange public keys.

7.7.4 Sending and receiving public keys


There are multiple ways to distribute your public key to friends or colleagues. By far the simplest way is to attach the key to a mail. In order for your friend to be able to trust that the message actually came from you, you should inform them in person (if possible) and also require them to reply to your mail. This should at least prevent easy forgeries. You have to decide for yourself what level of validation is necessary. This is also true when receiving emails from third-parties containing public keys. Contact your correspondent through some means of communication other than e-mail. You can use a telephone, text messages, Voice over Internet Protocol (VoIP) or any other method, but you must be absolutely certain that you are really talking to the right person. As a result, telephone conversations and face-to-face meetings work best, if they are convenient and if they can be arranged safely.

Sending your public key is easy.



1. In Thunderbird, click on the  icon.
2. Compose a mail to your friend or colleague and tell them you are sending them your PGP public key. If your friend does not know what that means, you may have to explain them and point them to this documentation.
3. Before actually sending the mail, click to **OpenPGP > Attach My Public Key** option on the menu bar of the mail compose window. Next to this option a marked sign will appear. See the example below.



4. Send your mail by clicking on the  button.

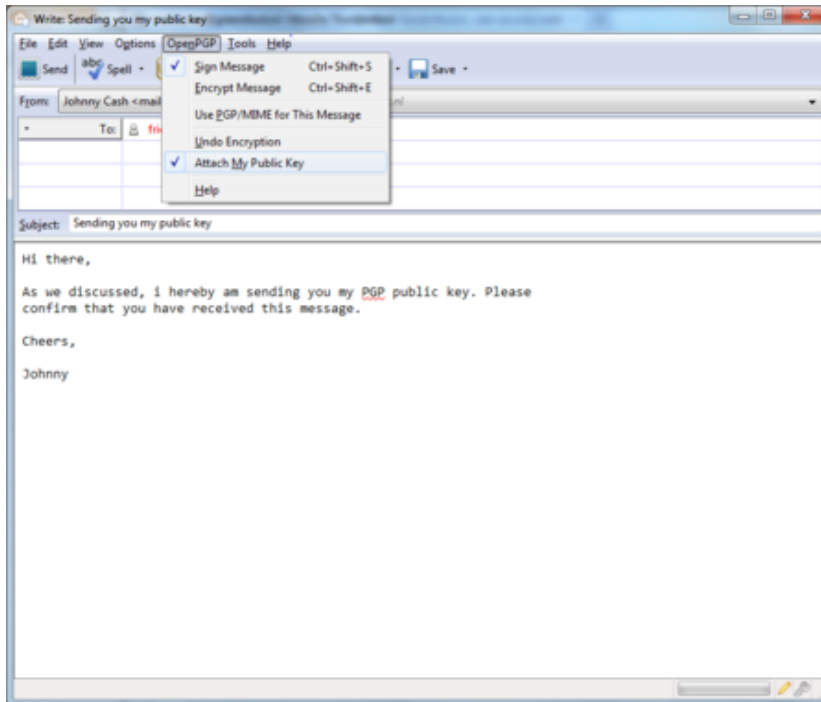


Figure 7.33: Daily GPG Usage

7.7.5 Receiving public keys and adding them to your keyring

Lets say we receive a public key from a friend by mail. The key will show up in Thunderbird as an *attached file*. Scroll down the message and below you will find tabs with one or two file names. The extension of this public key file will be `.asc`, different from the extension of an attached GPG signature, which ends with `.asc.sig`

Look at the example email in the next image, which is a received, signed GPG message containing an attached public key. We notice a yellow bar with a warning message: 'OpenPGP: Unverified signature, click on 'Details' button for more information'. Thunderbird warns us that the sender is not known yet, which is correct. This will change once we have accepted the public key.

What are all those strange characters doing in the mail message? Because Thunderbird does not yet recognize the signature as valid, it prints out the entire raw signature, just as it has received it. This is how digitally signed GPG messages will appear to those recipients who do not have your public key.

The most important thing in this example is to find the attached GPG public key. We mentioned it is a file that ends with `.asc`. In this example it's the first attachment on the left, in the red circle. Double-clicking on this attachment will make Thunderbird recognize the key.

After we have clicked on the attachment, the following pop-up will appear.

Thunderbird has recognized the GPG public key file. Click on 'Import' to add this key

7 Email Encryption

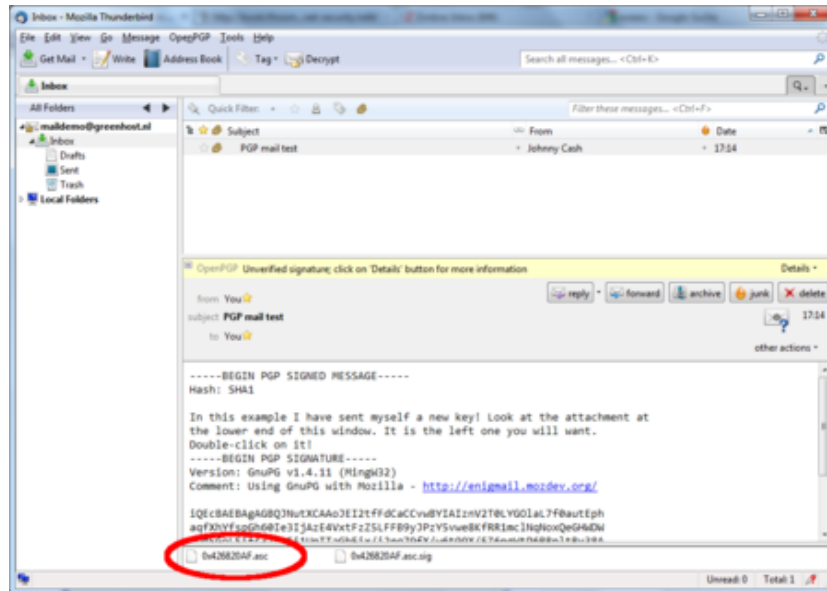


Figure 7.34: Daily GPG Usage

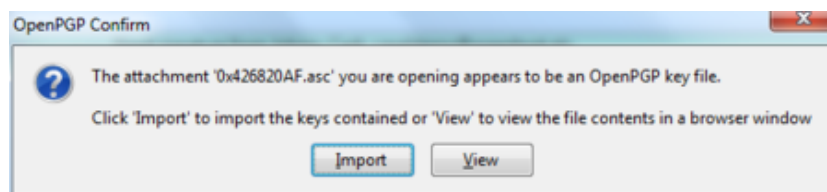


Figure 7.35: Daily GPG Usage

to your keyring. The following pop-up should appear. Thunderbird says the operation was successful. Click on ‘OK’ and you are almost done.

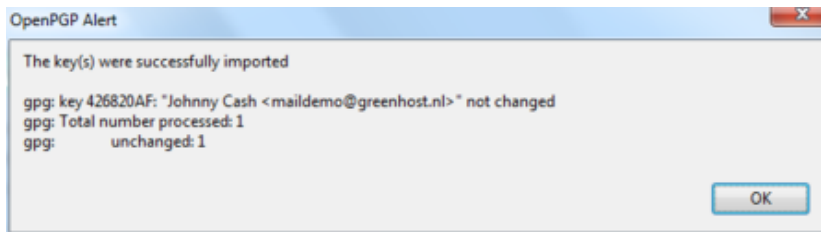


Figure 7.36: Daily GPG Usage

We are back in the main Thunderbird screen and we refresh the view on this particular example message, by clicking on some other message and back for example. Now the body of the message looks different (see below). This time Thunderbird *does* recognize the signature, because we have added the public key of the sender.

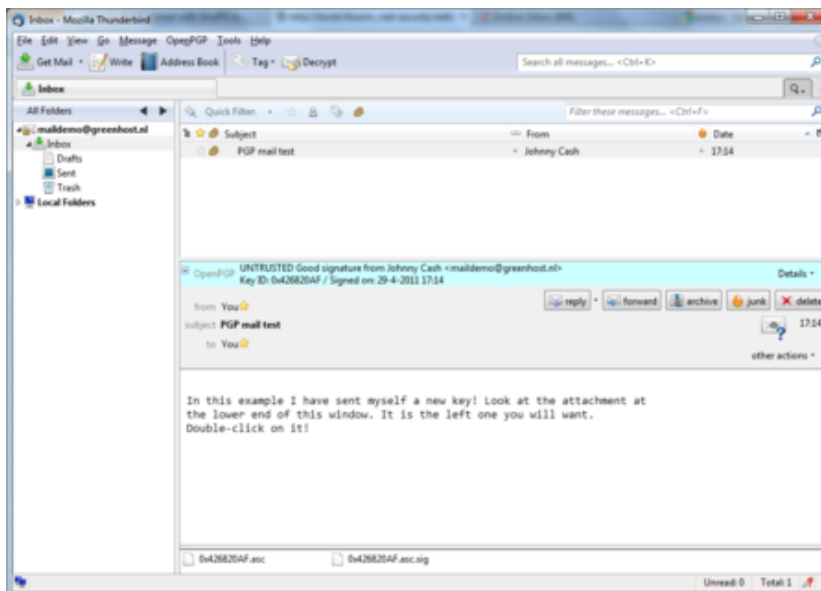


Figure 7.37: Daily GPG Usage

There is still one thing that remains. While Thunderbird now recognizes the signature, we should explicitly trust that the public key really belongs to the sender in real life. We realize this when we take a closer look at the green bar (see below). While the signature is good, it is still UNTRUSTED.

We will now decide to trust this particular public key and the signatures made by it. We can do this immediately by clicking on ‘Details’. A small menu will appear (see below). From this menu we should click on the option ‘Sign Sender’s Key ...’.

After we have selected ‘Sign Sender’s Key ...’ we will get another selection window

7 Email Encryption



Figure 7.38: Daily GPG Usage

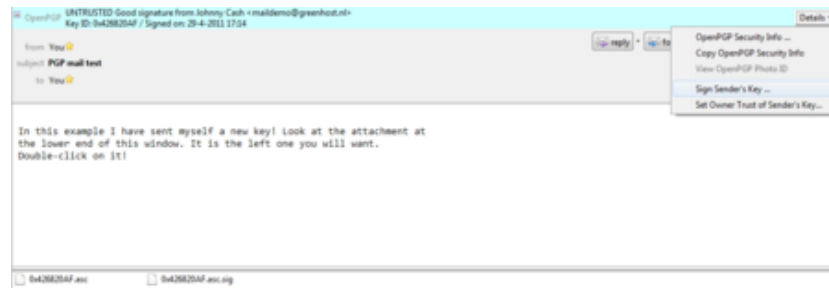


Figure 7.39: Daily GPG Usage

(see below). We are requested to state how carefully we have checked this key for validity. The explanation of levels of trust and trust networks in GPG falls outside the scope of this document. We will not use this information, therefore we will just select the option 'I will not answer'. Also select the option 'Local signature (cannot be exported)'. Click on the 'OK' button to finishing signing this key. This finishes accepting the public key. You can now send encrypted mail to this individual.

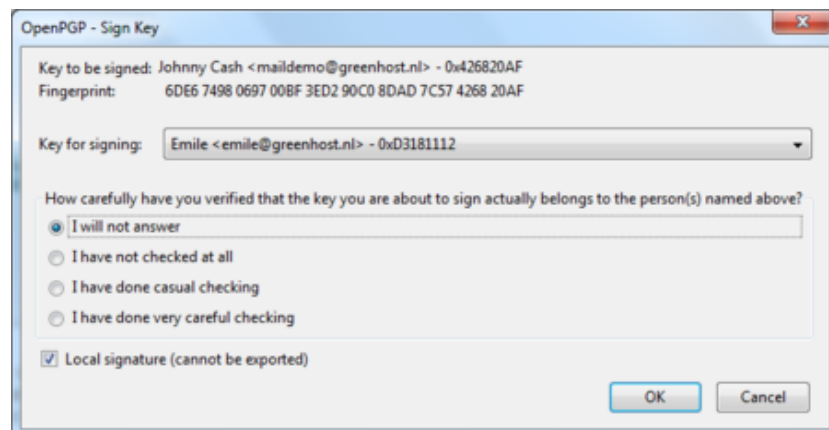


Figure 7.40: Daily GPG Usage

7.7.6 Using public key servers

Another method of distributing public keys is by putting them on a public key server. This allows anyone to check whether your email address has GPG support, and then download your public key.

To put your own key on a keyservers, take the following steps.

1. Head to the key manager by using the Thunderbird menu and click on OpenPGP > Key Management

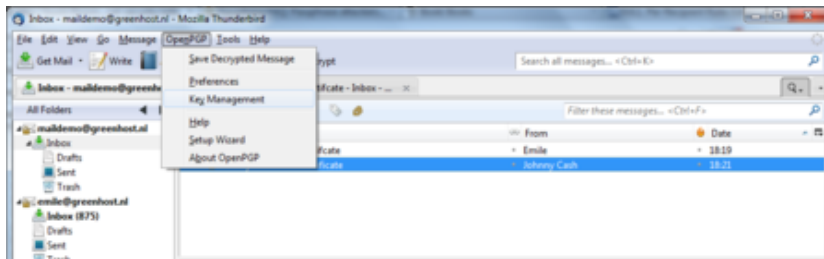


Figure 7.41: Daily GPG Usage

2. The key management window will be displayed and looks like this:

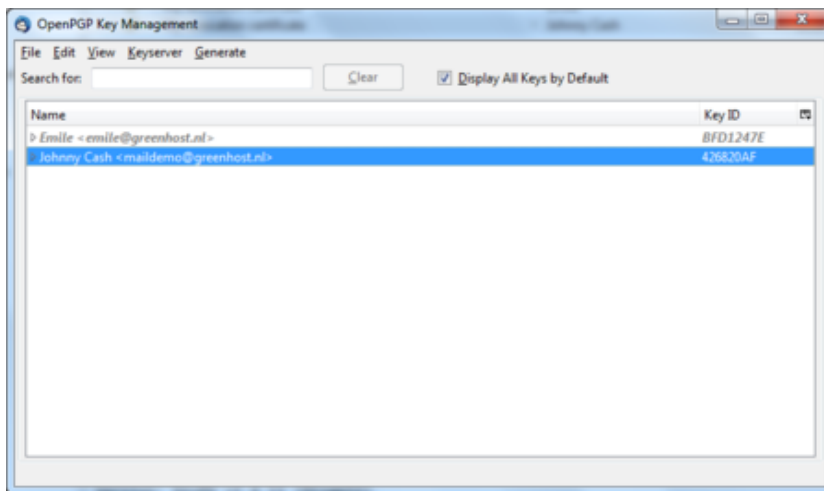


Figure 7.42: Daily GPG Usage

3. You need to have selected the 'Display All Keys by Default' option to get a list of all your keys. Look up your own email address in the list and right click on the address. A selection window will appear with some options. Select the option 'Upload Public Keys to Keyserver'.
4. You will see a small dialog window like below. The default server to distribute your keys to is good. Press 'OK' and distribute your public key to the world.

To look up whether some email address has a public key available on a server, take the following steps.

7 Email Encryption

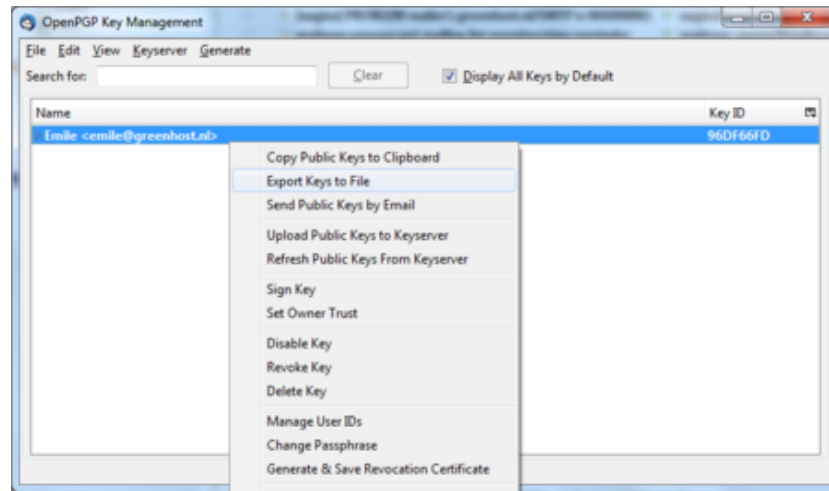


Figure 7.43: Daily GPG Usage

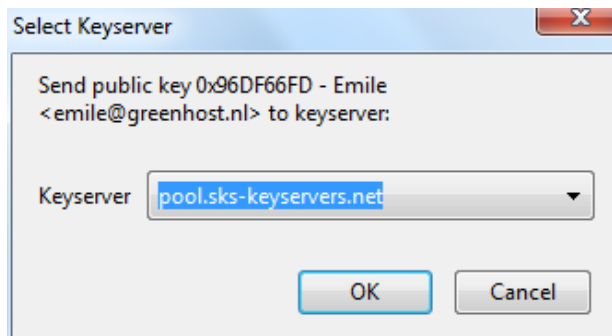


Figure 7.44: Daily GPG Usage

1. Head to the key manager by using the Thunderbird menu and click on OpenPGP > Key Management
2. In the key manager window menu bar, select Keyserver > Search for Keys

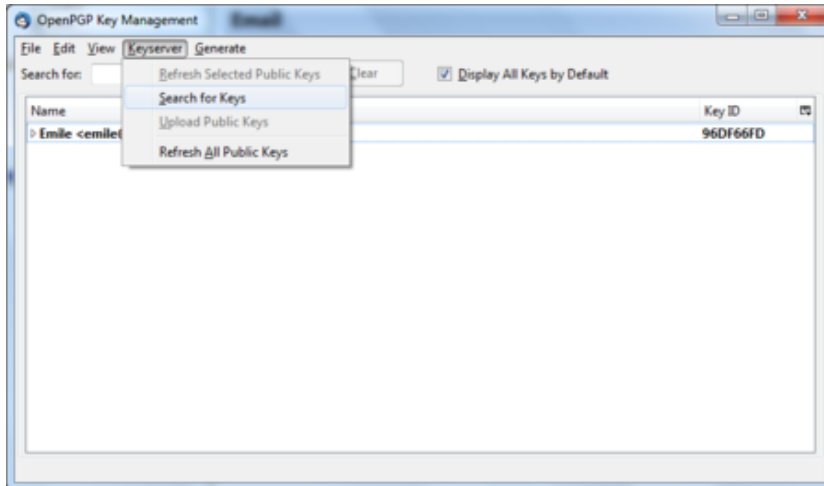


Figure 7.45: Daily GPG Usage

3. In this example we will look-up up the key for the creator of PGP software, Philip Zimmermann. After we have entered the email address, we click on 'OK'.

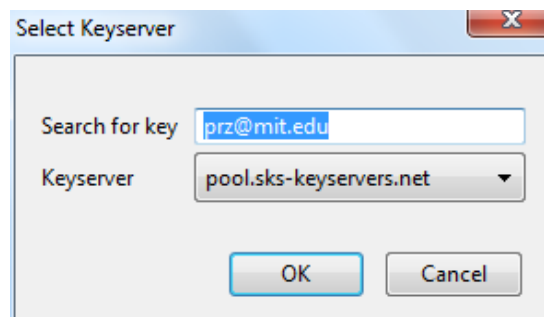


Figure 7.46: Daily GPG Usage

4. The next window displays the result of our search. We have found the public key. It is automatically selected. Just click on 'OK' to import the key.
5. Importing the key will take some time. On completion you should see a pop-up window like below.

7 Email Encryption

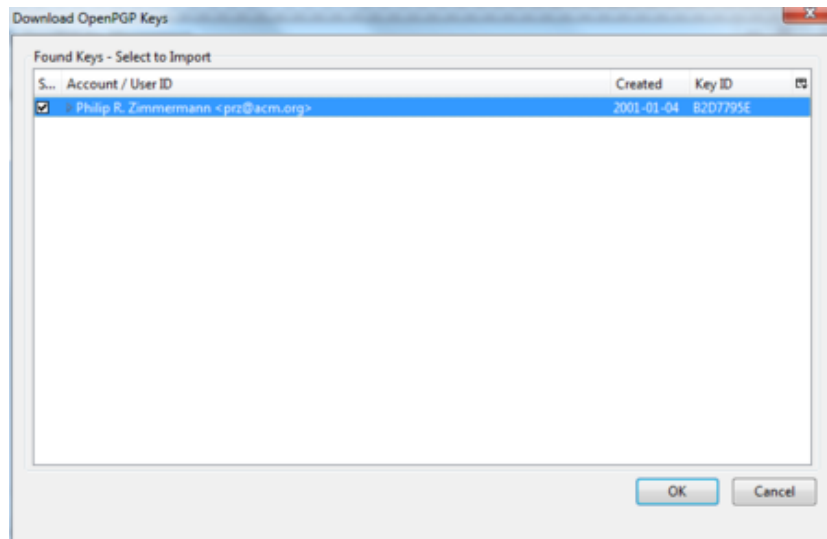


Figure 7.47: Daily GPG Usage

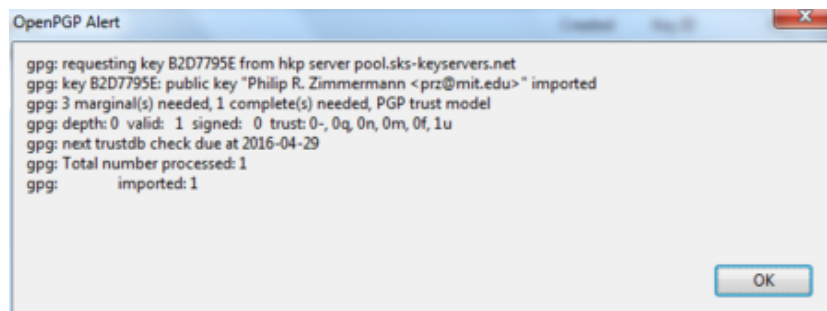


Figure 7.48: Daily GPG Usage

- The final step is to locally sign this key, to indicate that we trust it. When you are back in the key manager, make sure you have selected the ‘Display All Keys by Default’ option. You should now see the newly imported key in the list. Right-click on the address and select the option ‘Sign Key’ from the list.

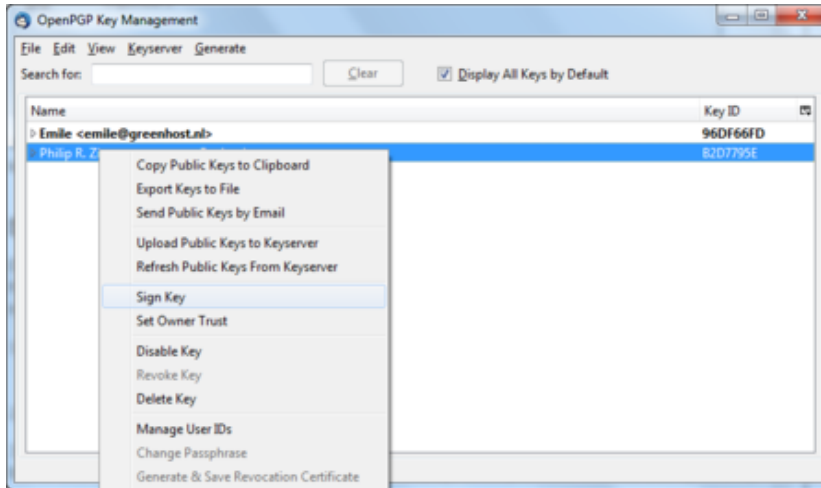


Figure 7.49: Daily GPG Usage

- Select the options ‘I will not answer’ and ‘Local signature (cannot be exported)’, then click on ‘OK’. You are now finished and can send Philip Zimmermann encrypted mail.

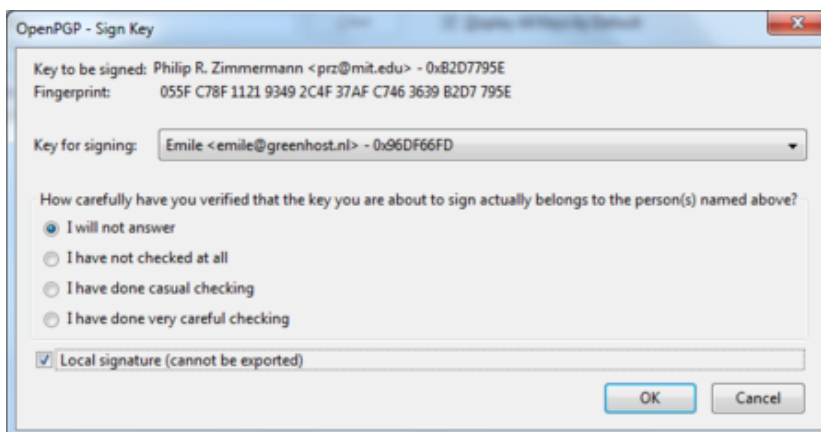


Figure 7.50: Daily GPG Usage


7 Email Encryption

7.7.7 Signing emails to an individual

Digitally signing email messages is a way to prove to recipients that you are the actual sender of a mail message. Those recipients who have received your public key will be able to *verify* that your message is authentic. However, take note that signing an email will make it very hard (if not impossible) to deny that you are the author of the message.

1. Offer your friend your public key, using the method described earlier in this chapter.



2. In Thunderbird, click on the  icon.
3. Before actually sending the mail, enable the **OpenPGP > Sign Message** option via the menu bar of the mail compose window, if it is not enable already. Once you have enabled this option, by clicking on it, a marked sign will appear. Clicking again should disable encryption again. See the example below.

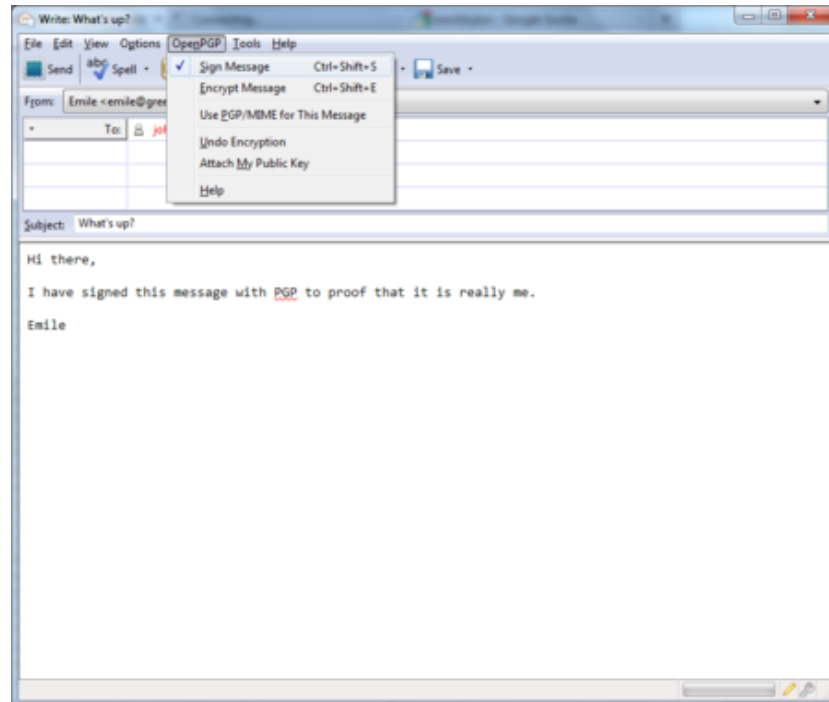



Figure 7.51: Daily GPG Usage




4. Click on the  button and your signed mail will be sent.

7.7.8 Sending encrypted mails to an individual

1. You should have received the public key from the friend or colleague you want to email and you should have accepted their public key, using the method describe earlier in this chapter.



2. In Thunderbird, click on the  icon.
3. Compose a mail to the friend or colleague, from who you have previously received their public key. **Remember the subject line of the message will not be encrypted**, only the message body itself, and any attachments.
4. Before actually sending the mail, enable the `OpenPGP > Encrypt Message` option via the menu bar of the mail compose window, if it is not enabled already. Once you have enabled this option, by clicking on it, a marked sign will appear. Clicking again should disable encryption again. See the example below.

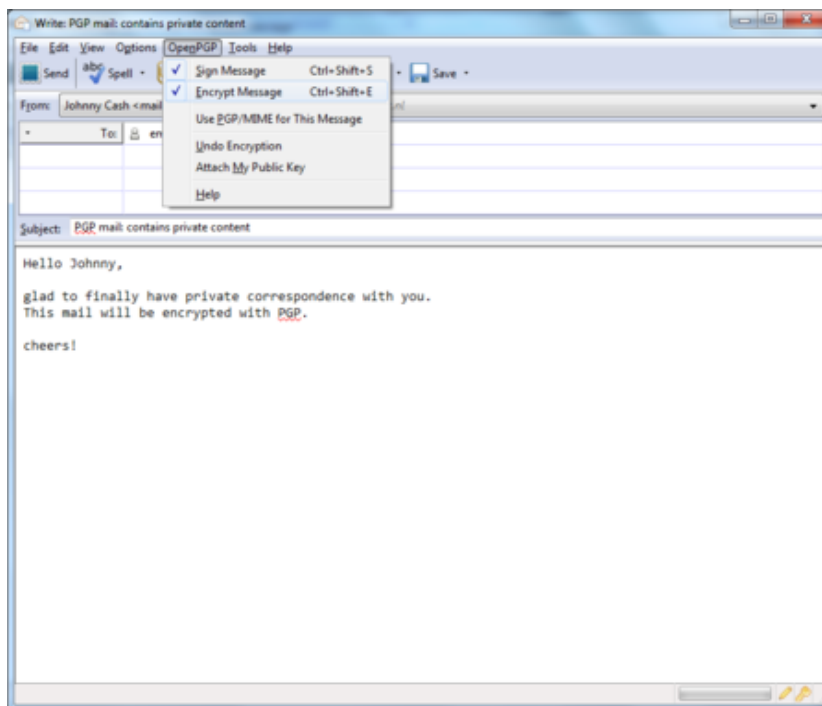



Figure 7.52: Daily GPG Usage



5. Click on the  button and your encrypted mail will be sent.

7.7.9 Automating encryption to certain recipients

You will often want to make sure all your messages to a certain colleague or friend are signed and encrypted. This is good practice, because you may forget to enable the encryption manually. You can do this by editing the per-recipient rules. To do this we access the OpenPGP per-recipient rule editor.

Select **OpenPGP > Preferences** from the Thunderbird menu bar.

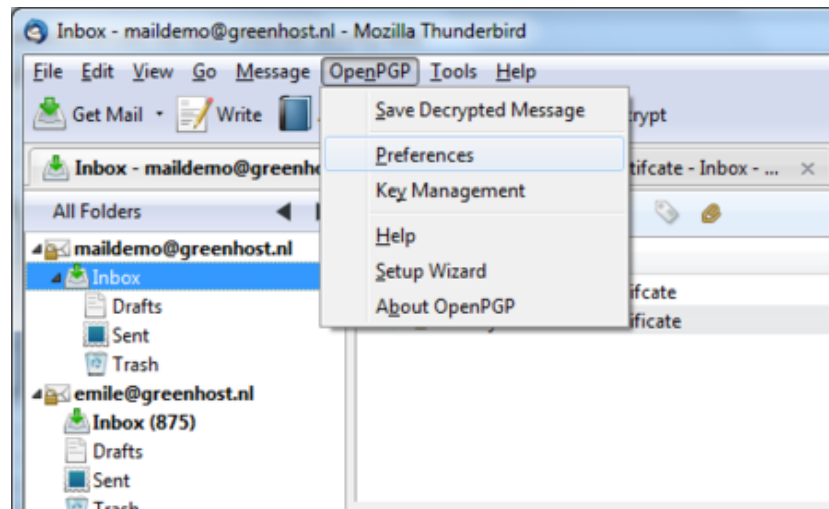


Figure 7.53: Daily GPG Usage

The preferences window will appear like below. We need to click on ‘Display Expert Settings’.

New menu tabs will appear in the window. Go to the tab ‘Key Selection’ and then click on the button labeled ‘Edit Rules ...’

We are now shown the per-recipient rules editor (see below). This editor can be used to specify the way how messages to certain recipients are sent. We will now add a rule saying we want to encrypt and sign all mail messages to `maildemo@greenhost.nl`

First click on the ‘Add’ button.

Now the window to add a new rule will be shown.

The first thing we should enter is the email address of the recipient. In the example below we have entered `maildemo@greenhost.nl`

Now we will set the encryption defaults by using the drop-downs below. For Signing select ‘Always’. For Encryption also select ‘Always’.

Finally we have to select the *public key* of the recipient, with which to encrypt our messages. Do not forget this important step, otherwise the e-mail will not be encrypted. Click on the button labeled ‘Select Key(s)...’. The key selection window will show up. The most obvious key will be selected by default. In the example below, we only have one public key available. We can select keys by clicking on the small box next to the address. Then we click ‘OK’ and close all relevant windows and we are finished.

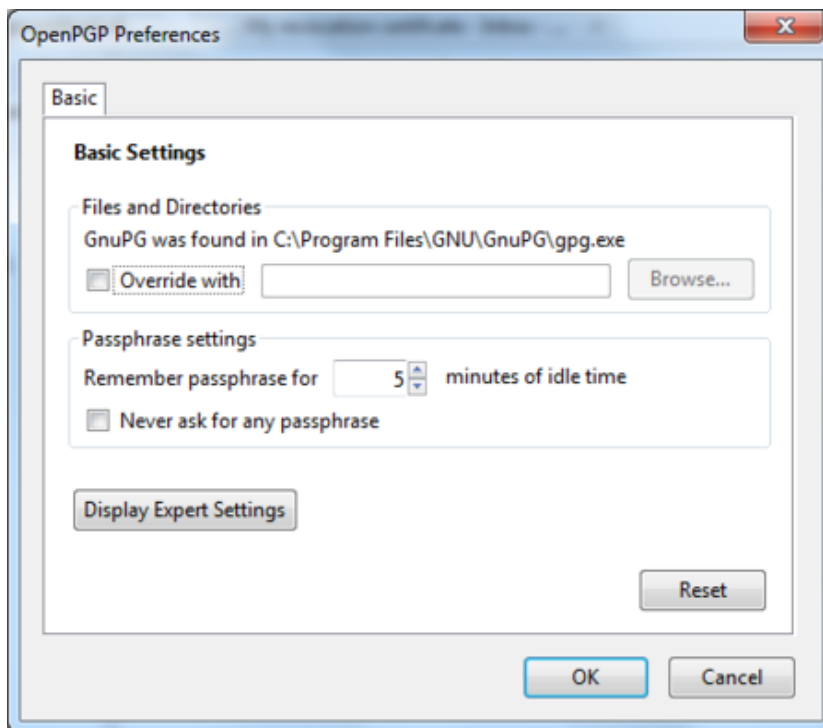


Figure 7.54: Daily GPG Usage

7 Email Encryption

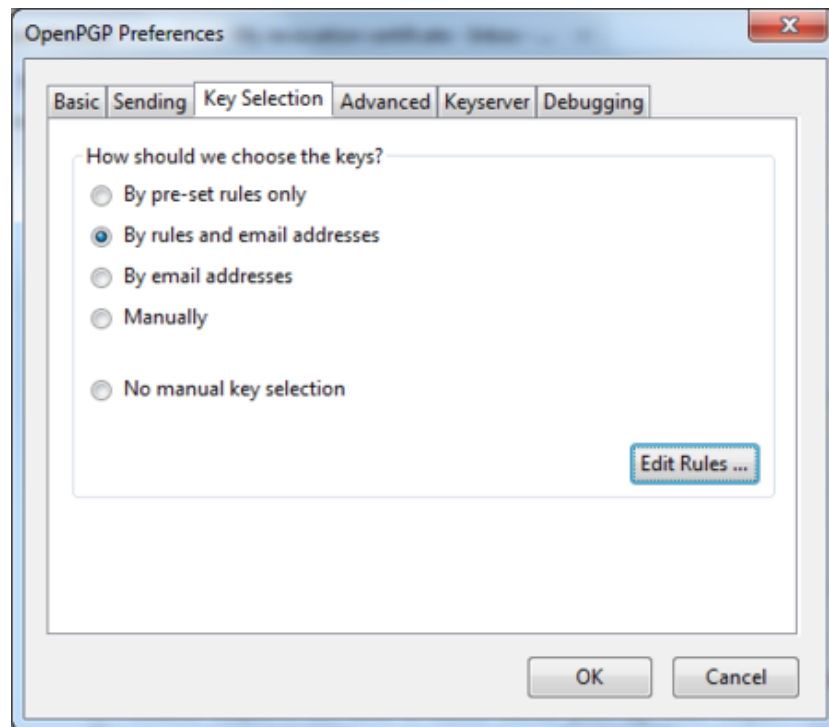


Figure 7.55: Daily GPG Usage

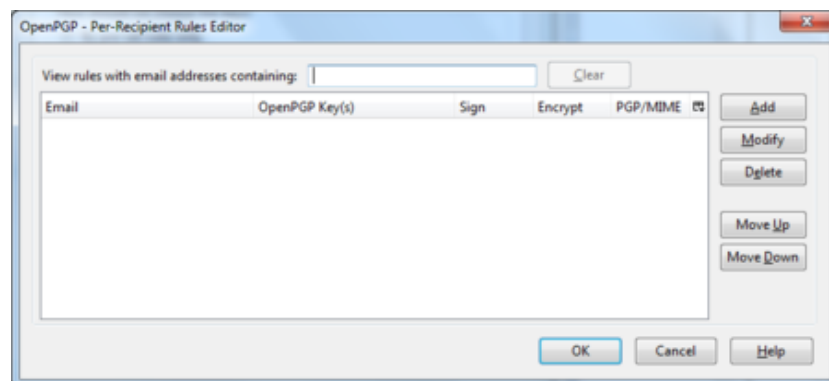


Figure 7.56: Daily GPG Usage

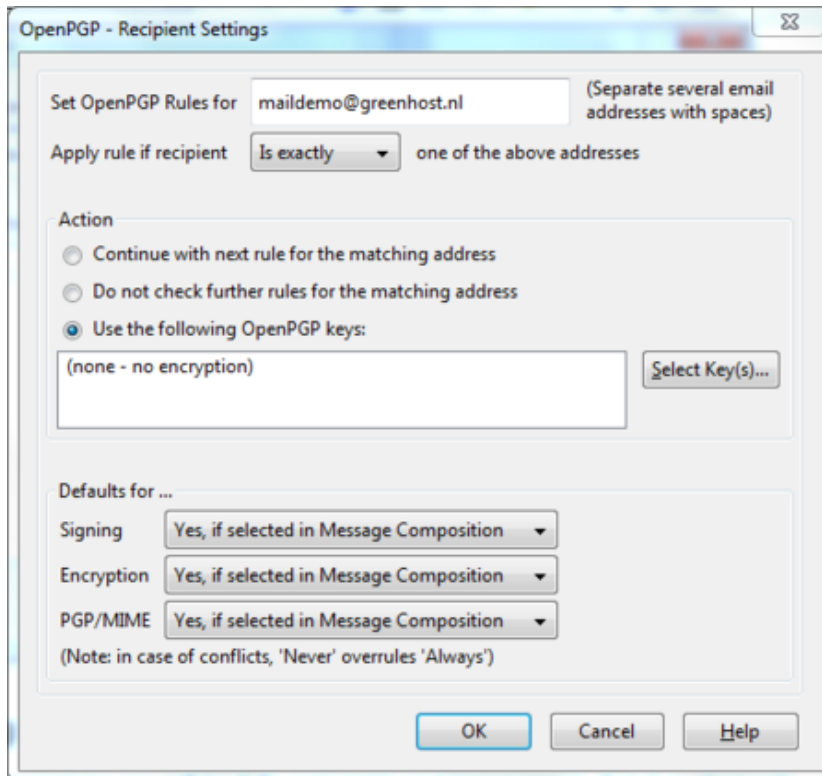


Figure 7.57: Daily GPG Usage

7 Email Encryption

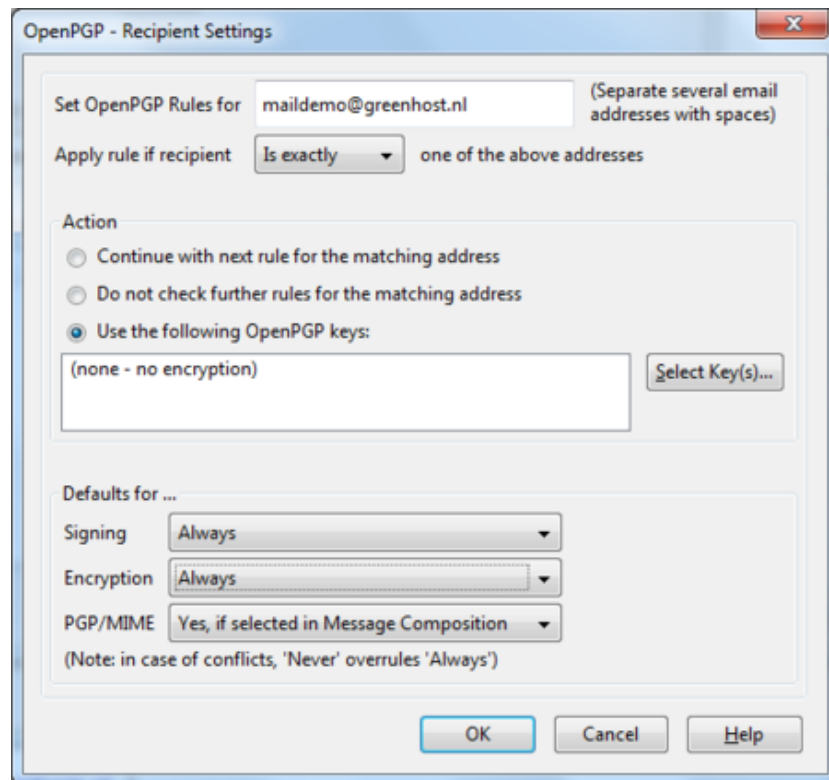


Figure 7.58: Daily GPG Usage

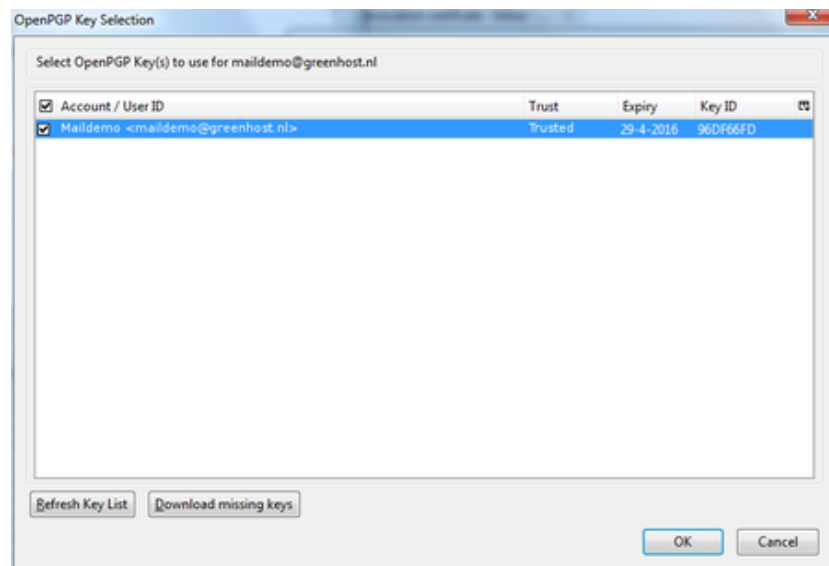


Figure 7.59: Daily GPG Usage

7.7.10 Verifying incoming e-mails

Decrypting email messages sent to you will be fully automatic and transparent. But it is obviously important to see whether or not a message to you has in fact been encrypted or signed. This information is available by looking at the special bar above the message body.

A valid signature will be recognized by a green bar above the mail message like the example image below.

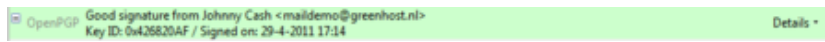


Figure 7.60: Daily GPG Usage

The last example message was signed but not encrypted. If the message had been encrypted, it would show like this:

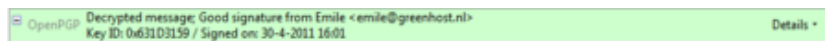


Figure 7.61: Daily GPG Usage

When a message which has been encrypted, but not signed, it could have been a forgery by someone. The status bar will become gray like in the image below and tells you that while the message was sent securely (encrypted), the sender could have been someone else than the person behind the email address you will see in the 'From' header. The signature is necessary to verify the real sender of the message. Of course it is perfectly possible that you have published your public key on the Internet and you allow people to send you emails anonymously. But is it also possible that someone is trying to impersonate one of your friends.

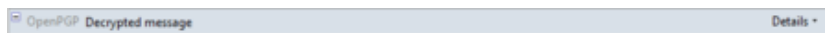


Figure 7.62: Daily GPG Usage

Similarly if you receive a signed email from somebody you know, and you have this person's public key, but still the status bar becomes yellow and displays a warning message, it is likely that someone is attempting to send you forged emails!

Sometimes secret keys get stolen or lost. The owner of the key will inform his friends and send them a so-called revocation certificate (more explanation of this in the next paragraph). Revocation means that we no longer trust the old key. The thief may afterwards still try his luck and send you a falsely signed mail message. The status bar will now look like this:

Strangely enough Thunderbird in this situation will still display a green status bar! It is important to look at the contents of the status bar in order to understand the encryption aspects of a message. GPG allows for strong security and privacy, but only if you are familiar with its use and concepts. Pay attention to warnings in the status bar.

7 Email Encryption



Figure 7.63: Daily GPG Usage



Figure 7.64: Daily GPG Usage

7.7.11 Revoking your GPG key-pair

Your secret key has been stolen by somebody. Your harddisk crashed and you have lost all your data. If your key is lost, you can no longer decrypt messages. If your key has been stolen, somebody else can decrypt your communication. You need to make a new set of keys. The process of creating keys, using the OpenPGP wizard in Thunderbird, has been described in this manual. But first you want to tell the world that your old public key is now worthless, or even dangerous to use.

7.7.12 What to do when you have lost your secret key, or forgot your passphrase

During the creation of your key-pair, the OpenPGP wizard offered you the possibility to create a so-called revocation certificate. This is a special file you send to others in the advent you have to disable your key. If you have a copy of this file, sending the revocation key is simply sending the file as an attachment to all your friends. You can no longer send signed mails (obviously, because you have lost your secret key). That doesn't matter. Send it as a normal mail. The revocation certificate file could only have been created by the owner of the secret key and proves he or she wants to revoke it. That's why it should normally be kept hidden from others.

If you do not have the revocation certificate, there exists no other option than for you to contact your friends personally and convince them your key is lost and that they should no longer trust it.

7.7.13 What to do when your secret key has been stolen, or compromised

If you have reason to believe your secret key has been compromised, or worse your secret key and passphrase, it is very important to contact others that they should stop sending you encrypted messages. With your secret key, other persons will be able to break the encryption of your e-mail messages if they also have your passphrase. This is also true for those messages you have send in the past. Cracking the passphrase is not trivial, but it may be possible if the party has lots of resources, like a state or a big organization for example, or if your passphrase is too weak. In any case you should assume the worst and assume your passphrase may have been compromised. Send a revocation certificate file to all your friends or contact them personally and inform them of the situation.

Even after you have revoked your old key pair, the stolen key may still be used to

decrypt your previous correspondence. You should consider other ways to protect that old correspondence, for instance by re-encrypting it with a new key. The latter operation will not be discussed in this manual. If you are uncertain you should seek assistance from experts or look up more information on the web.

7.7.14 Receiving a revocation certificate

If one of your friends sends you a revocation certificate, s/he asks you to distrust his public key from now on. You should always accept such a request and ‘import’ the certificate to disable their key. The process of accepting a revocation certificate is exactly the same as accepting a public key, as has already been described in the chapter. Thunderbird will ask you if you want to import the ‘OpenPGP key file’. Once you have done so, a confirmation pop-up should be displayed like below.

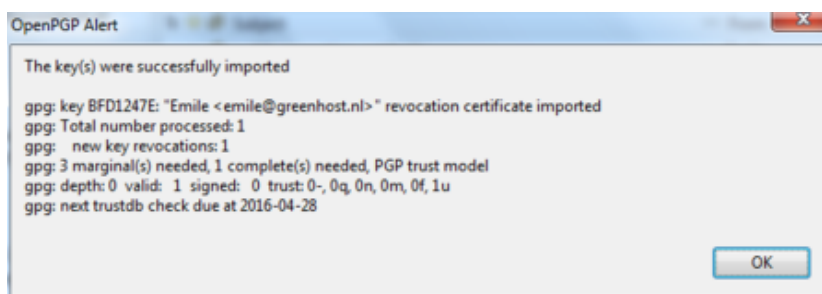


Figure 7.65: Daily GPG Usage

7.7.15 Preparing for the worst: backup your keys

Your keys are usually stored on your hard disk as normal files. They may get lost if your computer gets damaged. It is strongly advised to keep a backup of your keys in a safe place, like a vault. Making a backup of your secret key has another security advantage as well. Whenever you fear your laptop or computer is in immediate danger of being confiscated, you can safely delete your key-pair. Your email will be rendered unreadable immediately. At a later stage, you can retrieve your keys from the vault and re-import them in Thunderbird.

To make a backup of your key-pair, first head to the key manager by using the Thunderbird menu and click on **OpenPGP > Key Management**.

You need to have selected the ‘Display All Keys by Default’ option to get a list of all your keys. Lookup your own email address in the list and right click on the address. A selection window will appear with some options. Select the option ‘Export Keys to File’.

Now we will save the key-pair to a file. Thunderbird asks us if we want to include the secret key as well. We do want to include the secret key, therefore we select ‘Export Secret Keys’.

Finally Thunderbird asks us for the location of the key file. You can store the file anywhere you like, network disk, USB-stick. Just remember to hide it away from other

7 Email Encryption

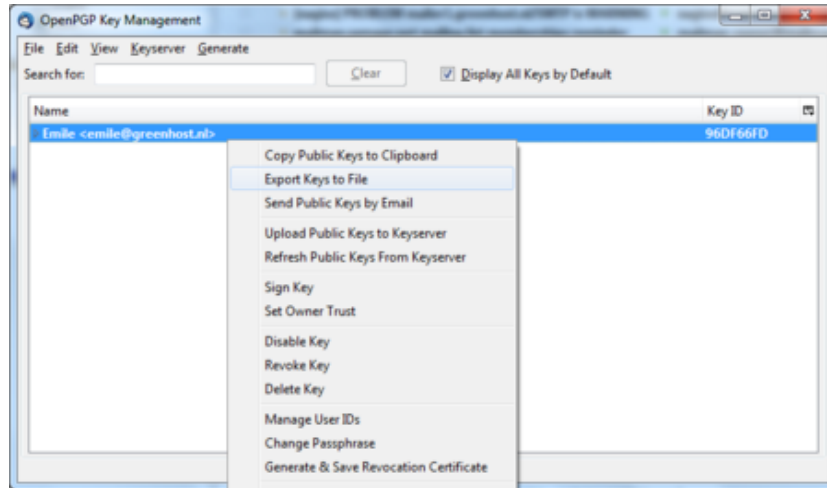


Figure 7.66: Daily GPG Usage

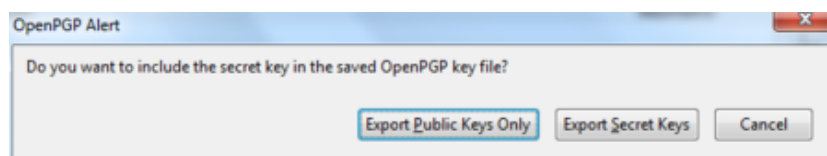


Figure 7.67: Daily GPG Usage

people.

7.7.16 Further reading

More documentation on using GPG with Thunderbird can be found on the website of the Enigmail plugin. The Enigmail handbook is the guide you will want to use.

<http://enigmail.mozdev.org/documentation/handbook.php.html>

7.8 Webmail and PGP

The only safe way of encrypting email inside of the browser window is to encrypt it outside and then copy & paste the encrypted text into the browser window.

For example, write the text in a text editor like gedit, vim or kate and save it as .txt file (in this example “message.txt”). Then type

```
gpg -ase -r <recipients email/gpg id> -r <your gpg id> message.txt
```

A new file called “message.asc” will be created. It contains the encrypted message and can thus be either attached to an email or its content safely copy & pasted into the browser window.

To decrypt a message from the browser window, simply type `gpg` into the command line and hit Enter. Then copy & paste the message to be decrypted into the commandline window and after being asked for your passphrase hit Ctrl+D (this enters a end-of-file character and prompts gpg to output the cleartext message).

If using the commandline seems too cumbersome to you, you might consider installing a helper application like `gpgApplet`, `kgpg` or whatever application ships with your operating system.

8 Safer Browsing

8.1 Why Firefox?

Firefox is open source software, developed by the non-profit organisation, the Mozilla Foundation. As such, it is independent from the interests of any one specific company although a large portion of its funding comes from Google for its placement as the default search engine within the Firefox browser. It is also highly extensible through the add-ons and plugins, which allows users greater control over how the browser acts as compared to Internet Explorer or Chrome (and its open-source'd version, Chromium). It should however be noted that this extensibility through add-ons is a double-edged sword and as such add-ons also have great power to subvert the browsers normal activities as well as enhance them.

If you are uncomfortable with Google as the default search engine, this can be changed through the 'Manage Search Engines...' option from the pull-down menu of the search box. Some more pro-privacy search engines that are worth considering are Startpage and DuckDuckGo.

8.2 Accessing Firefox on Ubuntu

Firefox is already installed on Ubuntu by default. To open it, click on the Unity side bar where you see the Firefox icon:



Figure 8.1: Firefox on Ubuntu

Firefox starts and a welcome window opens:



Figure 8.2: Firefox on Ubuntu

8.3 Installing on Mac OS X

1. To download Firefox, visit <https://www.mozilla.org/firefox> and click on the big green button labeled "Firefox Free Download". The download should start automatically, if it does not, click the link to download it manually.

2. When prompted, click **OK**.

Once the download is complete a window similar to this appears:

3. Click and drag the **Firefox** icon on top of the **Applications** icon.
4. When the installation is finished, close the two small Firefox windows.
5. Eject the Firefox disk image. If this does not work by normal means, select the disk image icon and then, in the Finder menu, select **File > Eject Firefox**.
6. Now, open the **Applications** directory and drag the **Firefox** icon to the dock:
7. Click the **Firefox** icon in the Dock to start Firefox. The Import Wizard dialog box appears:

8.3 Installing on Mac OS X

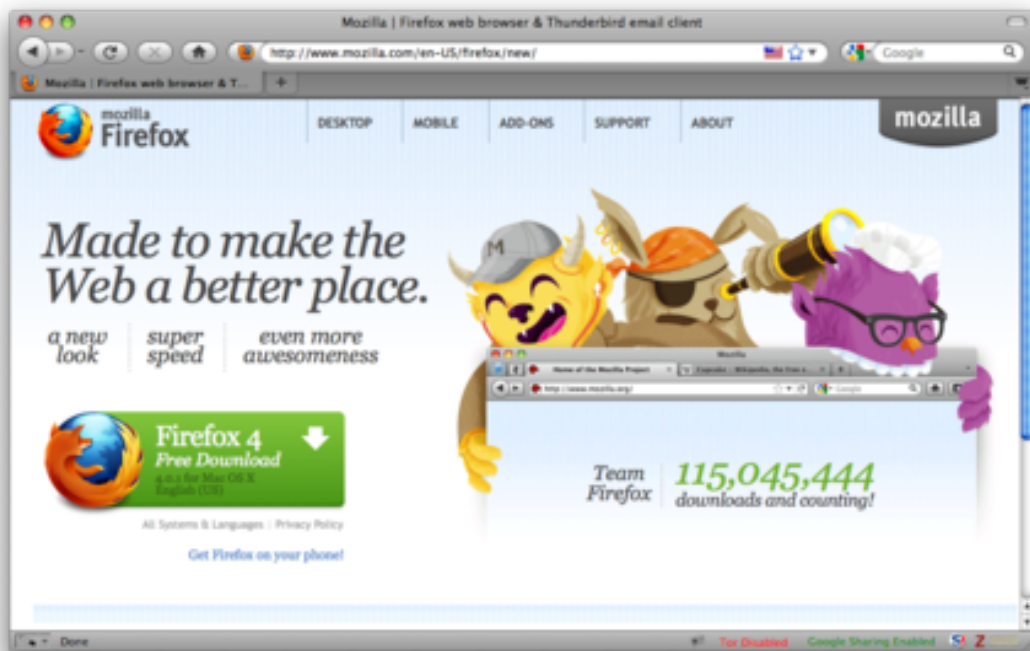


Figure 8.3: Mac OS X Firefox Install

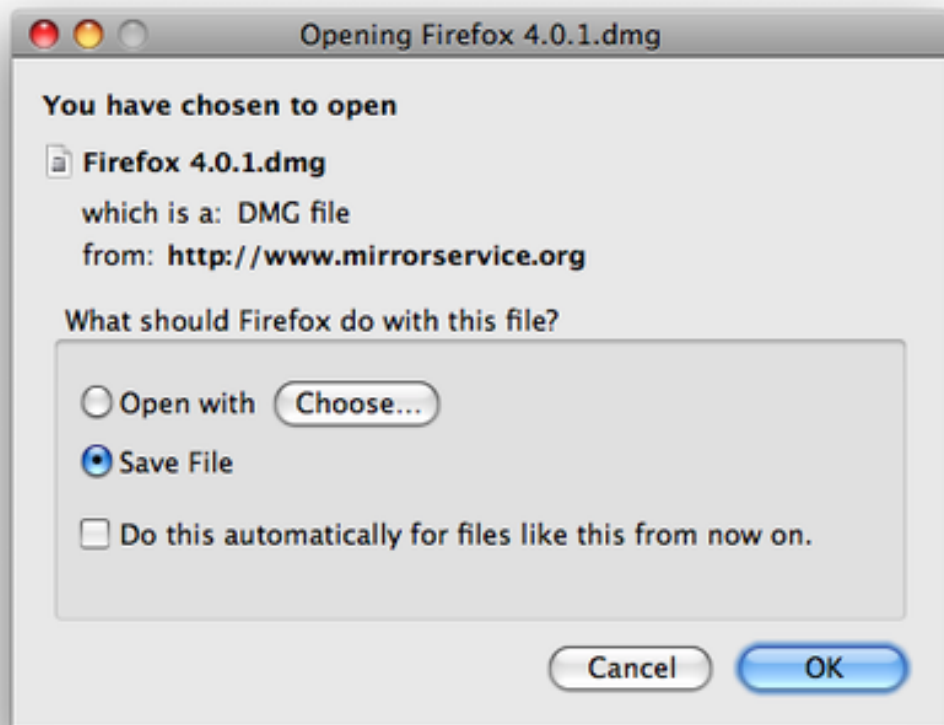


Figure 8.4: Mac OS X Firefox Install



Figure 8.5: Mac OS X Firefox Install



Figure 8.6: Mac OS X Firefox Install

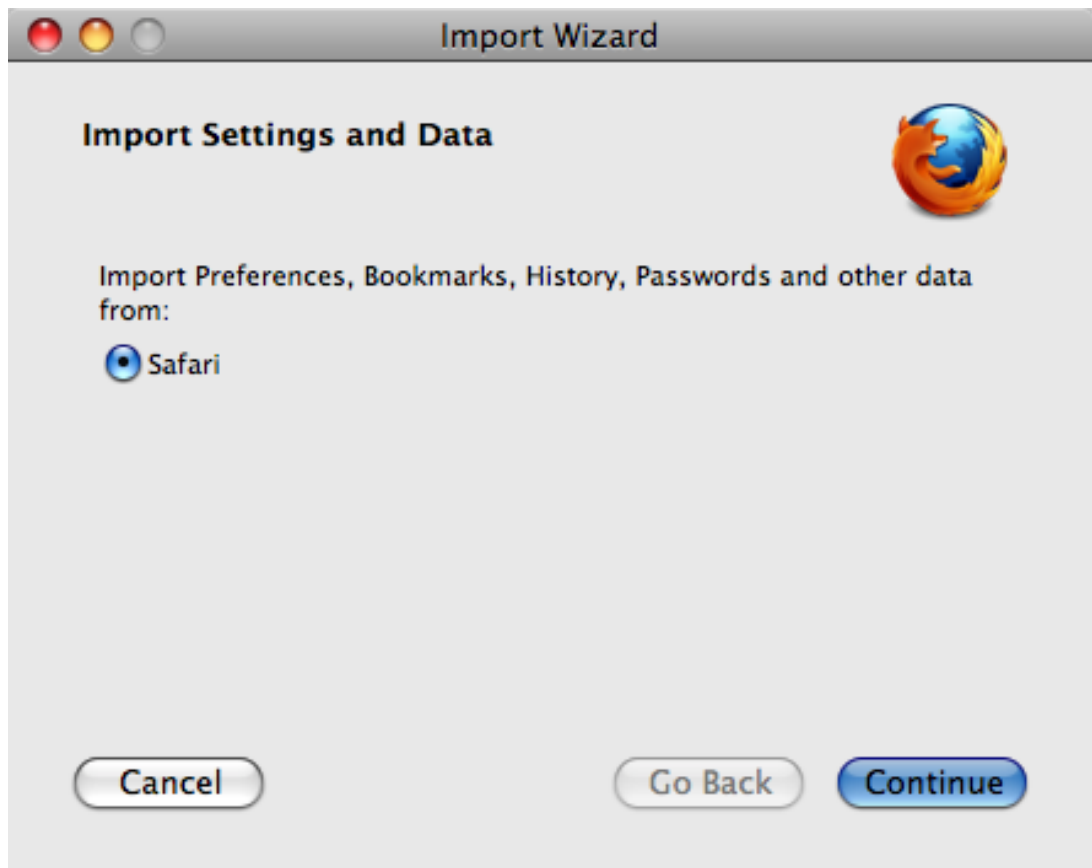


Figure 8.7: Mac OS X Firefox Install

8.4 Installing Firefox on Windows

8. To import your bookmarks, passwords and other data from Safari, click **Continue**. If you don't want to import anything, just select **Cancel**.

Congratulations, you are now ready to use Firefox!



Figure 8.8: Mac OS X Firefox Install

8.4 Installing Firefox on Windows

1. To download Firefox, visit <https://www.mozilla.com/firefox/>.
2. Click the download button and the installation file will begin to download to your computer.
3. Once the download is complete, double-click the installation file to start the Firefox installation wizard.
 - If you are running Windows Vista, you may get a User Account Control prompt. In this case, allow the setup to run by clicking **Continue**.


The image shows a screenshot of the Mozilla Firefox desktop download page. At the top left is the Mozilla Firefox logo. To its right are the words "DESKTOP" and "MOBILE" in a light blue box. The main headline reads "Made to make the Web a better place." Below this, three phrases are listed: "a new look", "super speed", and "even more awesomeness", each separated by a vertical dotted line. A large green button with a white download arrow contains the text "Firefox 4 Free Download" and "4.0.1 for Windows English (British)". Below the button, it says "All Systems & Languages | Privacy Policy" and "Get Firefox on your phone!".

mozilla
Firefox

DESKTOP | MOBIL

*Made to make the
Web a better place.*

a new look | *super speed* | *even more awesomeness*

 **Firefox 4**
Free Download
4.0.1 for Windows
English (British)

All Systems & Languages | Privacy Policy

Get Firefox on your phone!

Figure 8.9: Windows Firefox Install

- If you are running Windows 7, you will be asked whether to allow Firefox to make changes to your computer. Click on **Yes**.

A welcome screen appears.

4. Click **Next** to continue. You will be asked if you would like the standard installation, or whether you would like to customize it. Choose the standard installation and click **Next**.

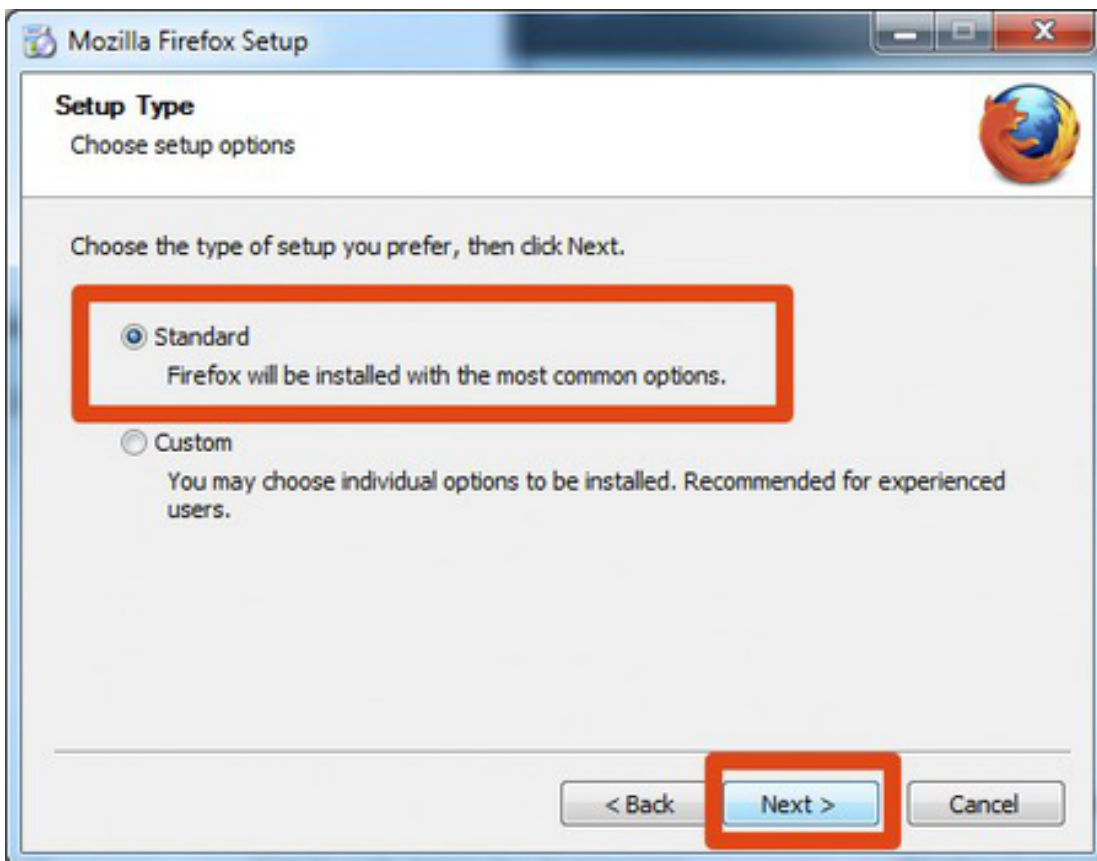


Figure 8.10: Windows Firefox Install

5. You will be asked if you want Firefox to be your default browser. This is recommended.
6. Click **Install**.
7. To import your bookmarks and other data from other browsers (for example Internet Explorer), click **Continue**. If you don't want to import anything, just select **Cancel**.

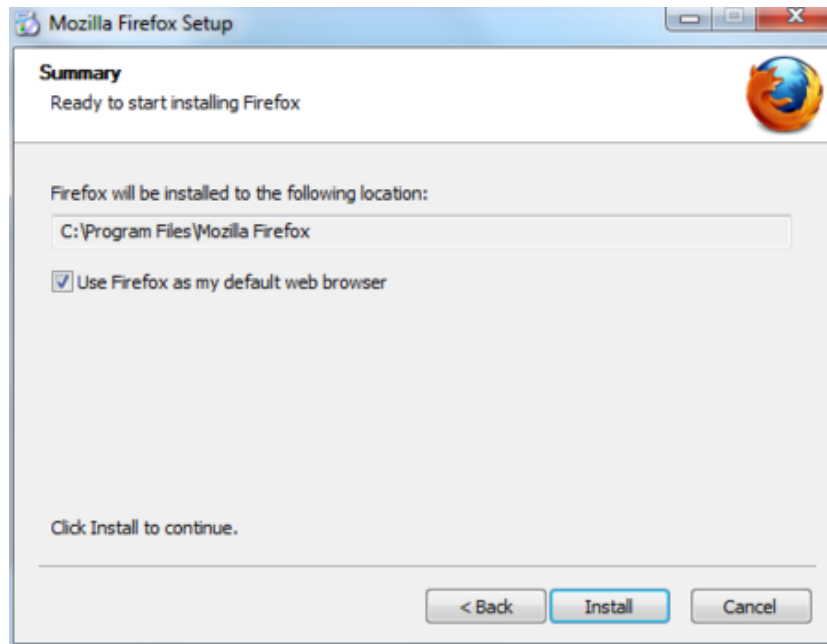


Figure 8.11: Windows Firefox Install

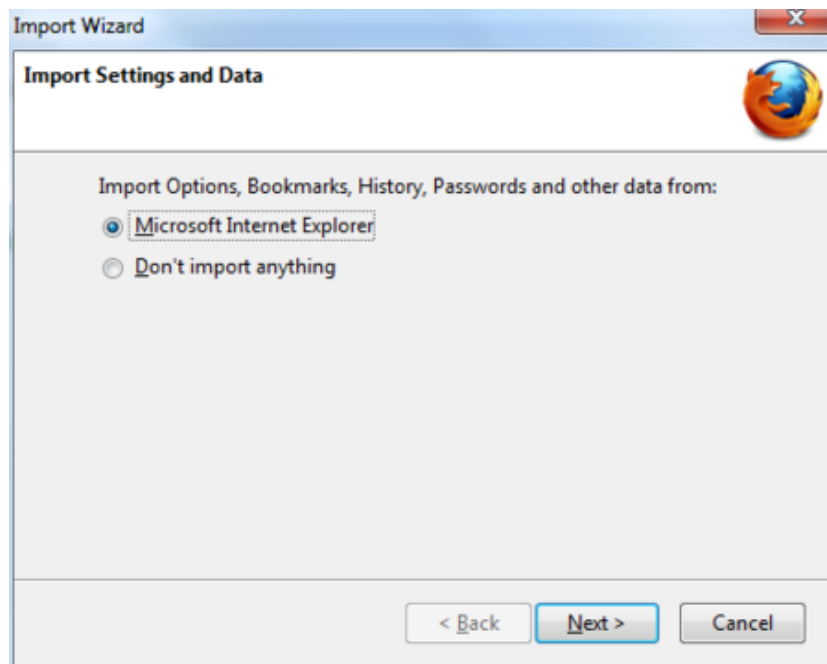


Figure 8.12: Windows Firefox Install

8. Once Firefox has been installed, click **Finish** to close the setup wizard.

If the **Launch Firefox now** check box is checked, Firefox will start after you click **Finish**. Otherwise you can launch Firefox through the start menu.

Windows Vista Users

If at any time throughout the installation process you are prompted with a User Account Control (UAC) window, press Continue, Allow, or Accept.

8.4.1 Troubleshooting

If you have problems starting Firefox, see <https://support.mozilla.com/kb/Firefox+will+not+start>

8.5 Extending Firefox

When you first download and install Firefox, it can handle basic browser tasks immediately. You can also add extra capabilities or change the way Firefox behaves by installing add-ons, small additions that extend Firefox's power.

Firefox extensions can pimp your browser, but they can also collect and transmit information about you. Before you install any add-on, keep in mind to choose add-ons from trusted sources. Otherwise, an add-on might share information about you without your knowing, keep a record on the sites you have visited, or even harm your computer.

There are several kinds of add-ons:

- *Extensions* add functionality to Firefox
- *Themes* change the appearance of Firefox.
- *Plugins* help Firefox handle things it normally can't process (i.e. Flash movies, Java applications).

For the topics covered in this book we are only going to need extensions. We will look at some add-ons that are particularly relevant for dealing with Internet security. The variety of available extensions is enormous. You can add dictionaries for different languages, track the weather in other countries, get suggestions for Web sites that are similar to the one you are currently viewing, and much more. Firefox keeps a list of current extensions on its site (<https://addons.mozilla.org/firefox>), or you can browse them by category at <https://addons.mozilla.org/firefox/browse>.

Caution: We recommend that you never install an add-on for Firefox unless it is available from the Firefox add-on pages. You should also never install Firefox unless you get the installation files from a trusted source. It is important to note that using Firefox on someone else's computer or in an Internet caf increases your potential vulnerability. Know that you can take Firefox on a CD or USB-stick (check our chapter on that issue).

While no tool can protect you completely against all threats to your online privacy and security, the Firefox extensions described in this chapter can significantly reduce your exposure to the most common ones, and increase your chances of remaining anonymous.

8.5.1 HTTPS Everywhere

HTTP is considered unsafe, because communication is transmitted in plain text. Many sites on the Web offer some support for encryption over HTTPS, but make it difficult to use. For instance, they may connect you to HTTP by default, even when HTTPS is available, or they may fill encrypted pages with links that go back to the unencrypted site. The HTTPS Everywhere extension fixes these problems by rewriting all requests to these sites to HTTPS. Although the extension is called “HTTPS Everywhere”, it only activates HTTPS on a particular list of sites and can only use HTTPS on sites that have chosen to support it. It cannot make your connection to a site secure if that site does not offer HTTPS as an option.

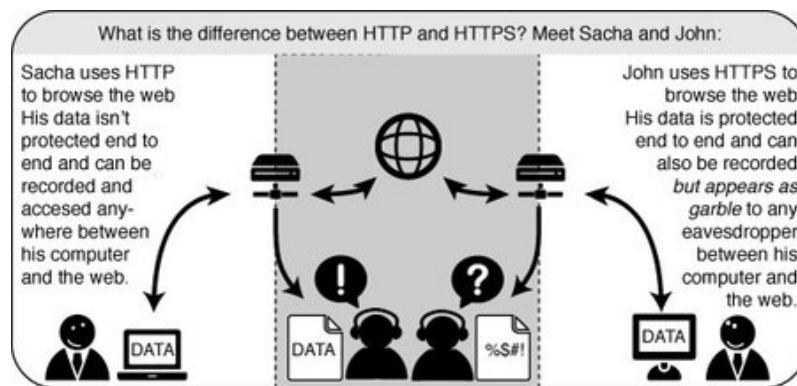


Figure 8.13: HTTPS Schema

Please note that some of those sites still include a lot of content, such as images or icons, from third party domains that is not available over HTTPS. As always, if the browser’s lock icon is broken or carries an exclamation mark, you may remain vulnerable to some adversaries that use active attacks or traffic analysis. However, the effort required to monitor your browsing should still be usefully increased.

Some Web sites (such as Gmail) provide HTTPS support automatically, but using HTTPS Everywhere will also protect you from TLS/SSL-stripping attacks, in which an attacker hides the HTTPS version of the site from your computer if you initially try to access the HTTP version.

Additional information can be found at: <https://www.eff.org/https-everywhere>.

8.5.2 Installation

First, download the HTTPS Everywhere extension from the official Web site: <https://www.eff.org/https-everywhere>

Select the newest release. In the example below, version 2.2 of HTTPS Everywhere was used. (A newer version may be available now.)

Click on “Allow”. You will then have to restart Firefox by clicking on the “Restart Now” button. HTTPS Everywhere is now installed.



HTTPS Everywhere

HTTPS Everywhere is a Firefox and Chrome extension that encrypts your communications with many major websites, making your browsing more secure.
Encrypt the web: Install HTTPS Everywhere today.

- HTTPS Everywhere
- FAQ
- Creating HTTPS Everywhere Rulesets
- Hack On The Code
- How to Deploy HTTPS Correctly



Install in Firefox
Version 2.2 Stable



Install in Chrome
Alpha Version

Figure 8.14: HTTPS Everywhere



HTTPS Everywhere

Figure 8.15: HTTPS Everywhere

8.5.3 Configuration

To access the HTTPS Everywhere settings panel in Firefox 4 (Linux), click on the Tools menu at the top of your screen and then select Add-ons. (Note that in different versions of Firefox and different operating systems, the Add-ons Manager may be located in different places in the interface.)



Figure 8.16: HTTPS Everywhere

Click on the Preferences button.

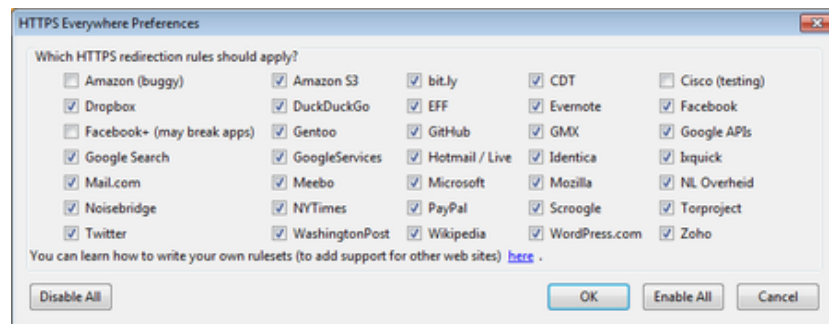


Figure 8.17: HTTPS Everywhere

A list of all supported Web sites where HTTPS redirection rules should be applied will be displayed. If you have problems with a specific redirection rule, you can uncheck it here. In that case, HTTPS Everywhere will no longer modify your connections to that specific site.

8.5.4 Usage

Once enabled and configured, HTTPS Everywhere is very easy and transparent to use. Type an insecure HTTP URL (for example, `http://www.google.com`).

Press Enter. You will be automatically redirected to the secure HTTPS encrypted Web site (in this example: `https://encrypted.google.com`). No other action is needed.

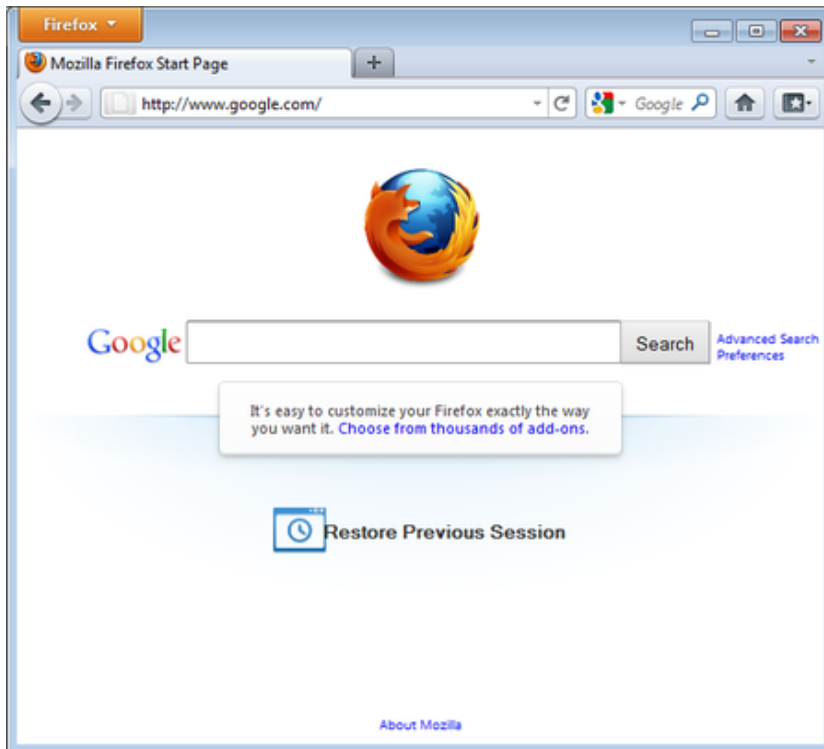


Figure 8.18: HTTPS Everywhere

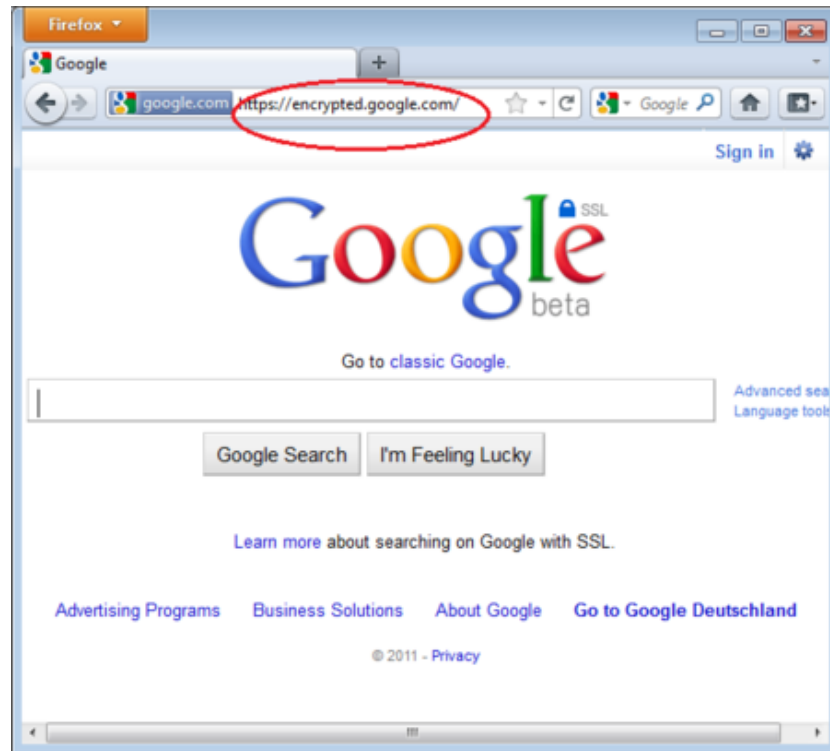


Figure 8.19: HTTPS Everywhere

8.5.5 If networks block HTTPS

Your network operator may decide to block the secure versions of Web sites in order to increase its ability to spy on what you do. In such cases, HTTPS Everywhere could prevent you from using these sites because it forces your browser to use only the secure version of these sites, never the insecure version. (For example, we heard about an airport WiFi network where all HTTP connections were permitted, but not HTTPS connections. Perhaps the WiFi operators were interested in watching what users did. At that airport, users with HTTPS Everywhere were not able to use certain Web sites unless they temporarily disabled HTTPS Everywhere.)

In this scenario, you might choose to use HTTPS Everywhere together with a circumvention technology such as Tor or a VPN in order to bypass the network's blocking of secure access to Web sites.

8.5.6 Adding support for additional sites in HTTPS Everywhere

You can add your own rules to the HTTPS Everywhere add-on for your favorite Web sites. You can find out how to do that at: <https://www.eff.org/https-everywhere/rulesets>. The benefit of adding rules is that they teach HTTPS Everywhere how to ensure that your access to these sites is secure. But remember: HTTPS Everywhere does not allow you to access sites securely unless the site operators have already chosen to make their sites available through HTTPS. If a site does not support HTTPS, there is no benefit to adding a ruleset for it.

If you are managing a Web site and have made an HTTPS version of the site available, a good practice would be to submit your Web site to the official HTTPS Everywhere release.

8.5.7 Enforcing secure HTTPS server connections

Even if you instruct your browser to use the HTTPS protocol when communicating with a web server, it is still possible that the server (due to unsecure configuration on its own side) enforces a unsecure SSL cipher protocol for the connection. The only way to prevent this is by telling the browser to not accept such unsecure SSL protocols (like those based on RC4 encryption).

To disable RC4 encryption for HTTPS connections you have to switch those off in Firefox. In an empty address bar type “about:config”, press return and close the warning dialog displayed next (you can disable this dialog if you want for the next time you configure Firefox). In the search field enter “rc4” and look at the list displayed as a search result:

Any entry with a “true” in the last column (“Value” field) is activated and should be deactivated. Simply right-click on the entry and “Toggle” the value field to false. Proceed for all entries until all of them have a value of “false”.

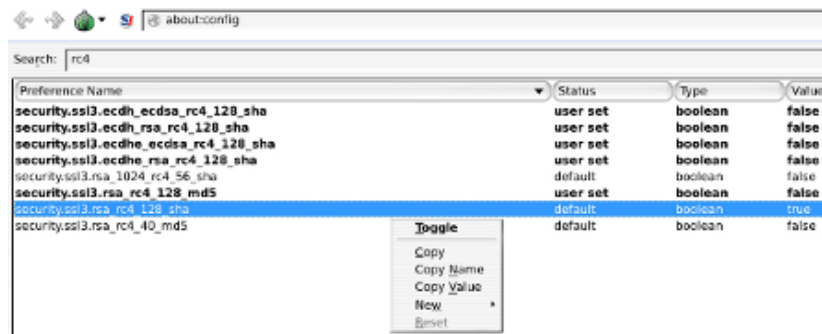


Figure 8.20: Disable RC4

8.5.8 Adblock Plus

Adblock Plus (<http://www.adblockplus.org>) is mainly known for blocking advertisements on websites. But it also can be used to block other content that may try to track you. To keep current with the latest threats, Adblock Plus relies on blacklists maintained by volunteers.

Extra Geek info: How does Adblock Plus block addresses?

The hard work here is actually done by Gecko, the engine on top of which Firefox, Thunderbird and other applications are built. It allows something called “content policies”. A content policy is simply a JavaScript (or C++) object that gets called whenever the browser needs to load something. It can then look at the address that should be loaded and some other data and decide whether it should be allowed. There is a number of built-in content policies (when you define which sites shouldn’t be allowed to load images in Firefox or SeaMonkey, you are actually configuring one of these built-in content policies) and any extension can register one. So all that Adblock Plus has to do is to register its content policy, other than that there is only application logic to decide which addresses to block and user interface code to allow configuration of filters.

8.5.9 Getting started with Adblock Plus

Once you have Firefox installed:

1. Download the latest version of Adblock Plus from the Add-On database of Firefox
2. Confirm that you want Adblock Plus by clicking “Install Now”.
3. After Adblock Plus has been installed, Firefox will ask to restart.

8.5.10 Choosing a filter subscription

Adblock Plus by itself doesn’t do anything. It can see each element that a Web site attempts to load, but it doesn’t know which ones should be blocked. This is what Adblock’s filters are for. After restarting Firefox, you will be asked to choose a filter subscription (free).

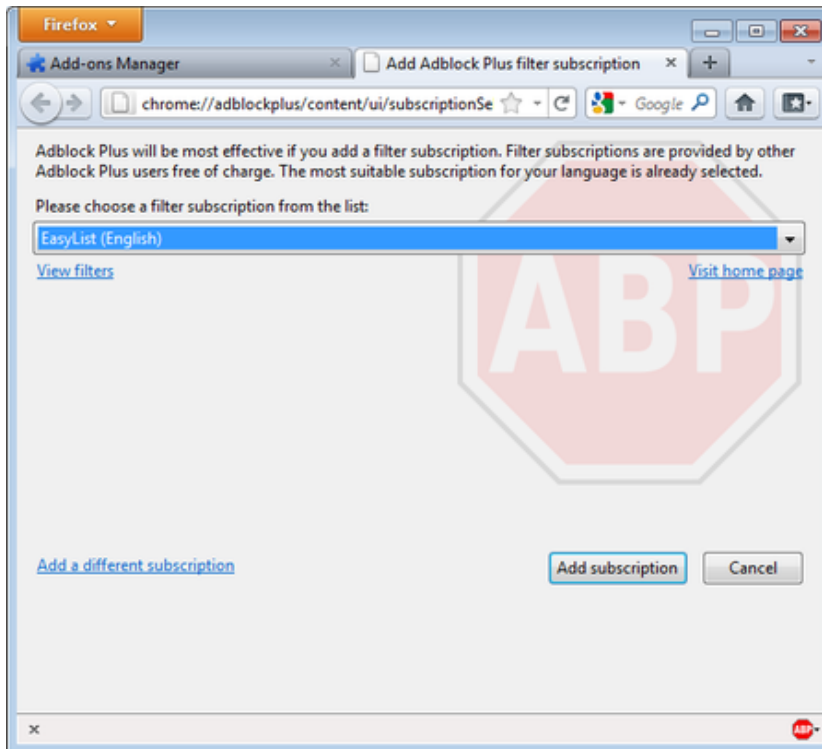


Figure 8.21: Ad Block Plus

Which filter subscription should you choose? Adblock Plus offers a few in its dropdown menu and you may wish to learn about the strengths of each. A good filter to start protecting your privacy is EasyList (also available at <http://easylist.adblockplus.org/en>).

As tempting as it may seem, don't add as many subscriptions as you can get, since some may overlap, resulting in unexpected outcomes. EasyList (mainly targeted at English-language sites) works well with other EasyList extensions (such as region-specific lists like RuAdList or thematic lists like EasyPrivacy). But it collides with Fanboy's List (another list with main focus on English-language sites).

You can always change your filter subscriptions at any time within preferences. Once you've made your changes, click OK.

8.5.11 Creating personalized filters

AdBlock Plus also lets you create your own filters, if you are so inclined. To add a filter, start with Adblock Plus preferences and click on "Add Filter" at the bottom left corner of the window. Personalized filters may not replace the benefits of well-maintained blacklists like EasyList, but they're very useful for blocking specific content that isn't covered in the public lists. For example, if you wanted to prevent interaction with Facebook from other Web sites, you could add the following filter:

```
||facebook.*$domain=~facebook.com|~127.0.0.1
```

The first part (`||facebook.*`) will initially block everything coming from Facebook's domain. The second part (`$domain=~facebook.com|~127.0.0.1`) is an exception that tells the filter to allow Facebook requests only when you are in Facebook or if the Facebook requests come from 127.0.0.1 (your own computer) in order to keep certain features of Facebook working.

A guide on how to create your own Adblock Plus filters can be found at <http://adblockplus.org/en/filters>.

8.5.12 Enabling and disabling AdBlock Plus for specific elements or Web sites

You can see the elements identified by AdBlock Plus by clicking on the ABP icon AdBlock Plus icon in your browser (usually next to the search bar) and selecting "Open blockable items". A window at the bottom of your browser will let you enable or disable each element on a case-by-case basis. Alternatively, you can disable AdBlock Plus for a specific domain or page by clicking on the ABP icon and ticking the option "Disable on [domain name]" or "Disable on this page only".

8.5.13 Other extensions that can improve your security

Below is a short list of extensions that are not covered in this book but are helpful to further protect you.

- **Flagfox** - puts a flag in the location bar telling you where the server you are visiting is most probably located. <https://addons.mozilla.org/en-US/firefox/addon/flagfox/>
- **BetterPrivacy** - manages “cookies” used to track you while visiting websites. Cookies are small bits of information stored in your browser. Some of them are used to track the sites you are visiting by advertisers. <https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/>
- **GoogleSharing** - If you are worried that google knows your search history, this extension will help prevent that. <https://addons.mozilla.org/en-us/firefox/addon/googlesharing/>
- **NoScript** - Although not friendly for beginners, this addon will block scripts and third party plugin content (eg, Adobe Flash) unless specifically allowed by the user, it also provides general protection against simple cross site scripting vectors. <http://noscript.net/>
- **User Agent Switcher** - Your browser supplies large amounts of identifying information to any remote server through the ‘User-Agent’ header, including Operating System and specific version information. This addon allows you to supply either a fake or generic User-Agent to the server. <http://chrispederick.com/work/user-agent-switcher/>

8.6 Proxy Settings

A proxy server allows you to reach a Web site or other Internet location even when direct access is blocked in your country or by your ISP. There are many different kinds of proxies, including:

- Web proxies, which only require that you know the address to the proxy Web site, which may have a URL similar to <http://proxy.com/cgi-bin/nph-proxy.cgi>
- HTTP proxies, which require that you modify your Browser settings. HTTP proxies only work for Web content. You may get the information about a HTTP proxy in the format `proxy.example.com:3128` or `192.168.0.1:8080`.
- SOCKS proxies, which also require that you modify your Browser settings. SOCKS proxies work for many different Internet applications, including e-mail and instant messaging tools. The SOCKS proxy information looks just like HTTP proxy information.

You can use a Web proxy directly without any configuration by typing in the URL. The HTTP and SOCKS proxies, however, have to be configured in your Web browser.

8.6.1 Default Firefox proxy configuration

In Firefox you can change the settings for using a proxy. You'll need to open the Options or Preferences window of Firefox. You can find this in the menu, by clicking on the top of the Window and selecting **Edit > Preferences** on Linux or **Tools > Options** on Windows.

Go to the Network section and open the Advanced tab.

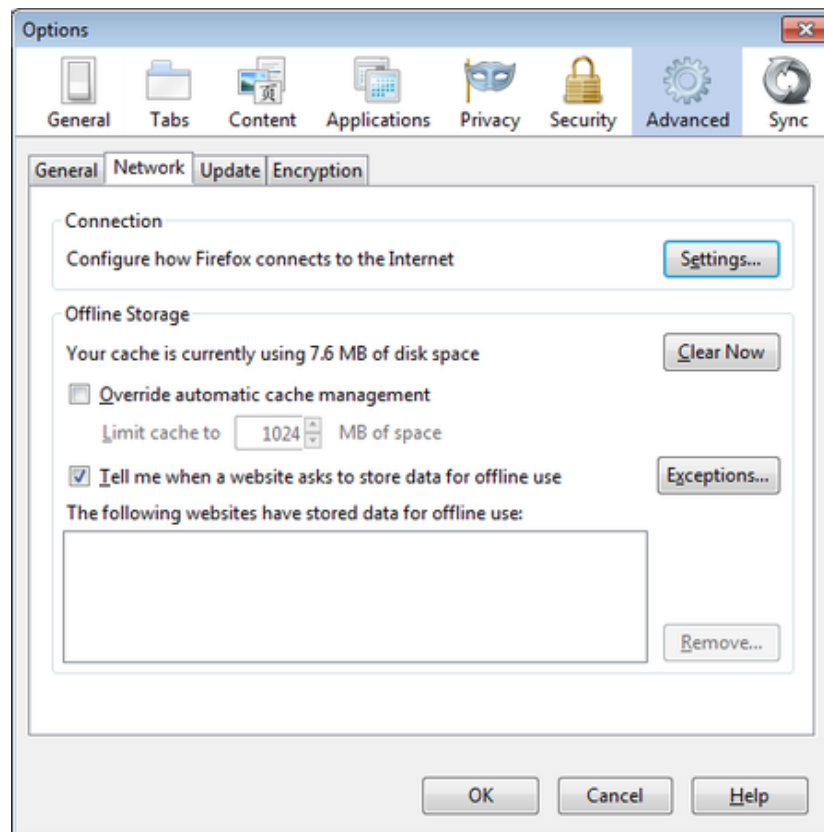


Figure 8.22: Firefox Proxy Settings

Select Settings, click on “Manual proxy configuration” and enter the information of the proxy server you want to use. Please remember that HTTP proxies and SOCKS proxies work differently and have to be entered in the corresponding fields. If there is a colon (:) in your proxy information, that is the separator between the proxy address and the port number. Your screen should look like this:

After you click OK, your configuration will be saved and your Web browser will automatically connect through that proxy on all future connections. If you get an error message such as, “The proxy server is refusing connections” or “Unable to find the proxy server”, there is a problem with your proxy configuration. In that case, repeat the steps above and select “No proxy” in the last screen to deactivate the proxy.

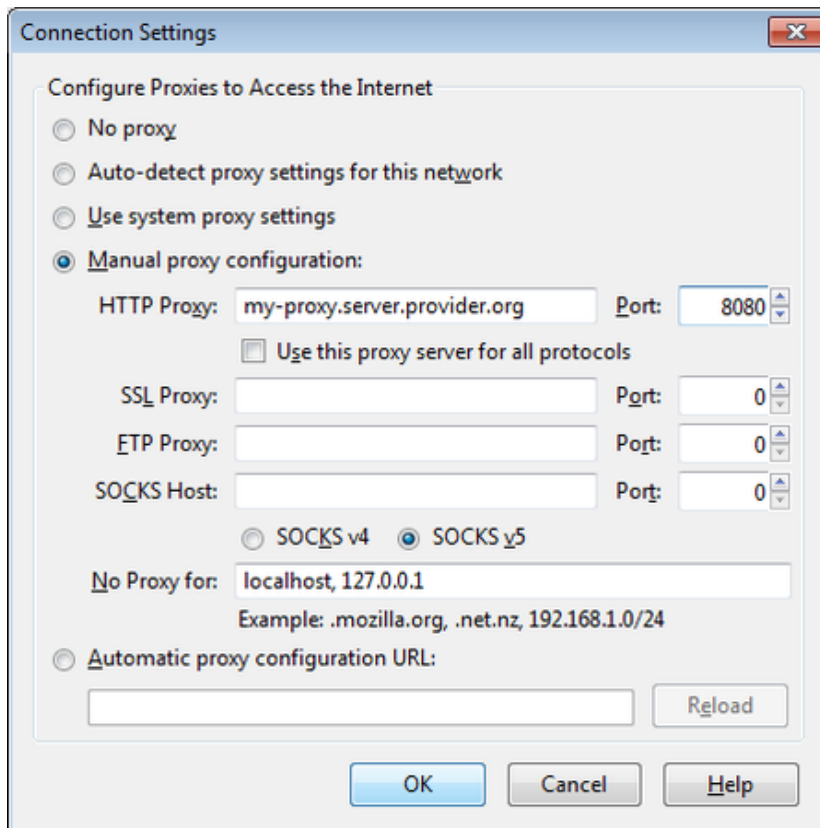


Figure 8.23: Firefox Proxy Settings

8.7 Using Tor?

Tor is a system intended to enable online anonymity, composed of client software and a network of servers which can hide information about users' location and other factors which might identify them. Imagine a message being wrapped in several layers of protection: every server is only able to take off one layer, thereby immediately deleting the sender information of the previous server.

If Alice wants to view Bob's website, instead of directly talking to Bob like this:

Alice -> Bob

This is fine, and Alice and Bob can use end to end cryptography to ensure privacy, integrity and authenticity of their communications, however if Alice does not want Bob to know that she is viewing his website or does not want Eve (a hypothetical eavesdropper, on Alice or Bobs side of the connection) to know she and Bob are communicating, extra steps must be taken.

Alice instead makes an encrypted connection to an EntryNode on the Tor network, here they establish a TLS connection and the EntryNode allows Alice to make a further connection through it. Once again a TLS connection is established this time through the already encrypted EntryNode connection, and once again the process is repeated through the RelayNode to the ExitNode. Now, Alice is encrypting the data 3 times, first for the ExitNode, then for the RelayNode and finally for the EntryNode. Creating a network path like this:

Alice -> EntryNode -> RelayNode -> ExitNode -> Bob

When the EntryNode receives Alice's data it is still encrypted for the RelayNode and ExitNode, it knows where the data is coming from but not the final destination or the message content, it then passes the data on to the RelayNode. The RelayNode receives the data but it is still encrypted for the ExitNode, it knows it is coming from the EntryNode and going to the ExitNode but does not know the final destination or the original sender, it then passes the data to the ExitNode which removes the final layer of encryption, the ExitNode knows what the message is, that it came from RelayNode but does not know where it entered the network, or who sent it.

This layered approach is where Tor derives it's name from (The Onion Router), each 'layer' knows only of the layer on either side of it, meaning that none in the chain except Alice knows the full path the data is taking, however Alice, Bob and the ExitNode are all able to see the message content, thus end-to-end cryptography is still required to ensure privacy, integrity and authenticity of the communications across the Tor network.

Use of this system makes it more difficult to trace internet traffic to the user, including visits to Web sites, online posts, instant messages, and other communication forms. It is intended to protect users' personal freedom, privacy, and ability to conduct confidential business, by keeping their internet activities from being monitored. The software is open-source and the network is free of charge to use.

Like all current low latency anonymity networks, Tor cannot and does not attempt to protect against monitoring of traffic at the boundaries of the Tor network, i.e., the traffic entering and exiting the network. While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called end-to-end correlation)

Caution: As Tor does not, and by design cannot, encrypt the traffic between an exit node and the target server, any exit node is in a position to capture any traffic passing through it which does not use end-to-end encryption such as TLS. (If your postman is corrupt he might still open the envelope and read the content). While this may or may not inherently violate the anonymity of the source, if users mistake Tor's anonymity for end-to-end encryption they may be subject to additional risk of data interception by third parties. So: the location of the user remains hidden; however, in some cases content is vulnerable for analysis through which identifying or revealing information about the user may be gained.

8.7.1 Using Tor Browser Bundle

The Tor Browser Bundle lets you use Tor on Windows, OSX and/or Linux without requiring you to configure a Web browser. Even better, it's a portable application that can be run from a USB flash drive, allowing you to carry it to any PC without installing it on each computer's hard drive.

8.7.2 Downloading Tor Browser Bundle

You can download the Tor Browser Bundle from the torproject.org Web site (<https://www.torproject.org>).

If the torproject.org Web site is filtered from where you are, type "tor mirrors" in your favorite Web search engine: The results probably include some alternative addresses to download the Tor Browser Bundle.

Please follow the instructions on the Tor Project Website on how to install the Tor Browser.

Caution: When you download Tor Bundle (plain or split versions), you should check the signatures of the files. This step ensures that the files have not been tampered with. To learn more about signature files and how to check them, read <https://www.torproject.org/docs/verifying-signatures>

8.7.3 Running a Relay or Bridge

Tor is a network of volunteers who run relays and bridges. If you would like to grow the Tor network by contributing bandwidth and spare CPU cycles, consider running a relay. Plus, running a relay may improve your anonymity since an attacker can't distinguish between traffic that originated from you or from the relay. See the Tor FAQ for more details.

However, if you do run a relay, your IP address will be listed on the Internet as a Tor relay. Tor clients depend on this list, provided by Tor Directory Servers, so that they can build circuits. If you wish to contribute to Tor, but do not want to run a public relay,

consider running a bridge. Since Tor relays are public, some ISP block access to the Tor network by blocking *all the relays*. Tor Bridges are unlisted are therefore, more difficult to find.

Tor's goal is to protect anonymity on the Internet, but sometimes Tor is used for illegal purposes. As a relay operator, consult the Legal FAQ, written by the Electronic Frontier Foundation (EFF). The EFF is a U.S. based non-profit organization whose mission is to "protect your digital right." Other countries should seek the advice of similar organizations. However, legal risks can be minimized by running a non-exit relay or bridge.

If you'd like to configure your computer to run a relay or a bridge, visit the Tor website for thorough instructions.

8.8 Extending Google Chrome

Chrome is Google's browser. Here are some useful tips and extensions:

8.8.1 Disabling Instant Search

Chrome can search as you type. The advantage of this is that you get search suggestions and can use Google's predictions - but the disadvantage is that every character you type is sent to Google's servers, where it may be logged.

To disable, open Chrome's settings by clicking the menu button at the right of the address bar and clicking Settings. Or, simply type `chrome://settings/` in your address bar.

Ensure that the **Enable Instant for faster searching (omnibox input may be logged)** checkbox is unchecked.

8.8.2 AdBlock for Chrome

Just like Firefox, AdBlock removes ads. Install from this Chrome Webstore page.

8.8.3 HTTPS Everywhere

Forces encrypted https connections wherever possible. Installation link can be found on the EFF HTTPS Everywhere homepage.

8.8.4 PrivacyFix

PrivacyFix (beta) gives you a dashboard view of your privacy settings on Facebook and Google, as well as Do-Not-Track headers and tracking cookies. It provides links to quickly change these privacy settings without digging through many drilldown pages. Install from the Chrome web store page

9 Passwords

9.1 Keeping passwords safe

Passwords are like keys in the physical world. If you lose a password you will not be able to get in, and if others copy or steal it they can use it to enter. A good password should not be easy for others to guess and not easy to crack with computers, while still being easy for you to remember.

9.1.1 Password length and complexity

To protect your passwords from being guessed, length and complexity are important. Passwords like the name of your pet or a birth date are very unsafe, as is using single word that can be found in a dictionary. Do not use a password containing only numbers. Most importantly a secure password is long. Using combinations of lower case letters, capitals, numbers and special characters can improve the security, but length is still the most important factor.

For use with important accounts like the pass phrase which protects your PGP/GPG or TrueCrypt encrypted data, or the password for your main email account, use 20 characters or more, the longer the better. See this XKCD cartoon "`correct horse battery staple`" vis-À-vis "`Tr0ub4dor&3`" for an explanation.

9.1.2 Easy to remember and secure passwords

One way to create strong and easy to remember passwords is to use sentences.

A few examples:

- `IloveDouglasAdamsbecausehe'sreallyawesome.`
- `Peoplelovemachinesin2029A.D.`
- `BarneyfromHowIMetYourMotherisAWESOME!`

Sentences are easy to remember, even if they are 50 characters long and contain uppercase characters, lowercase characters, symbols and numbers.

9.1.3 Minimizing damage

It is important to minimize the damage if one of your passwords is ever compromised. Use different passwords for different websites or accounts, that way if one is compromised, the others are not. Change your passwords from time to time, especially for accounts you consider to be sensitive. By doing this you can block access to an attacker who may have learned your old password.

9.1.4 Using a password manager

Remembering a lot of different passwords can be difficult. One solution is to use a dedicated application to manage most of your passwords. The next section in this chapter will discuss *Keepass*, a free and open source password manager with no known vulnerabilities, so long as you chose a sufficiently long and complex “master password” to secure it with.

For website passwords only, another option is the built-in password manager of the Firefox browser. Make sure to set a master password, otherwise this is very insecure!

9.1.5 Physical protection

When using a public computer such as at a library, an internet cafe, or any computer you do not own, there are several dangers. Using “over the shoulder” surveillance, someone, possibly with a camera, can watch your actions and may see the account you log in to and the password you type. A less obvious threat is software programs or hardware devices called “keystroke loggers” that record what you type. They can be hidden inside a computer or a keyboard and are not easily spotted. Do not use public computers to log in to your private accounts, such as email. If you do, change your passwords as soon as you get back to a computer you own and trust.

9.1.6 Other caveats

Some applications such as chat or mail programs may ask you to save or “remember” your username and password, so that you don’t have to type them every time the program is opened. Doing so may mean that your password can be retrieved by other programs running on the machine, or directly from your hard disk by someone with physical access to it.

If your login information is sent over an insecure connection or channel, it might fall into the wrong hands. See the chapters on secure browsing for more information.

9.2 Installing KeePass

We will cover installing KeePass on Ubuntu and Windows.

Mac OSX comes with an excellent built-in password manager called Keychain that is just as safe. Downsides are that it isn’t Open Source and doesn’t work on other systems. If you’d need to take your passwords from one Operating System to another it is better to stick with Keepass after all. How to use Keychain is covered in the next chapter.

9.2.1 Installing KeePassX on Ubuntu

To install on Ubuntu we will use the Ubuntu Software Center. Type KeePass in the search field at the top right and the application KeePassX should automatically appear in the listing.

Highlight the item (it may already be highlighted by default) and then press 'Install'. You will be asked to Authorise the installation process:



Figure 9.1: KeePass Install

Enter your password and press 'Authenticate' the installation process will then begin.

Ubuntu does not offer very good feedback to show the software is installed. If the green progress indicator on the left has gone and the progress bar on the right has gone then you can assumed the software is installed.

9.2.2 Installing KeePass on Windows

First visit the KeePass download webpage and choose the appropriate installer. For this chapter we are using the current installer.

Download this to your computer then double click on the installer. You will first be asked to select a language, we will choose English:

Press 'OK' and you will be shown the following screen:

Just press 'Next >' and go to the next screen:

In the screen shown above we must select 'I accept the agreement' otherwise we will not be able to install the software. Choose this option and then press 'Next >'. In the next screen you will be asked to determine the installation location. You can leave this with the defaults unless you have good reason to change them.

Click on 'Next >' and continue.

The above image shows the KeePass components you can choose from. Just leave the defaults as they are and press 'Next >'. You will come to a new screen:

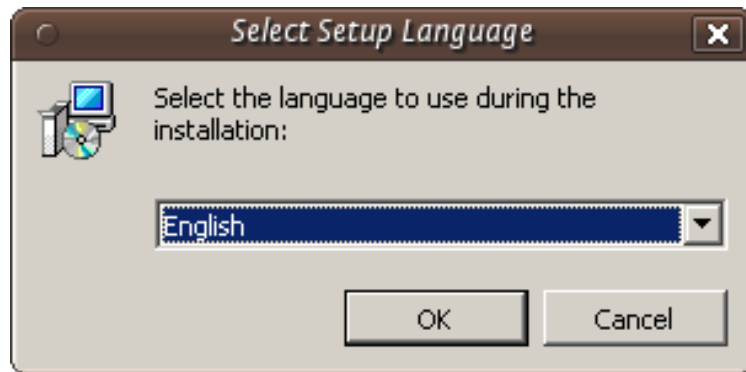


Figure 9.2: KeePass Install



Figure 9.3: KeePass Install

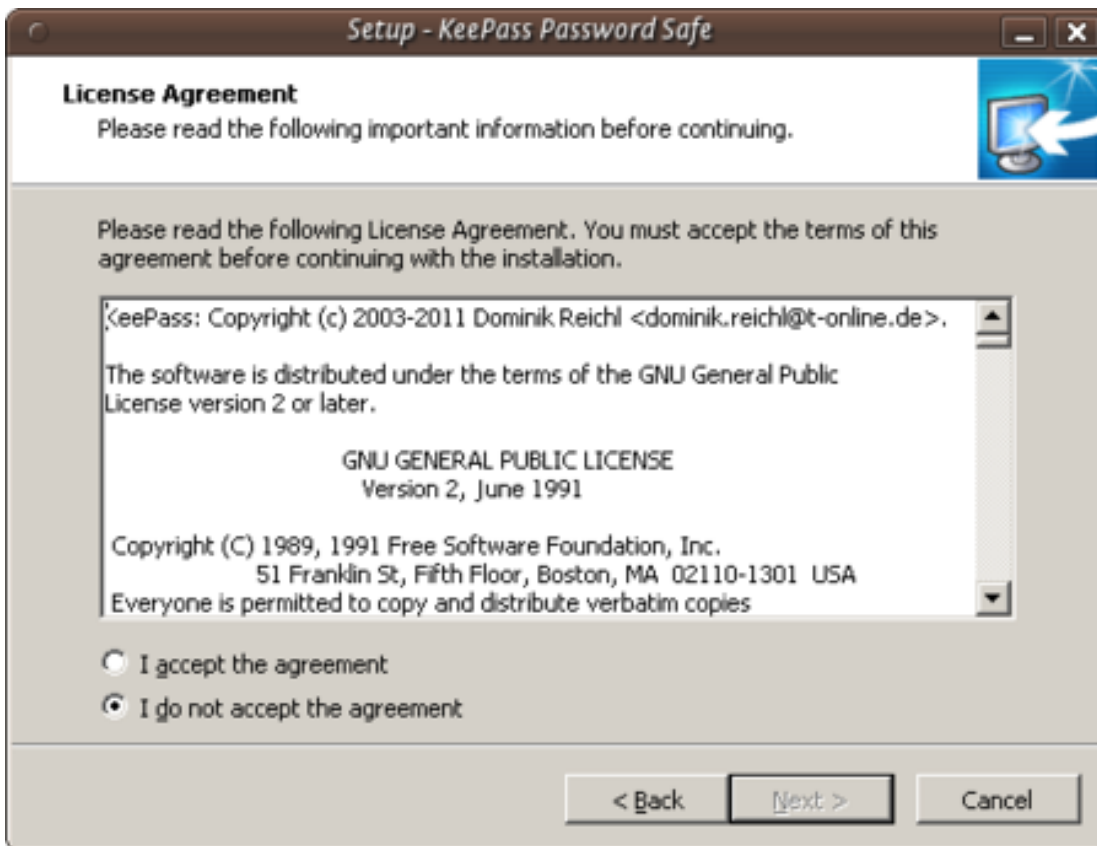


Figure 9.4: KeePass Install

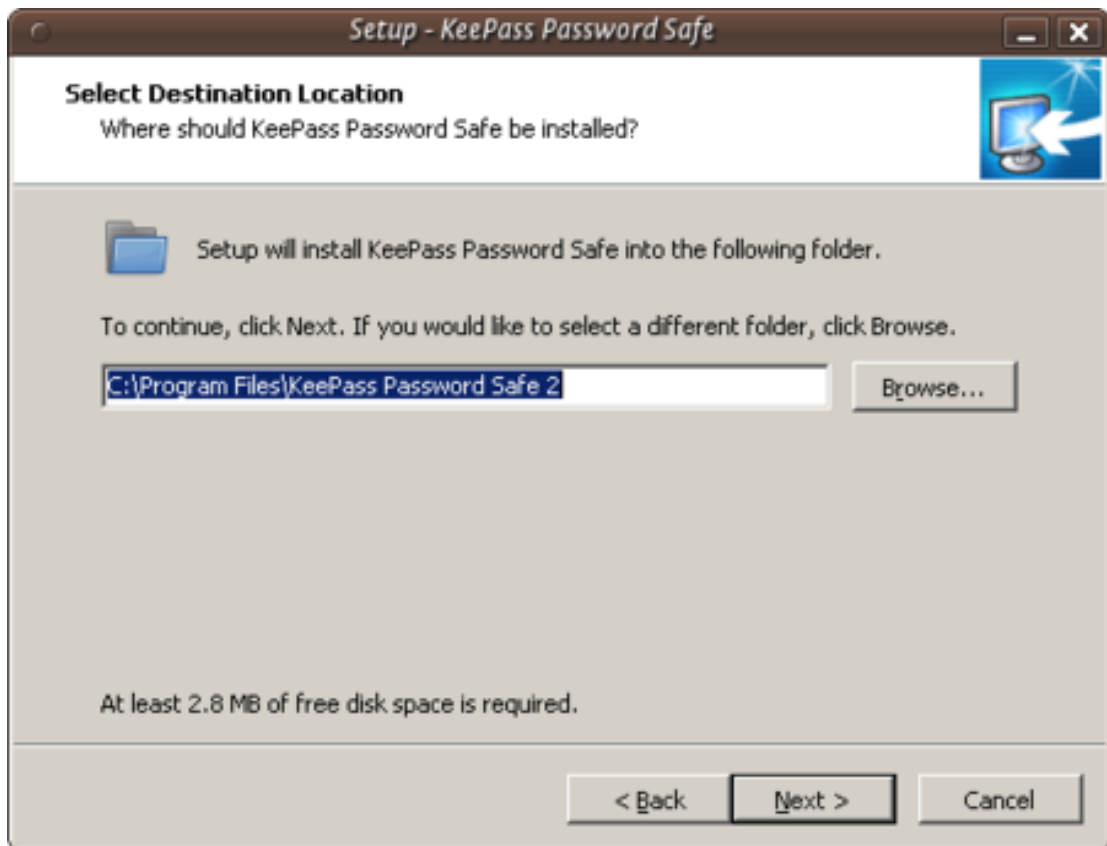


Figure 9.5: KeePass Install

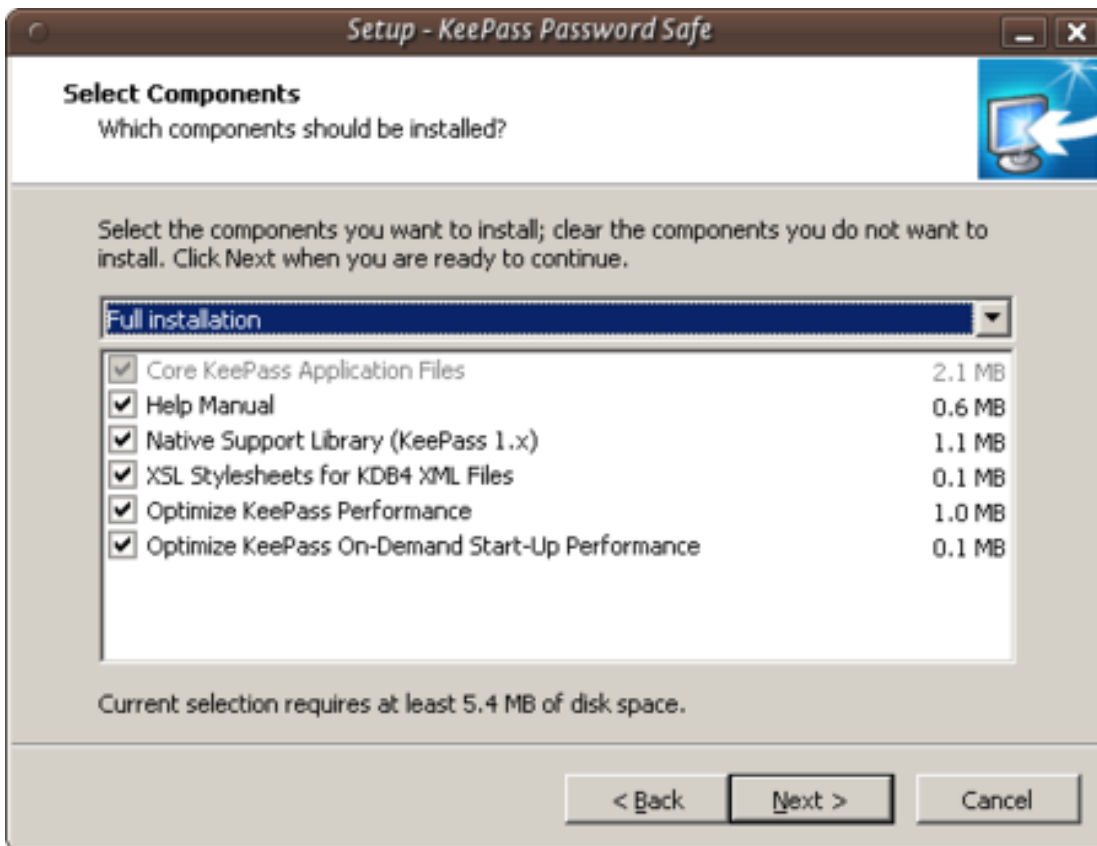


Figure 9.6: KeePass Install



Figure 9.7: KeePass Install

This doesn't do anything but give you a summary of your options. Press 'Install' and the installation process will begin.

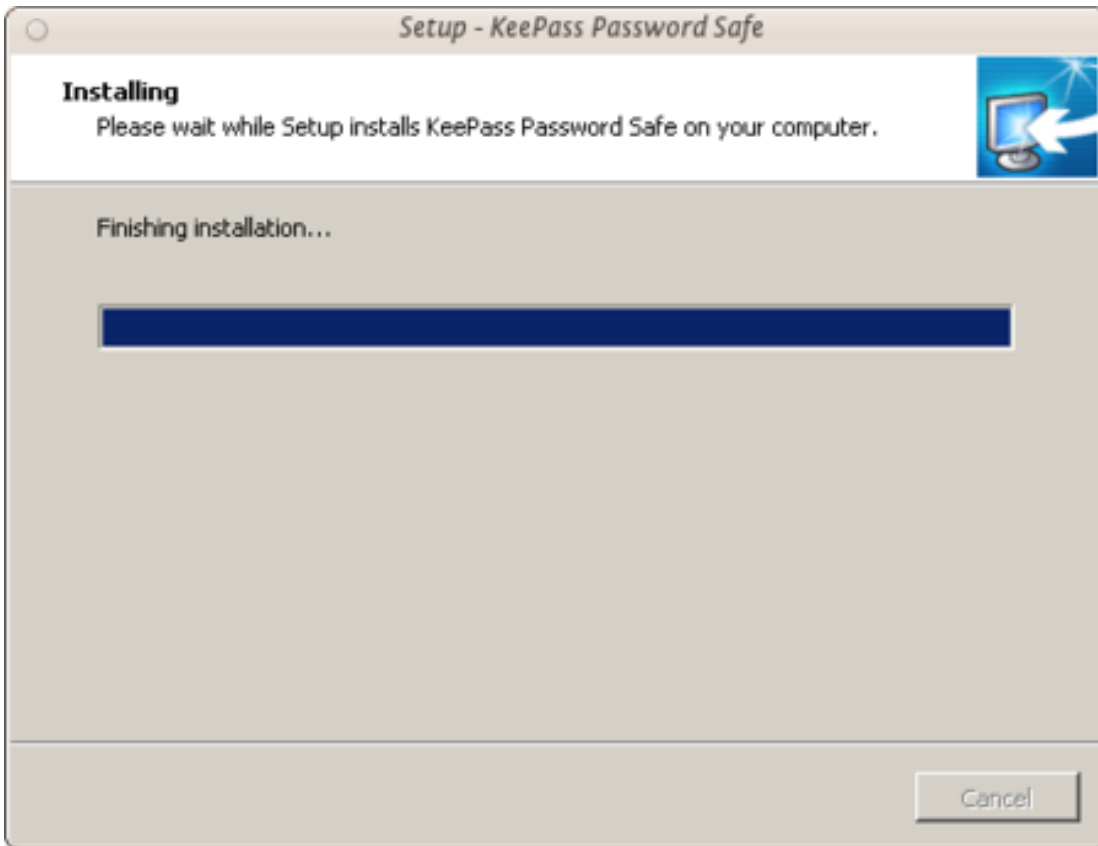


Figure 9.8: KeePass Install

9.2.3 Installing KeePass on Mac OS X

Although Keychain in Mac OS X does an excellent job of storing your passwords, you may want to run your own password database and manager. KeePass allows this added flexibility. First visit the KeePass download webpage <http://keepass.info/download.html> and choose the appropriate installer. Although the official installers are listed at the top of the page, there are unofficial/contributed installers further down. Scroll down to find [KeePass 2.x for Mac OS X]<http://keepass2.openix.be/>:

As this is an external link, your browser will be redirected to <http://keepass2.openix.be/>:

Note here that you must install the Mono framework first, so that KeePass can run in OS X. So click on each of the links Mono 2.10.5 and KeePass2.18 to download the DMG files to your computer. Double-click on each of the DMGs in your downloads folder to unpack the volumes to your desktop.

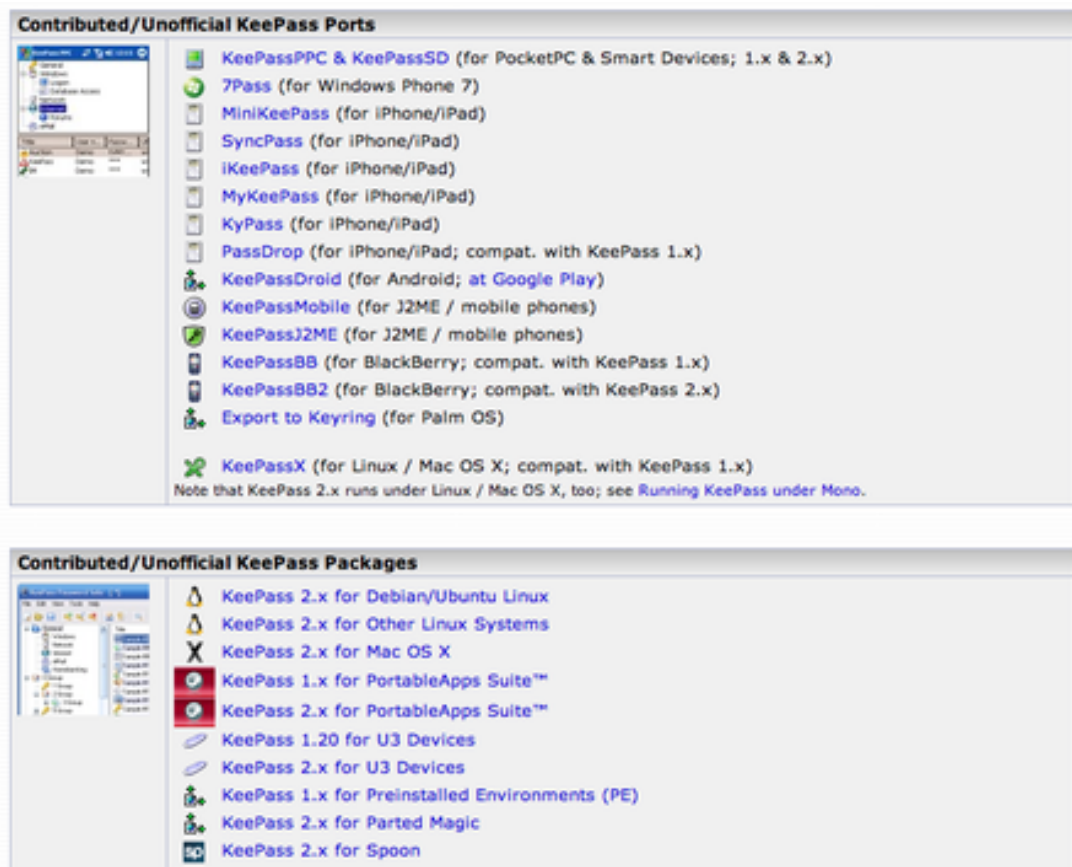


Figure 9.9: KeePass Install

KeePass 2.18 for OS X

Download

Installation instructions:

1. Download and Install Mono for OS X from the link below, this is mandatory step, KeePass not work otherwise
2. Download and Install KeePass from the link below

[Mono 2.10.5](#)
Mono 2.10.5

[KeePass2.18](#)
KeePass 2.18 application package for OS X - md5sum 0a8348a8b21078ae48e66f5a4e47ca89

KeePass 2 for OS X updated to version 2.18!

[Donate](#)

MasterCard VISA

Litecoin:
LgaRBU1Xyfc5XgBvtNMfd6jMyeKCYC644

Bitcoin:
12uPSWW6RVKkD4jHfpcZLPXATe9hncTuPE

Hosted by [openix.be](#)

Figure 9.10: KeePass Install

9 Passwords

The Mono Package installer is in case called something similar to ‘MonoFramework-MRE-2.10.5_0.macos10.xamarin.x86.pkg’, so double-click on this document:

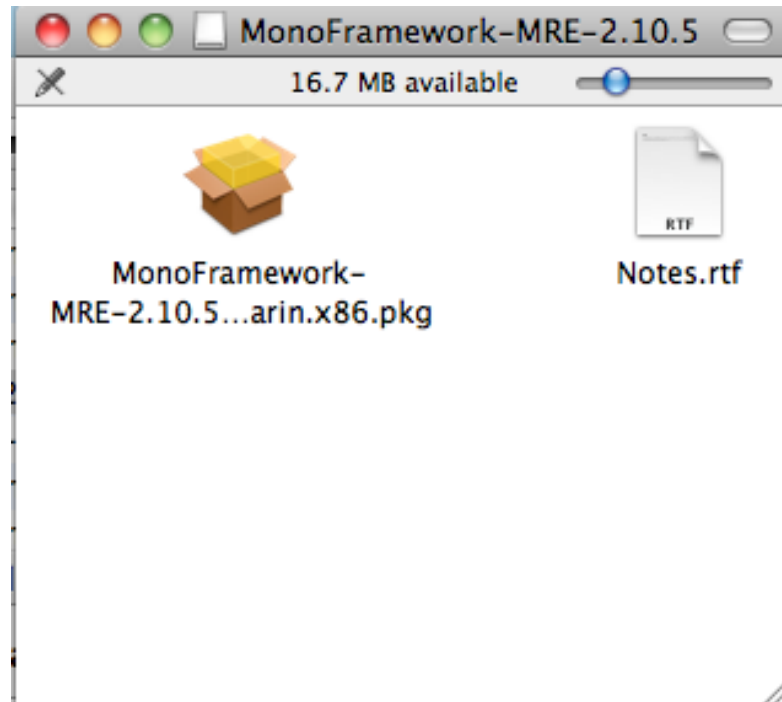


Figure 9.11: KeePass Install

The installer will open and run:

Follow each of the steps by clicking ‘Continue’, the next step being ‘Read Me’. In here is important information such as all of the files that the package will install, including information on how to uninstall Mono:

Click ‘Continue’ to the next screen, the license. Clicking ‘Continue’ on the license screen pops up the agree/disagree dialogue box. If you agree with the license conditions, the installation will continue:

The following two steps in the installation ask you to choose an installation destination, and check there is enough space on the install disk. When the installation has completed, you will see this screen:

Now you can quit the installer. Next take a look at the KeePass disk image, double-click to open it, and drag the KeePass application into your Applications folder:

Now KeePass is ready to use for Mac OS X.

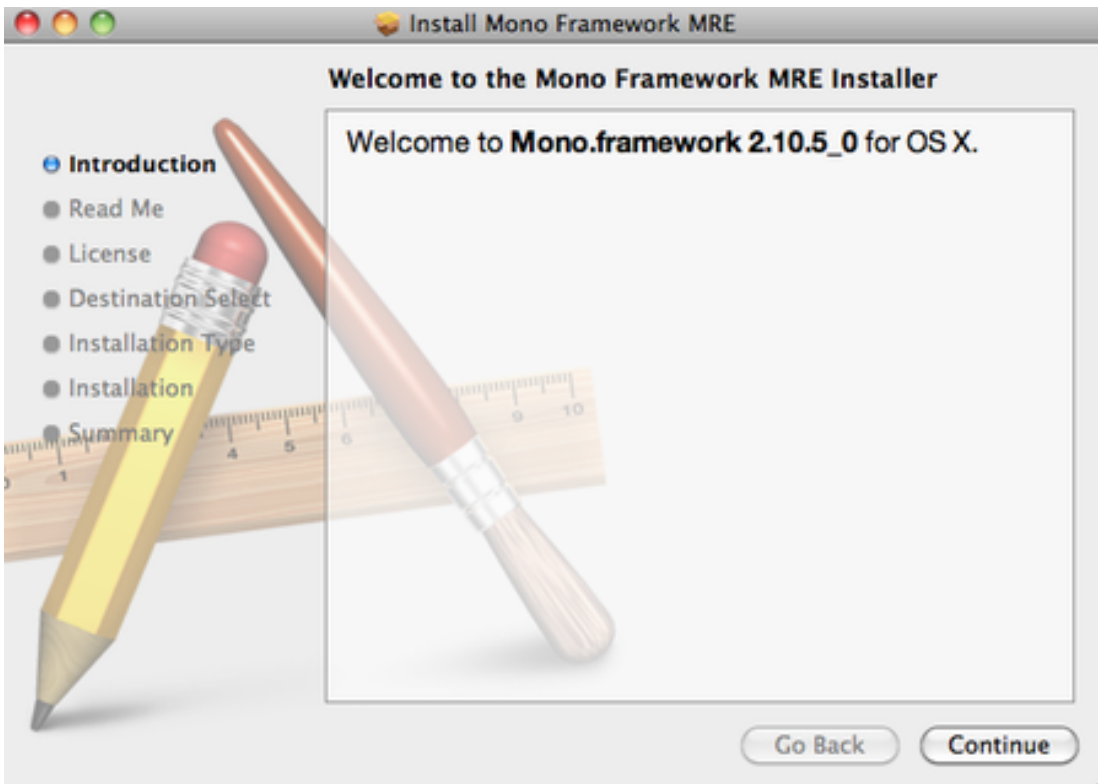


Figure 9.12: KeePass Install

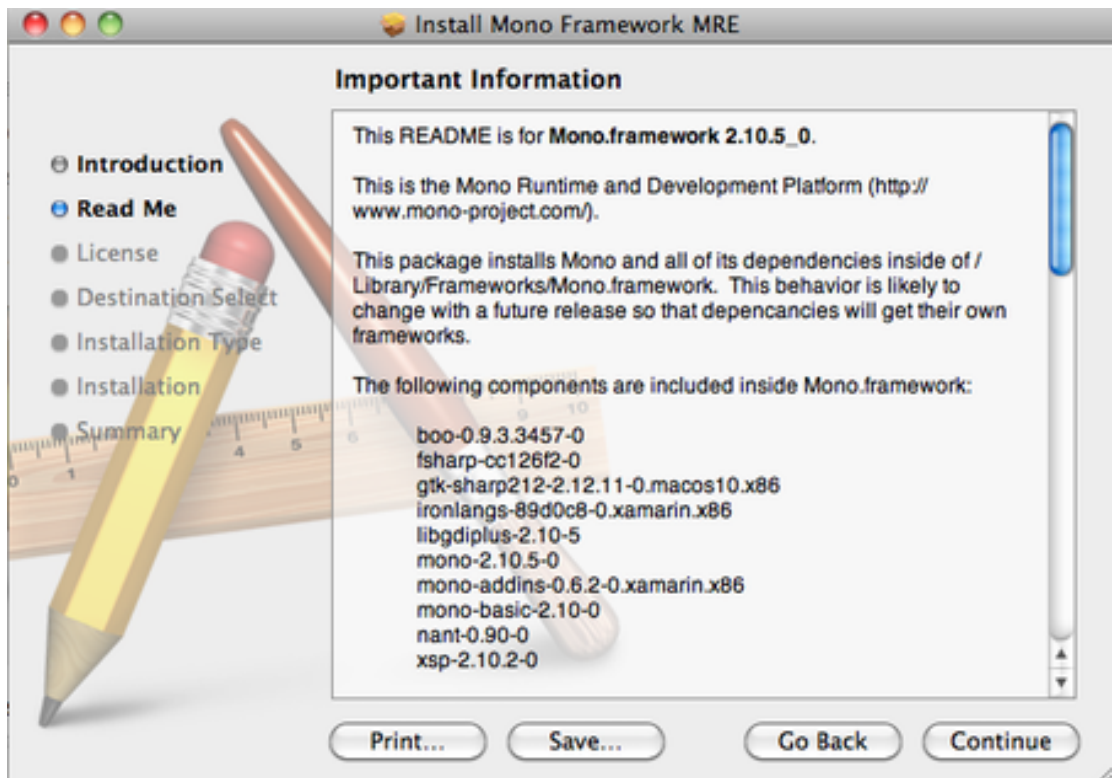


Figure 9.13: Keepass Install

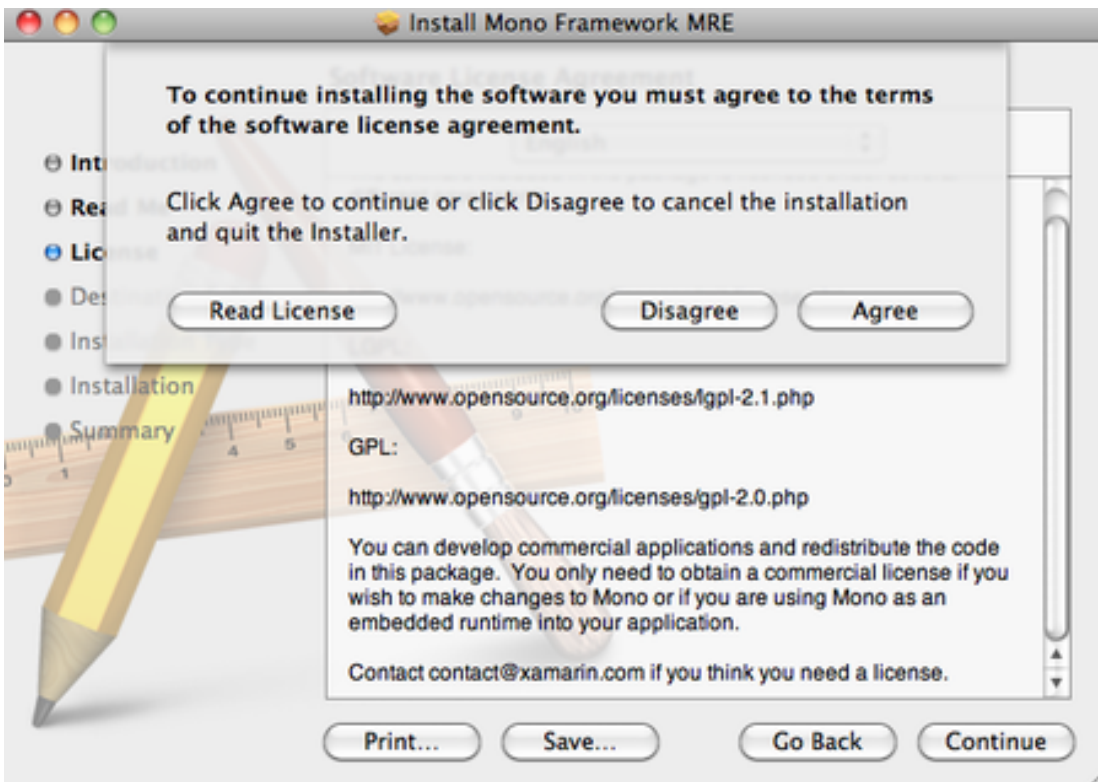


Figure 9.14: KeePass Install

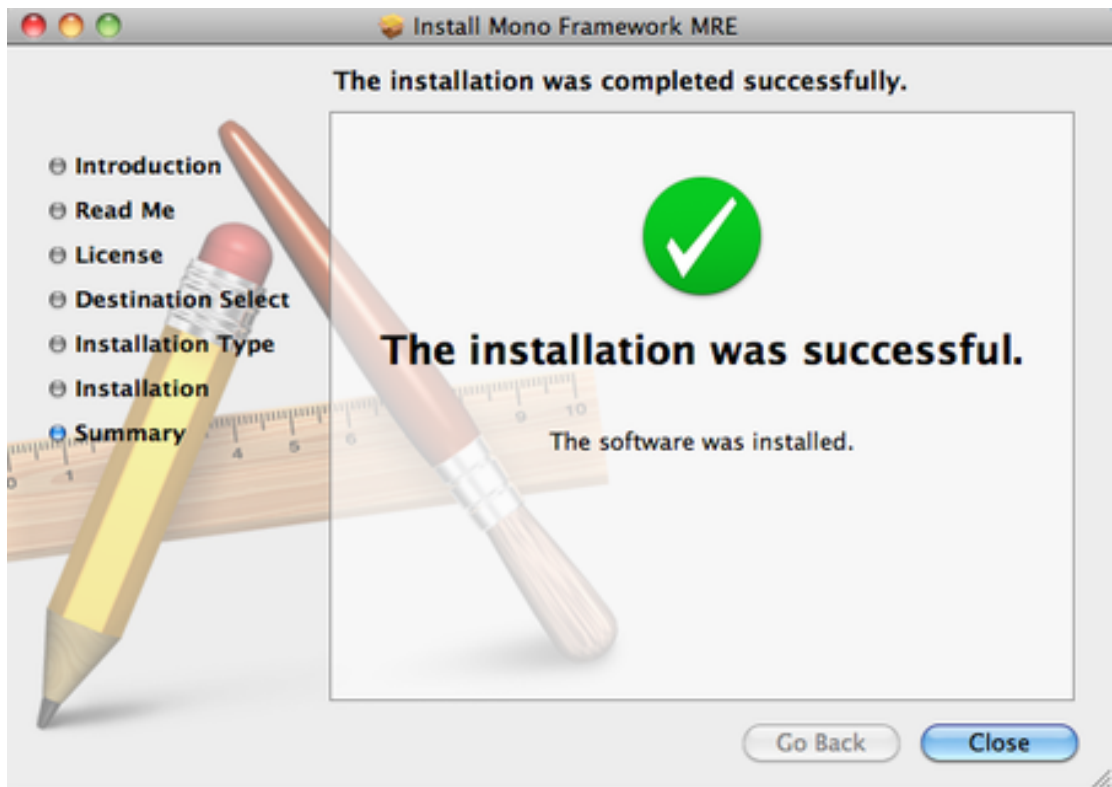


Figure 9.15: KeePass Install



Figure 9.16: KeePass Install

9.3 Encrypting Passwords with a Password Manager

To encrypt password we use KeePass on Windows and KeePassX Ubuntu, and Keychain on OSX. The basic principle is the same; you have a file on your computer which is encrypted with *one single very secure password*. This is sometimes referred to as a ‘Master Password’, ‘Admin-Password’, ‘Root-Password’ etc. but they are all *the ultimate key* to all your other keys and secure data. For this reason you can’t and shouldn’t think to light about creating this password.

If a password manager is part of your OS (like it is with OSX) it unlocks automatically for you after you login to your account and so opening secure information like passwords. For this, and other, reasons you should disable ‘Automatically Login’. When you start-up your computer you should always have to login and, even better, set your computer to automatically logout or lock the screen after a set amount of time.

9.3.1 Encrypting Passwords with KeePassX on Ubuntu

First open KeePassX from the Applications->Accessories -> KeePassX menu.

The first time you use KeePassX you need to set up a new database to store your passwords. Click on File->New Database

You will be asked to set a master key (password).

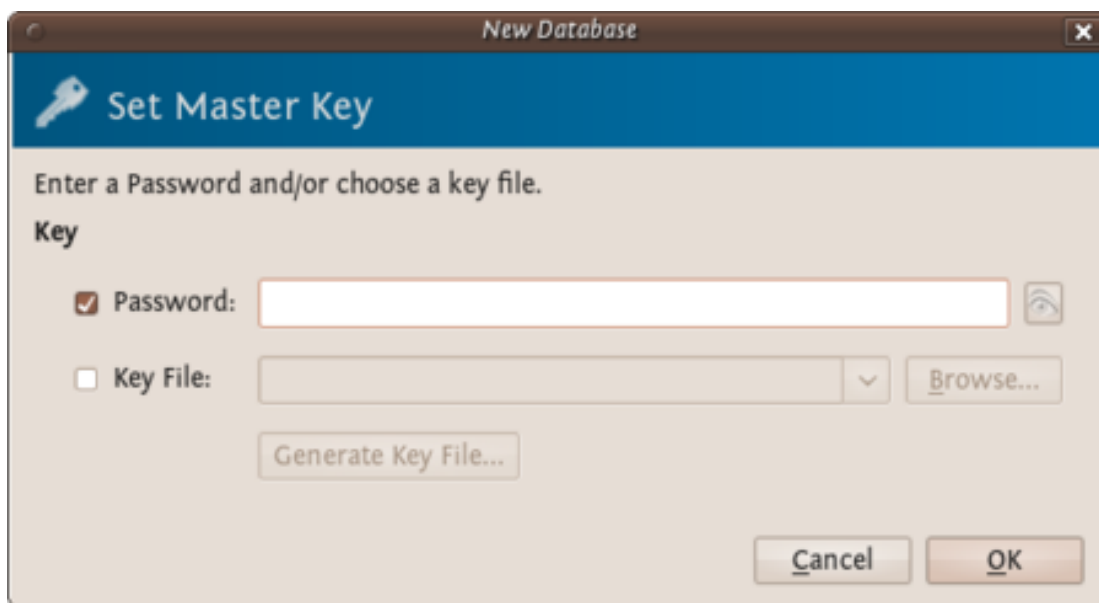


Figure 9.17: Password Manager

Choose a strong password for this field - refer to the chapter about passwords if you would like some tips on how to do this. Enter the password and press ‘OK’. You then are asked to enter the password again. Do so and press ‘OK’. If the passwords are the same you will see a new KeePassX ‘database’ ready for you to use.

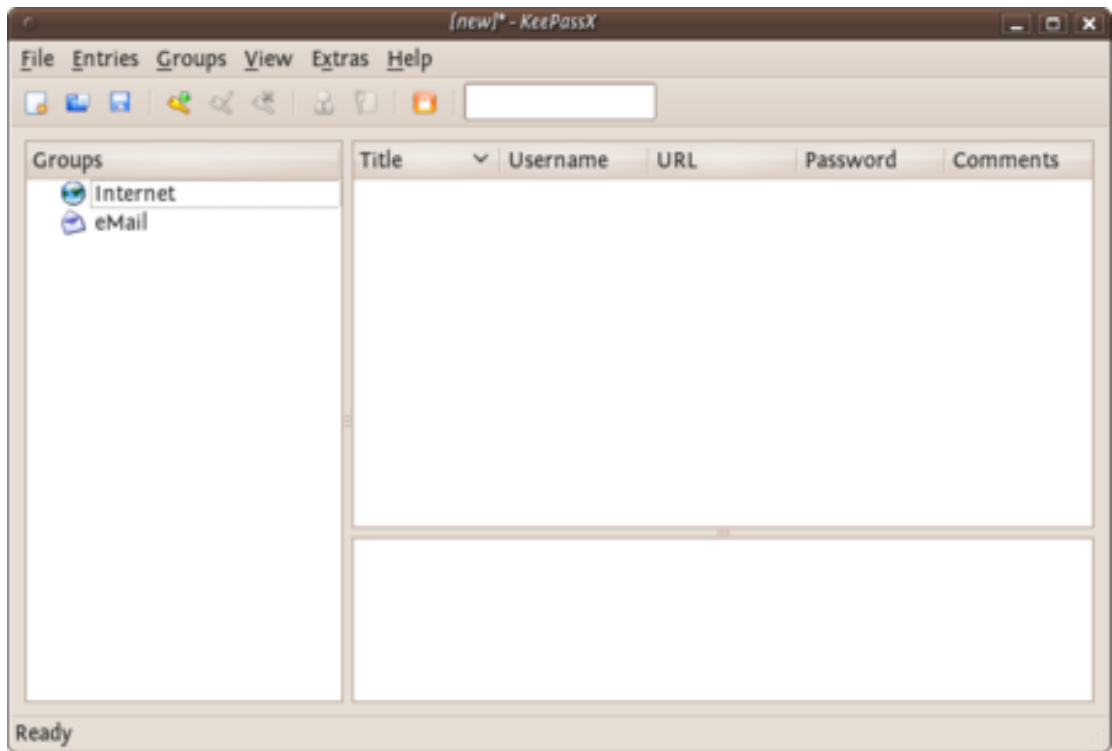


Figure 9.18: Password Manager

9.3 Encrypting Passwords with a Password Manager

Now you have a place to store all your passwords and protect them by the ‘master’ password you just set. You will see two default categories ‘Internet’ and ‘Email’ - you can store passwords just under these two categories, you can delete categories, add subgroups, or create new categories. For now we just want to stay with these two and add a password for our email to the email group. Right click on the email category and choose ‘Add New Entry...’:

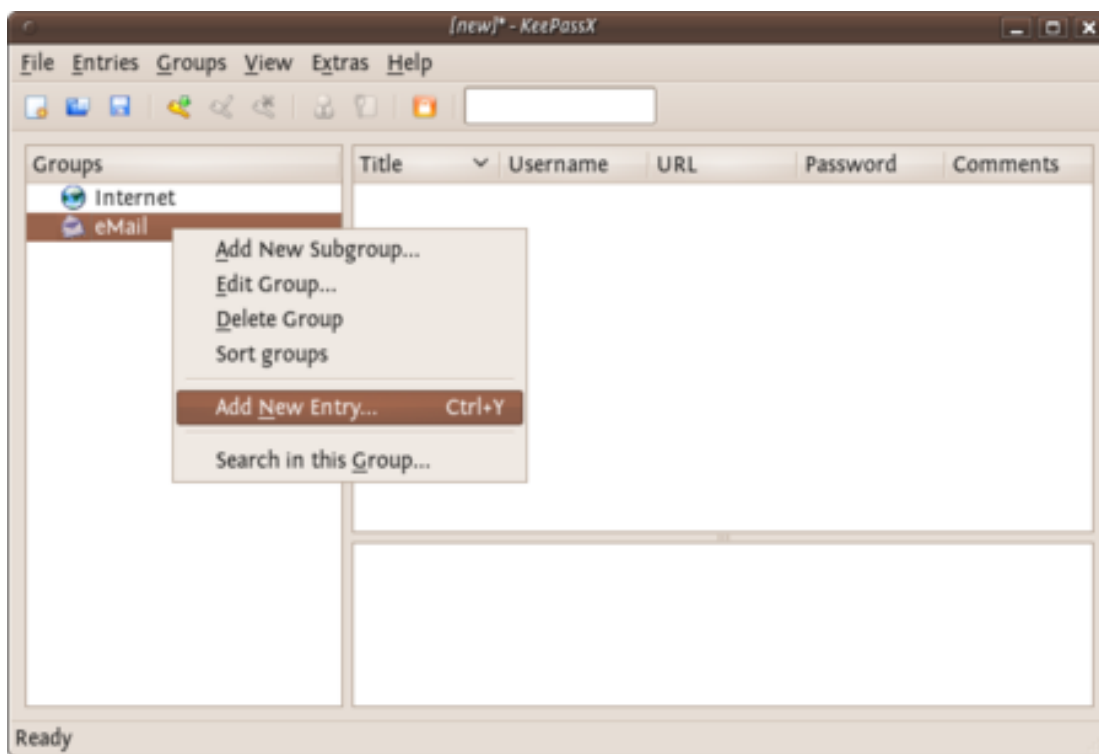


Figure 9.19: Password Manager

So now fill this form out with the details so you can correctly identify which email account the passwords are associated with. You need to fill out the fields ‘Title’ and the password fields. All else is optional.

KeePassX gives some indication if the passwords you are using are ‘strong’ or ‘weak’. As may be obvious, you should try to use stronger passwords. For advice on this see the chapter on creating good passwords. Press ‘OK’ when you are done and you will see something like this:

To recover the passwords (see them) you must double click on the enter and you will see the same window you used for recording the information. If you click on the ‘eye’ icon to the right of the passwords they will be converted from stars (***) to the plain text so you can read it.

Now you you can use KeePassX to store your passwords. However before getting too excited you must do one last thing. When you close KeePassX (choose File->Quit) it

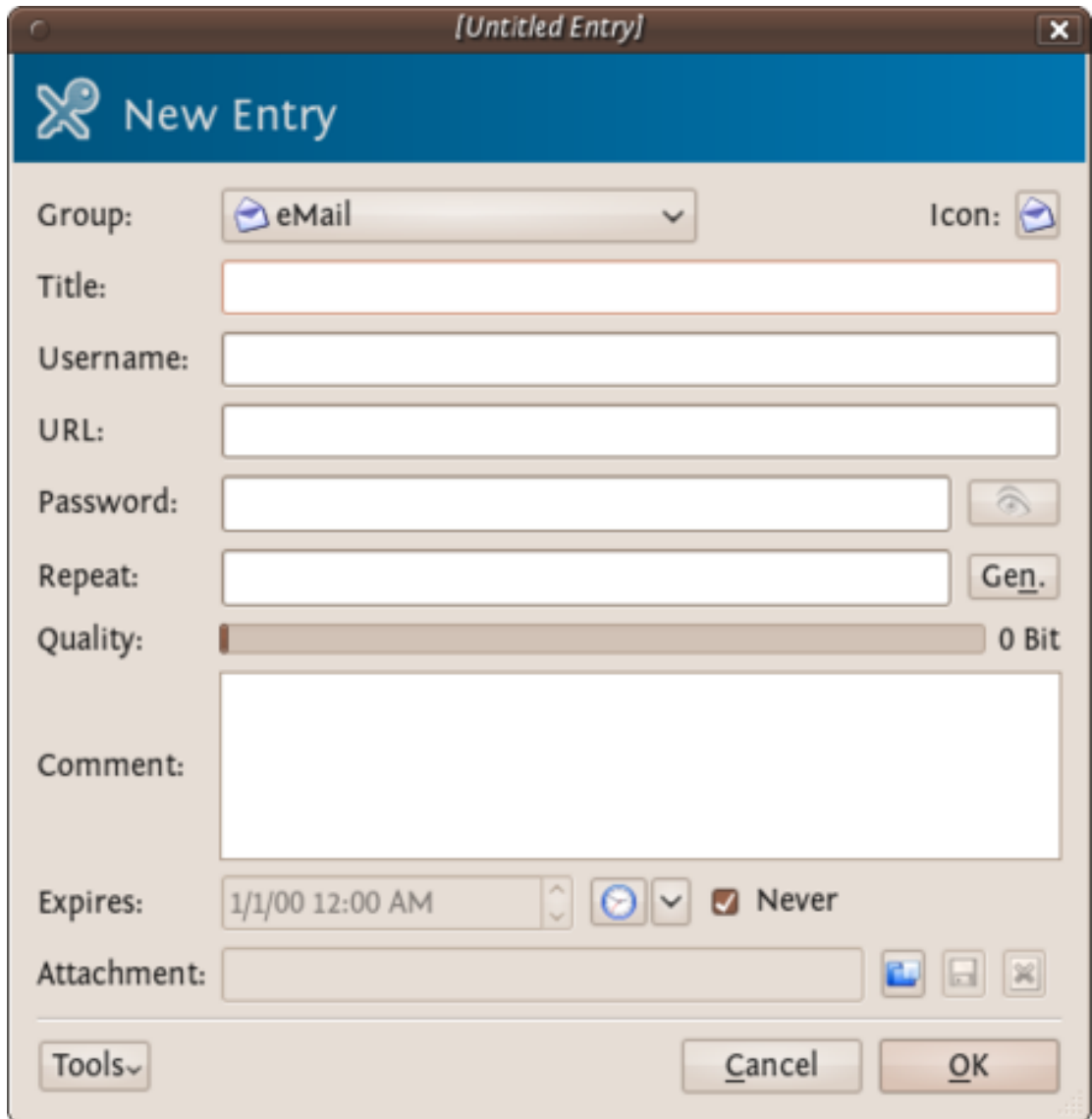


Figure 9.20: Password Manager

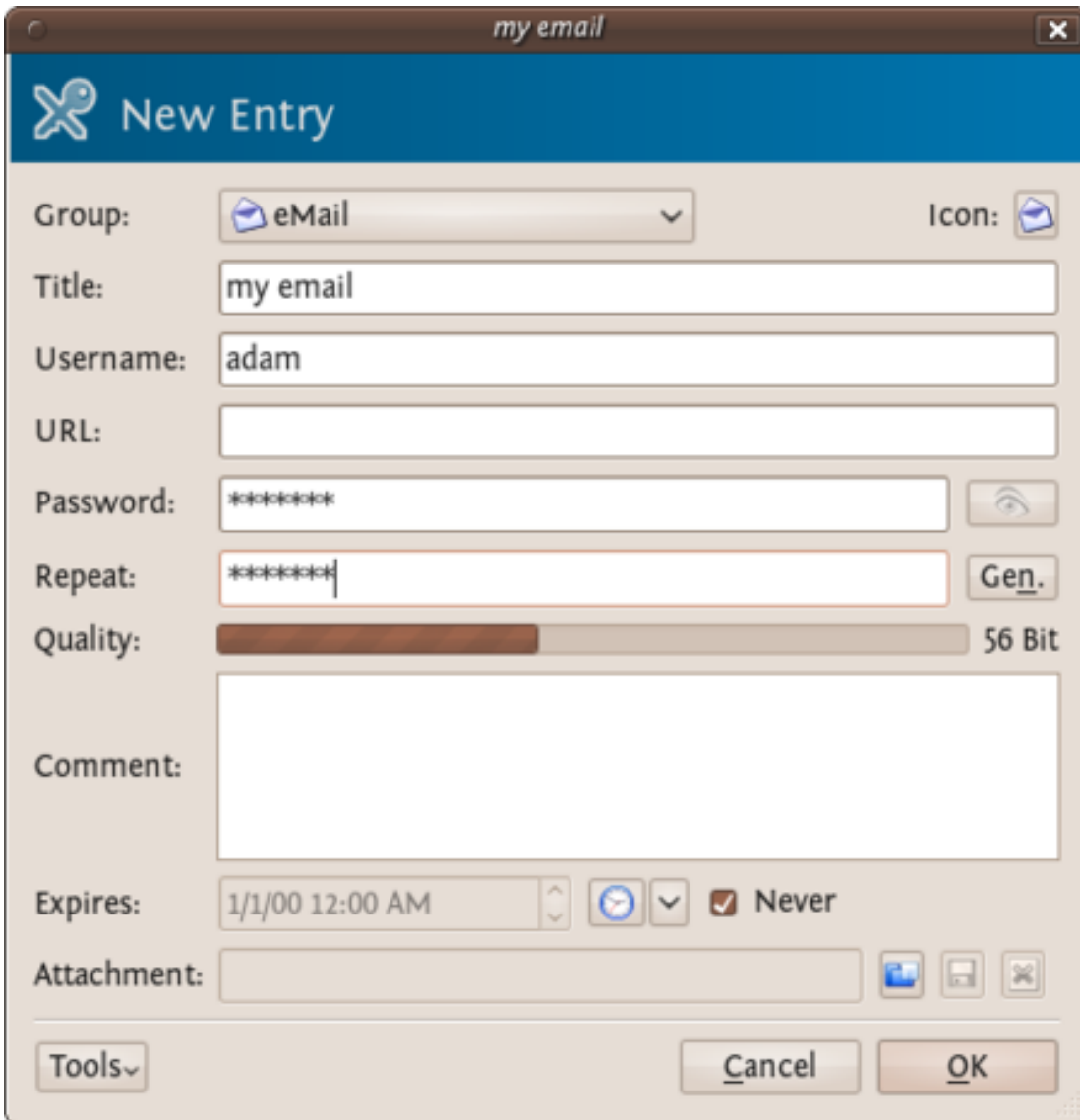


Figure 9.21: Password Manager

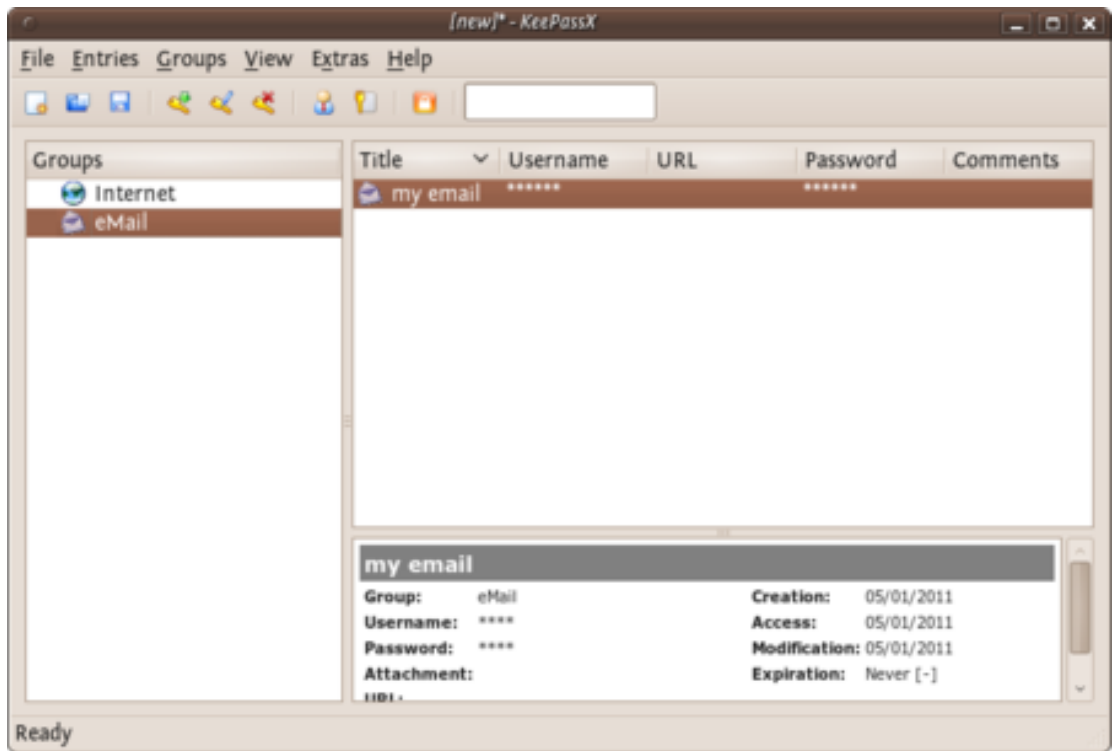


Figure 9.22: Password Manager

asks you if you would like to save the changes you have made.

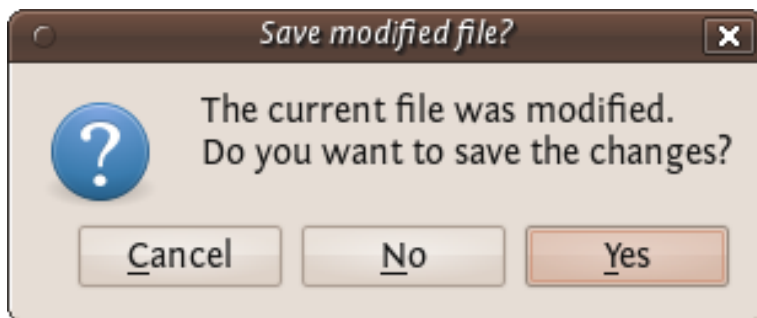


Figure 9.23: Password Manager

Press ‘Yes’. If it is the first time you used KeePassX (or you have just created a new database) you must choose a place to store your passwords. Otherwise it will save the updated information in the file you have previously created.

When you want to access the passwords you must then open KeePassX and you will be asked for the master key. After typing this in you can add all your passwords to the database and see all your entries. It is not a good idea to open KeePassX and have it open permanently as then anyone could see your passwords if they can access your computer. Instead get into the practice of just opening it when you need it and then closing it again.

9.3.2 Encrypting Passwords with KeePass on Windows

After you installed KeePass on Windows you can find it in the application menu. Launch the application and the following window should appear.

You start by making a database, the file which will contain your key. From the menu select **File > New**. You have to choose the name and the location of the file in the dialog window below. In this example we call our database `my_password_database`.

The next screen will ask you for the master password. Enter the password and click on ‘OK’. You will not need to select anything else.

The next window allows you to configure your new database. We do not need to edit anything. Just click on ‘OK’.

Now the main window appears again and we see some default password categories on the left side. Lets add a new password in the category ‘Internet’. First click on the word ‘Internet’, then click on the add entry icon under the menu bar.

A window will appear like below. Use the fields to give a description of this particular password, and of course, enter the password itself. When done, click on ‘OK’.

9 Passwords

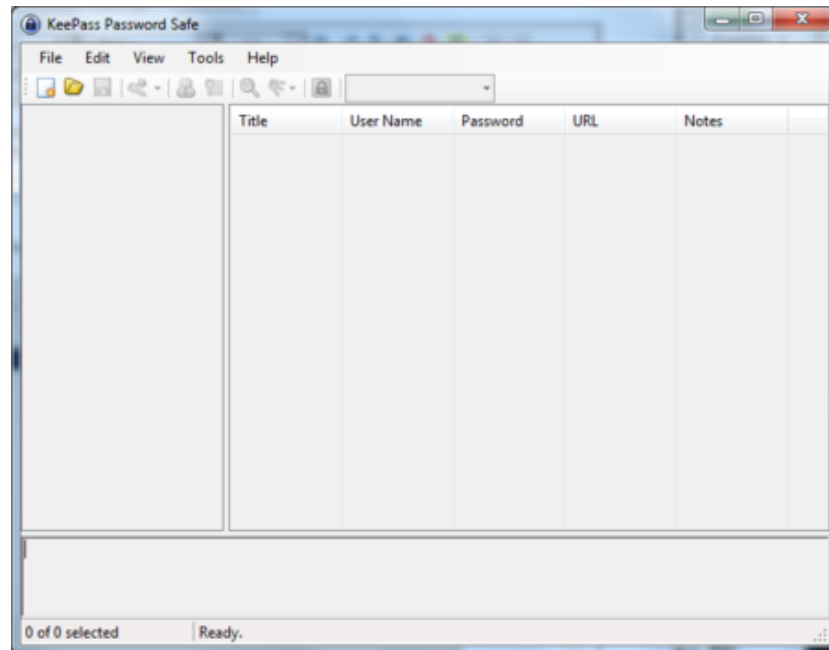


Figure 9.24: Password Manager

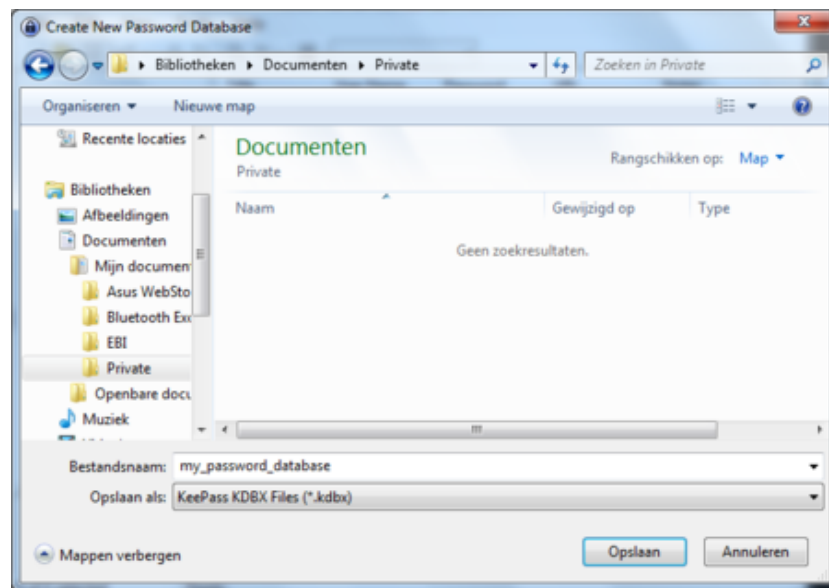


Figure 9.25: Password Manager

9.3 Encrypting Passwords with a Password Manager

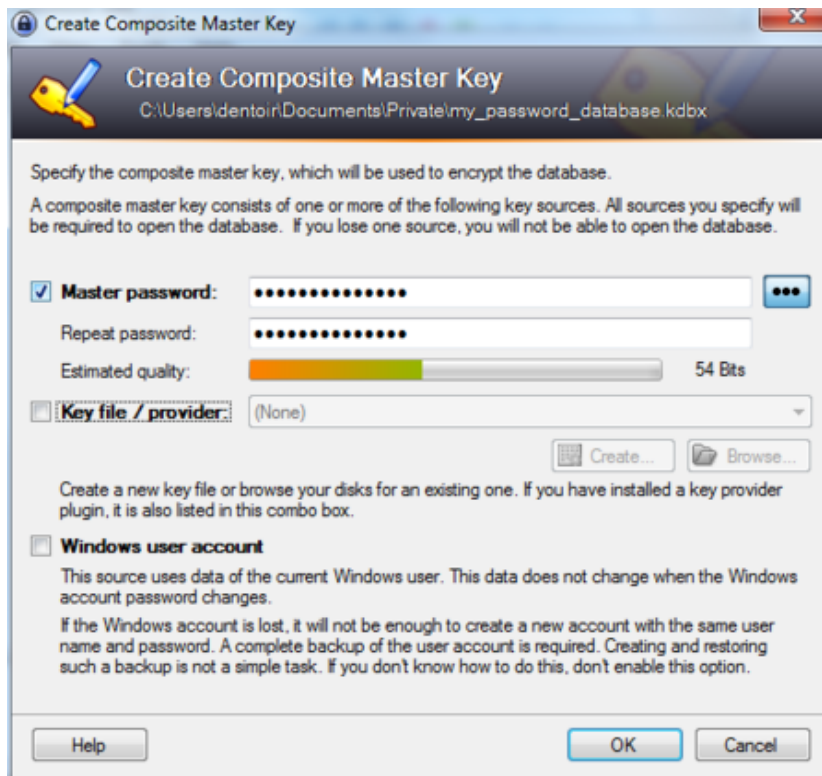


Figure 9.26: Password Manager

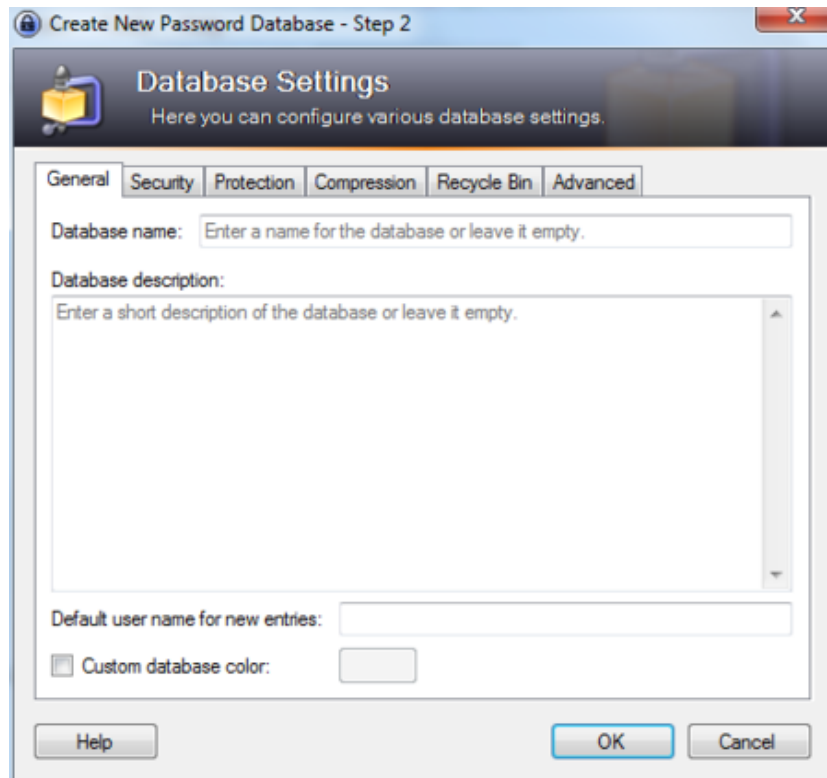


Figure 9.27: Password Manager

9.3 Encrypting Passwords with a Password Manager

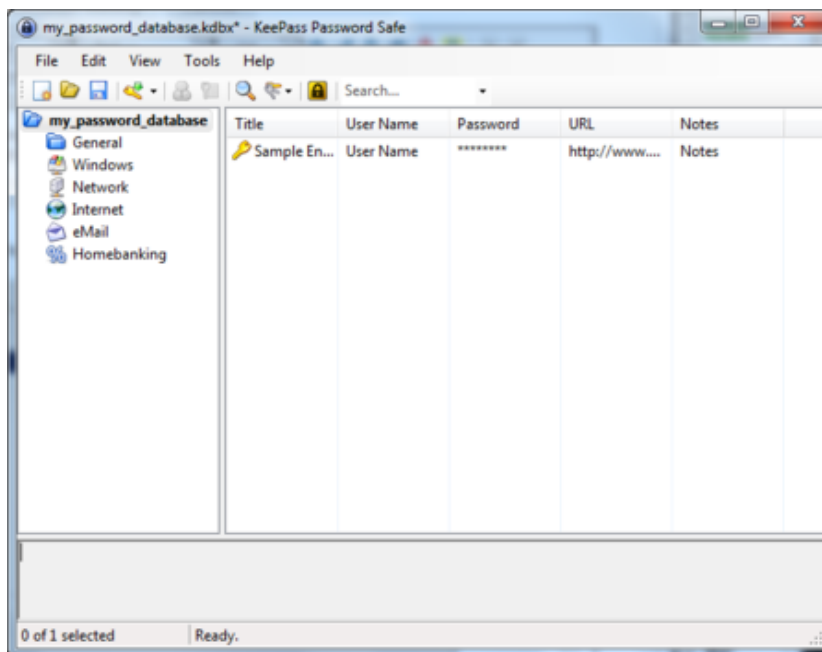


Figure 9.28: Password Manager

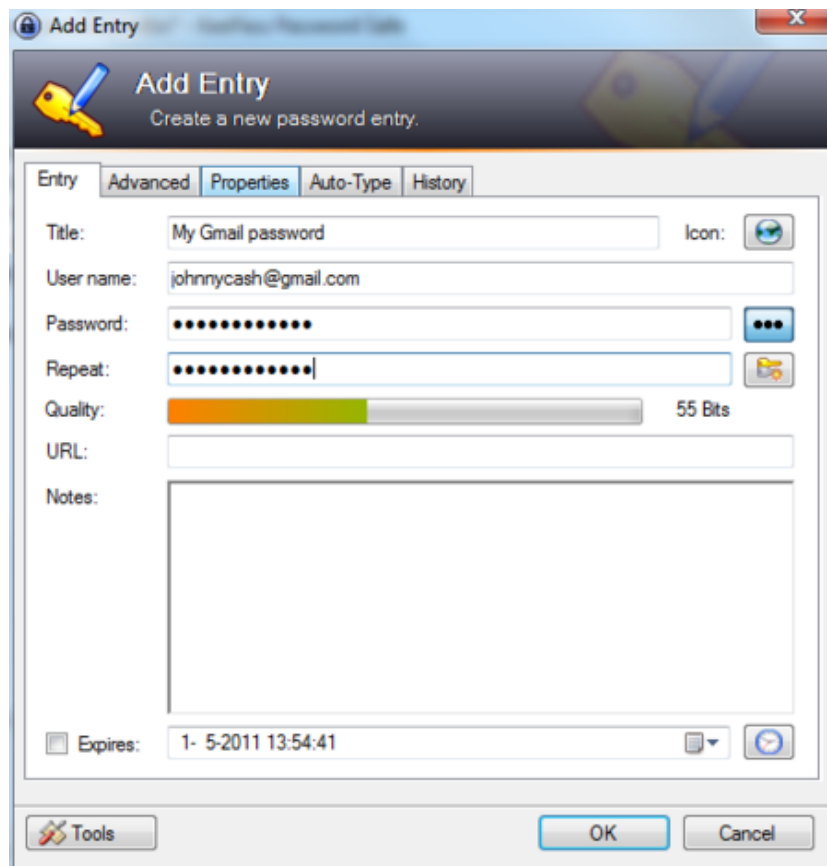


Figure 9.29: Password Manager

9.3.3 Encrypting Passwords with Keychain on Mac OSX

Mac OSX comes pre-installed with the built in password manager 'Keychain'. Because of its tight integration with the OS most of the time you will hardly know it exists. But every now and then you will have a pop-up window in almost any application asking 'do you want to store this password in your keychain?'. This happens when you add new email accounts to your mail client, login to a protected wireless network, enter your details in your chat client etc. etc. etc.

Basically what happens is that Mac OSX offers you to store all that login data and different passwords in an encrypted file which it unlocks as soon as you login to your account. You can then check your mail, logon to your WiFi and use your chat client without having to enter your login data all the time over and over again. This is a fully automated process, but if you want to see what is stored where and alter passwords, or lookup a password you will have to open the Keychain program.

You can find the Keychain program in the Utilities folder which lives in the Applications folder.

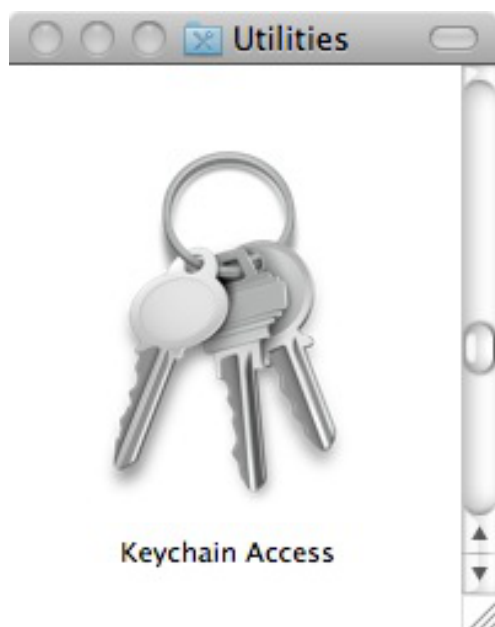


Figure 9.30: Password Manager

When you open it you will see that your 'Login' keychain is unlocked and see all the items contained in it on the right bottom side of the window.

(note: the window here is empty because it seemed to be deceiving the purpose of this manual to make a screenshot of my personal keychain items and share it here with you)

You can double click any of the items in the Keychain to view its details and tick 'Show password:' to see the password associated with the item.

You will note that it will ask you for your master or login password to view the item.

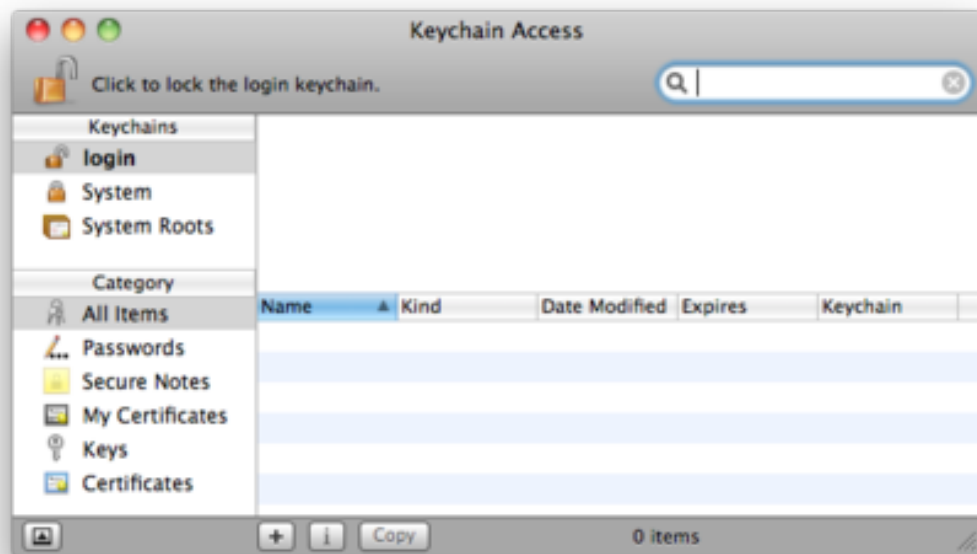


Figure 9.31: Password Manager

You can access modify any of the items and also use the Keychain to securely save any bits and pieces of text using the notes. To do this click on notes and than choose 'New secure Note item' from the file menu.

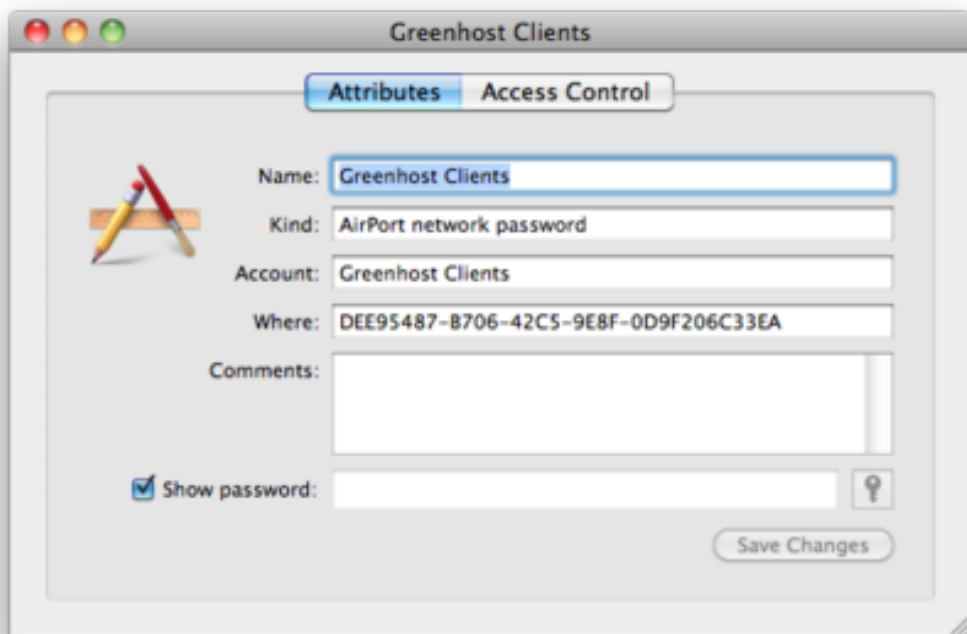


Figure 9.32: Password Manager

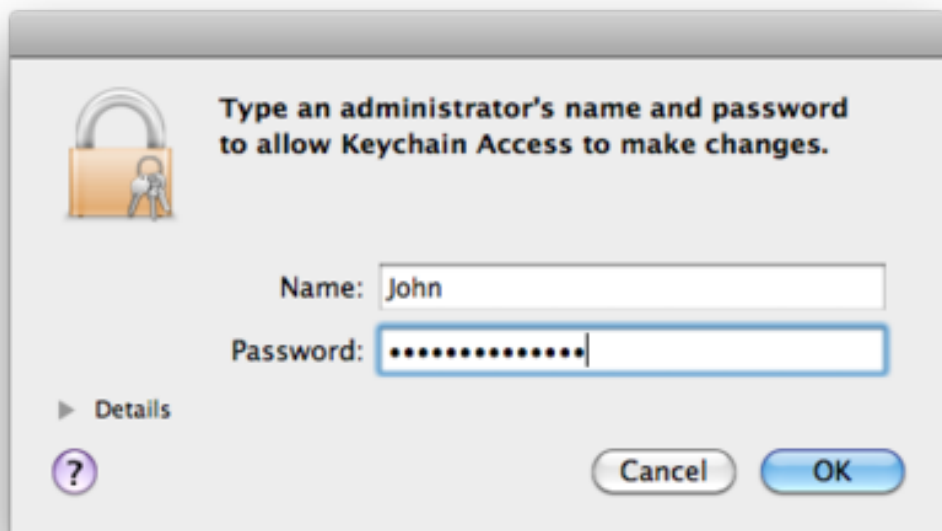


Figure 9.33: Password Manager

10 Using Vpn

10.1 Getting, setting-up and testing a VPN account

In all the VPN systems, there is one computer set up as a server (in an unrestricted location), to which one or more clients connect. The set up of the server is out of the scope of this manual and the set up of this system is in general covered by your VPN provider. This server is one of the two ends of the encrypted tunnel. It is important that the company running this server can be trusted and is located in an area you trust. So to run a VPN, an account is needed at such a trusted server.

Please keep in mind that an account can often only be used on one device at a time. If you want to use a VPN with both your mobile and laptop concurrently, it is very well possible you need two accounts.

10.1.1 An account from a commercial VPN provider

There are multiple VPN providers out there. Some will give you free trial time, others will begin charging right away at an approximate rate of €5 per month. Look for a VPN provider that offers OpenVPN accounts - it is an Open Source, trusted solution available for Linux, OS X, and Windows, as well as Android and iOS.

When choosing a VPN provider you need to consider the following points:

- Information that is required from you to register an account - the less that is needed the better. A truly privacy concerned VPN provider would only ask you for email address (make a temporary one!), username and password. More isn't required unless the provider creates a user database which you probably don't want to be a part of.
- Payment method to be used to pay for your subscription. Cash-transfer is probably the most privacy-prone method, since it does not link your bank account and your VPN network ID. Paypal can also be an acceptable option assuming that you can register and use a temporary account for every payment. Payment via a bank transfer or by a credit card can severely undermine your anonymity on and beyond the VPN.
- Avoid VPN providers that require you to install their own proprietary client software. There is a perfect open source solution for any platform, and having to run a "special" client is a clear sign of a phony service.
- Avoid using PPTP based VPNs, as several security vulnerabilities exist in that protocol. In fact, if two providers are otherwise equal, choose the one *not* offering PPTP if feasible.

- Look for a VPN provider that's using OpenVPN - an open source, multi-platform VPN solution.
- Exit gateways in countries of your interest. Having a choice of several countries allows you to change your geo-political context and appears to come from a different part of the world. You need to be aware of legislation details and privacy laws in that particular country.
- Anonymity policy regarding your traffic - a safe VPN provider will have a non-disclosure policy. Personal information, such as username and times of connection, should not be logged either.
- Allowed protocols to use within VPN and protocols that are routed to the Internet. You probably want most of the protocols to be available
- Price vs. quality of the service and its reliability.
- Any known issues in regard to anonymity of the users the VPN provider might have had in the past. Look online, read forums and ask around. Don't be tempted by unknown, new, cheap or dodgy offers.

There are several VPN review oriented places online that can help you make the right choice:

- <http://www.bestvpnservice.com/vpn-providers.php>
- <http://vpncreative.com/complete-list-of-vpn-providers>
- <http://en.cship.org/wiki/VPN>

Setting up your VPN client

“OpenVPN [...] is a full featured SSL VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate GNU/Linux, OSX, Windows and environments. OpenVPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/or private cloud network resources and applications with fine-grained access control.” (<http://openvpn.net/index.php/access-server/overview.html>)

There is a number of different standards for setting up VPNs, including PPTP, L2TP/IPSec and **OpenVPN**. They vary in complexity, the level of security they provide, and which operating systems they are available for. Do not use PPTP as it has several security vulnerabilities. In this text we will concentrate on OpenVPN. It works on most versions of GNU/Linux, OSX, Windows. OpenVPN is TLS/SSL-based - it uses the same type of **encryption** that is used in HTTPS (Secure HTTP) and a myriad of other encrypted protocols. OpenVPN encryption is based on **RSA** key exchange algorithm. For this to work and in order to communicate, both the server and the client need to have public and private RSA keys.

Once you obtain access to your VPN account the server generates those keys and you simply need to download those from the website of your VPN provider or have them sent

to your email address. Together with your keys you will receive a *root certificate (*.ca)* and a *main configuration file (*.conf or *.ovpn)*. In most cases only the following files will be needed to configure and run an OpenVPN client:

- **client.conf** (or `client.ovpn`) - configuration file that includes all necessary parameters and settings. NOTE: in some cases certificates and keys can come embedded inside the main configuration file. In such a case the below mentioned files are not necessary.
- **ca.crt** (unless in configuration file) - root authority certificate of your VPN server, used to sign and check other keys issued by the provider.
- **client.crt** (unless in configuration file) - your client certificate, allows you to communicate with VPN server.

Based on a particular configuration, your VPN provider might require a username and password to authenticate your connection. Often, for convenience, these can be saved into a separate file or added to the main configuration file. In other cases, key-based authentication is used, and the key is stored in a separate file:

- **client.key** (unless in configuration file) - client authentication key, used to authenticate to the VPN server and establish an encrypted data channel.

In most cases, unless otherwise necessary, you don't need to change anything in the configuration file and (surely!) **do not edit key or certificate files!** All VPN providers have thorough instructions regarding the setup. Read and follow those guidelines to make sure your VPN client is configured correctly.

NOTE: Usually it's only allowed to use one key per one connection, so you probably shouldn't be using the same keys on different devices at the same time. Get a new set of keys for each device you plan to use with a VPN, or attempt to set up a local VPN gateway (advanced, not covered here).

Download your OpenVPN configuration and key files copy them to a safe place and proceed to the following chapter.

10.1.2 Setting up OpenVPN client

In the following chapters some examples are given for setting up OpenVPN client software. On any flavor of GNU/Linux use your favorite package manager and install **openvpn** or **openvpn-client** package.

If you want to use OpenVPN on Windows or OSX, have look at:

- <http://openvpn.se> (Windows interface)
- <http://code.google.com/p/tunnelblick> (OSX interface)

10.1.3 Caveats & Gotchas

Although a VPN will obfuscate your IP address, due to the nature of most VPNs your TCP/IP stack meta-data and other identifying information will be sent across the wire as-is.

This may seem trivial, but consider, a standard IP header is 20 bytes in size, some of this is covered by required obvious information, (4 bytes for source IP, 4 bytes for destination IP), etc but some of this header may be other arbitrary options, the TCP header is at least 20 bytes also, with the potential for another 20 bytes of options. The specific configuration of these options varies between operating systems, and even versions of operating system, as such a single TCP SYN packet is often enough to identify a users operating system, version and other potentially revealing information, like the systems uptime. There are readily available tools which you can use to fingerprint this information, as a test, try connecting to a server running this tool with your normal internet connection, then connecting again over your VPN. You will most likely find that the fingerprints are an identicle match both with and without the VPN, and that if your friend were to connect their fingerprint would be different.

As such, it is important to remember some facts: * No one will go to jail for you, if your VPN provider is served a legal request for information about you, they will provide it. Just because they claim they don't log, does not mean they do not have logs. * VPNs provide privacy, they do not provide anonymity, regardless of the advertising and marketing materials provided.

10.2 VPN on Ubuntu

If you use Ubuntu as your operating system, you can connect to a VPN by using the built-in *NetworkManager*. This application is able to set up networks with OpenVPN. PPTP should not be used for security reasons. Unfortunately at the time of writing a L2TP interface is not available in Ubuntu. (It can be done manually, but it goes beyond the scope of this document).

The following example will explain how to connect with an OpenVPN-server. Under all situations we assume you already have a VPN account as described earlier in this section.

10.2.1 Preparing Network Manager for VPN networks

For Ubuntu there is an excellent network utility: Network Manager. This is the same utility you use to set up your Wireless (or wired) network and is normally in the upper right corner of your screen (next to the clock). This tools is also capable of managing your VPNs, but before it can do so, it's necessary to install some extensions.

Installing OpenVPN extension for Network Manager

To install the plugins for Network Manager we will use the Ubuntu Software Center.

1. Open the Ubuntu Software Center by typing software in the Unity search bar



Figure 10.1: VPN on Ubuntu

2. The Ubuntu Software Center enables you to search, install and remove software on your computer. Click on the search box at the top right of the window.
3. In the search box, type in “network-manager-openvpn-gnome” (which is the extension that will enable OpenVPN). It’s necessary to type the full names because the packages are classified as “technical” and don’t pop-up earlier. These packages include all the files you need to establish a VPN connection successfully.
4. Ubuntu may ask you for additional permissions to install the program. If that is the case, type in your password and click Authenticate. Once the package is installed, you can close the Software Center window.
5. To check if the extensions are correctly installed, click on the NetworkManager (the icon at the left of your system clock) and select VPN Connections > Configure VPN.
6. Click Add under the VPN tab.
7. If you see a pop-up asking for the type of VPN and the tunnel technology (OpenVPN) option is available, this means that you have installed the VPN extension in Ubuntu correctly. If you have your VPN login information ready, you can continue right away, else you first have to get a VPN account from a VPN-provider. If this is the case, click cancel to close the Network Manager.



Figure 10.2: VPN on Ubuntu

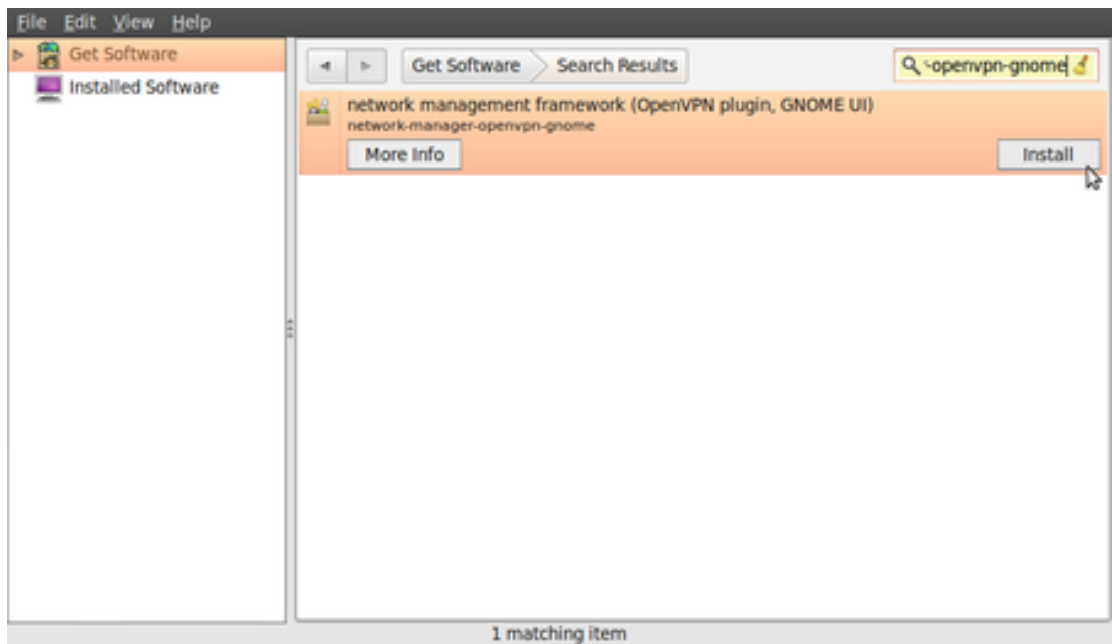


Figure 10.3: VPN on Ubuntu

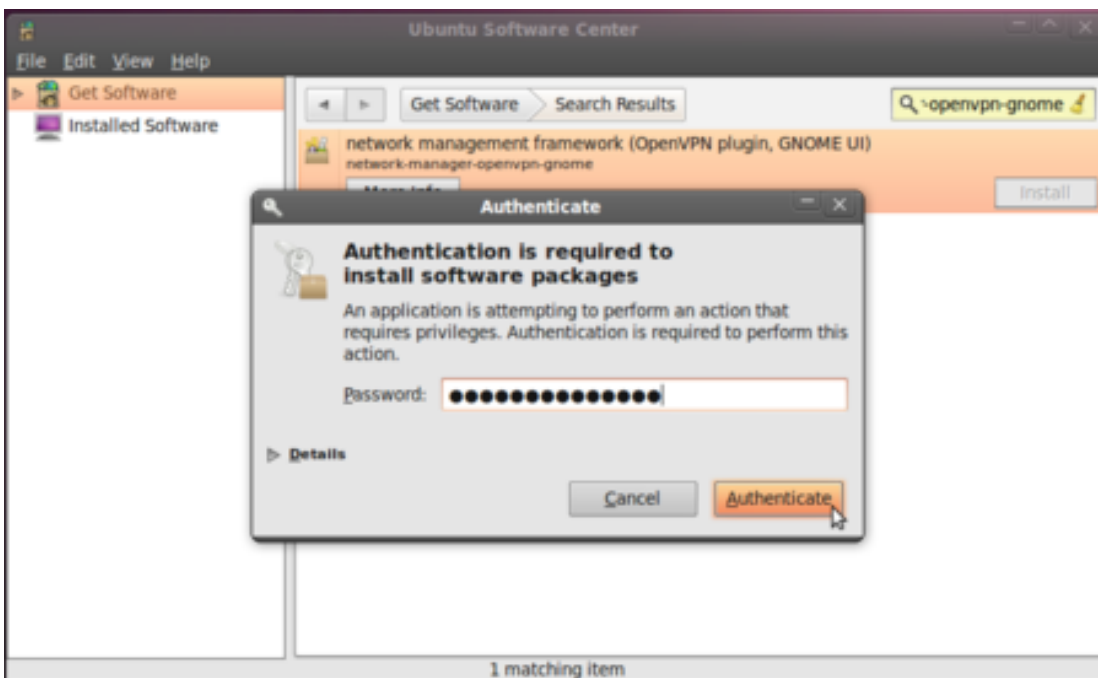


Figure 10.4: VPN on Ubuntu

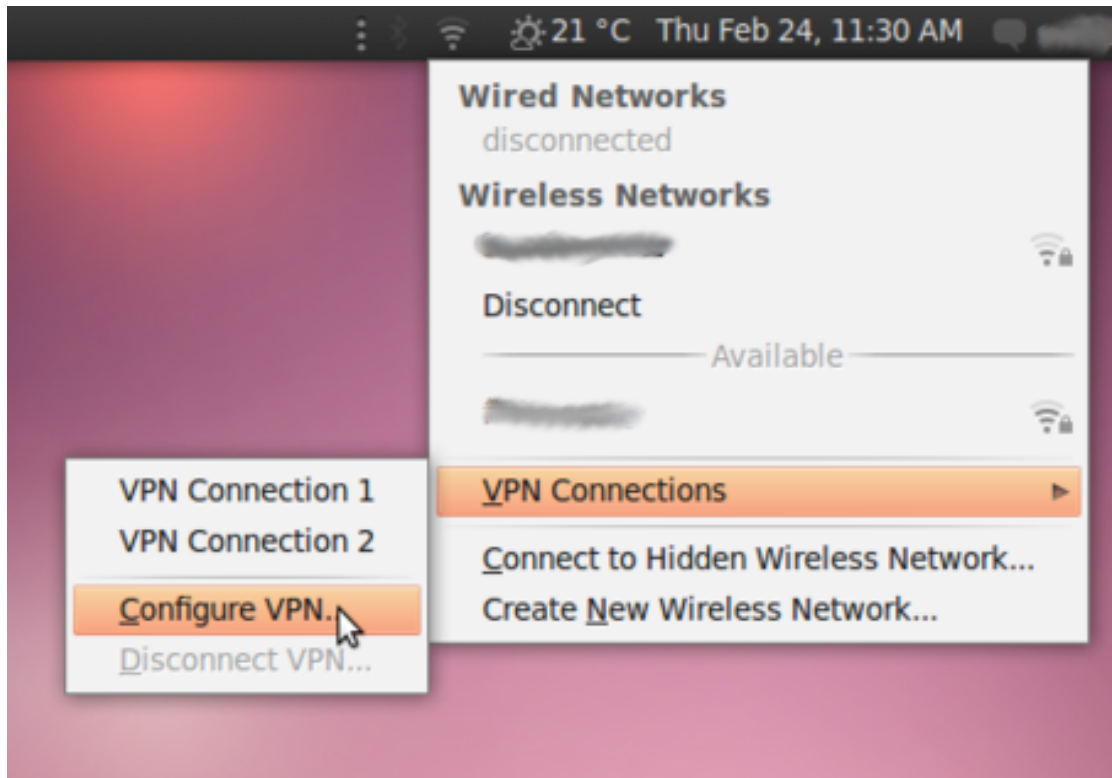


Figure 10.5: VPN on Ubuntu

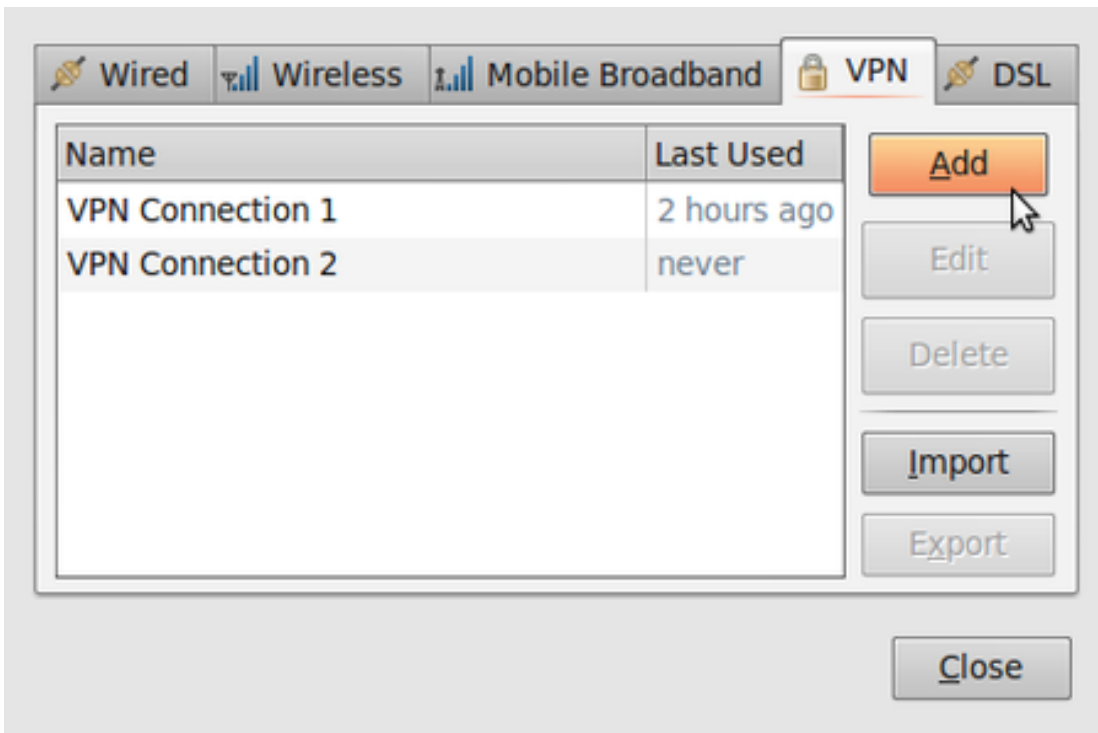


Figure 10.6: VPN on Ubuntu



Figure 10.7: VPN on Ubuntu

10.2.2 Configuring an OpenVPN network

Let us assume you have received your configuration files and credentials from your VPN provider. This information should contain the following

- an *.ovpn file, ex. air.ovpn
- The file: ca.crt (this file is specific for every OpenVPN provider)
- The file: user.crt (this file is your personal certificate, used for encryption of data)
- The file: user.key (this file contains your private key. It should be protected in a good manner. Losing this file will make your connection insecure)

In most cases your provider will send these files to you in a zip file. Some openvpn providers use username and password authentication which will not be covered.

1. Unzip the file you have downloaded to a folder on your hard drive (for example “/home/[yourusername]/.vpn”). You should now have four files. The file “air.ovpn” is the configuration file that you need to import into NetworkManager.

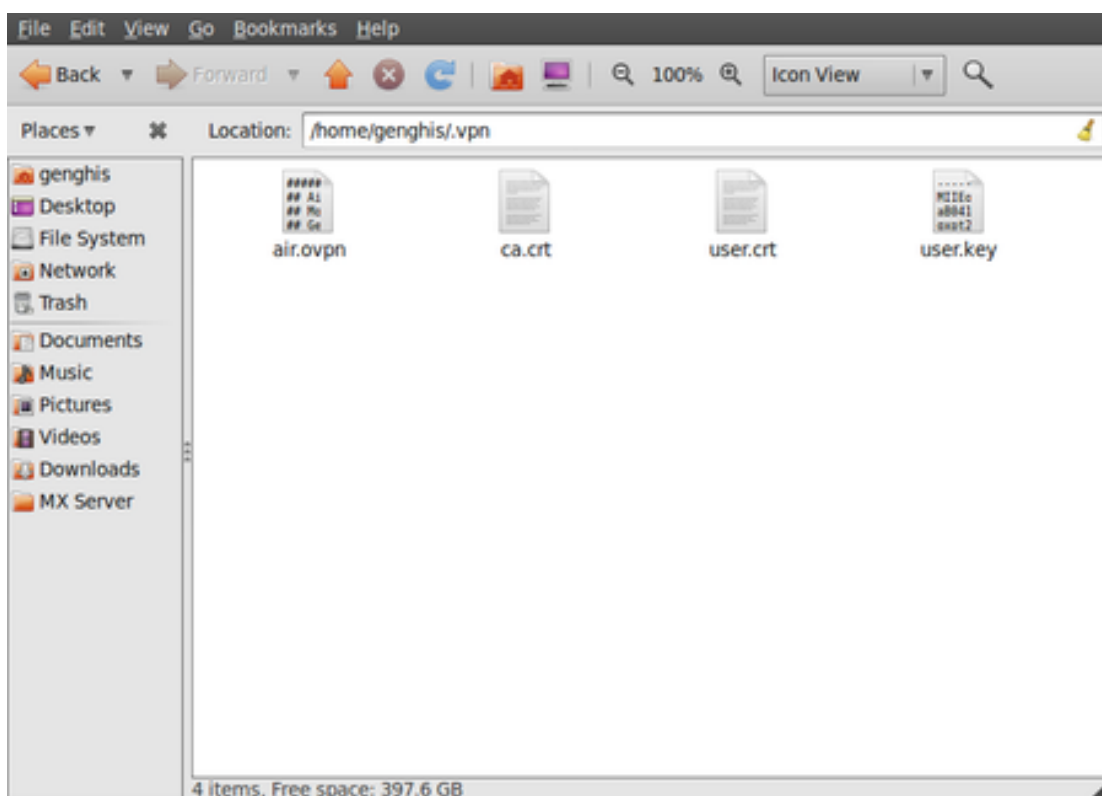


Figure 10.8: VPN on Ubuntu

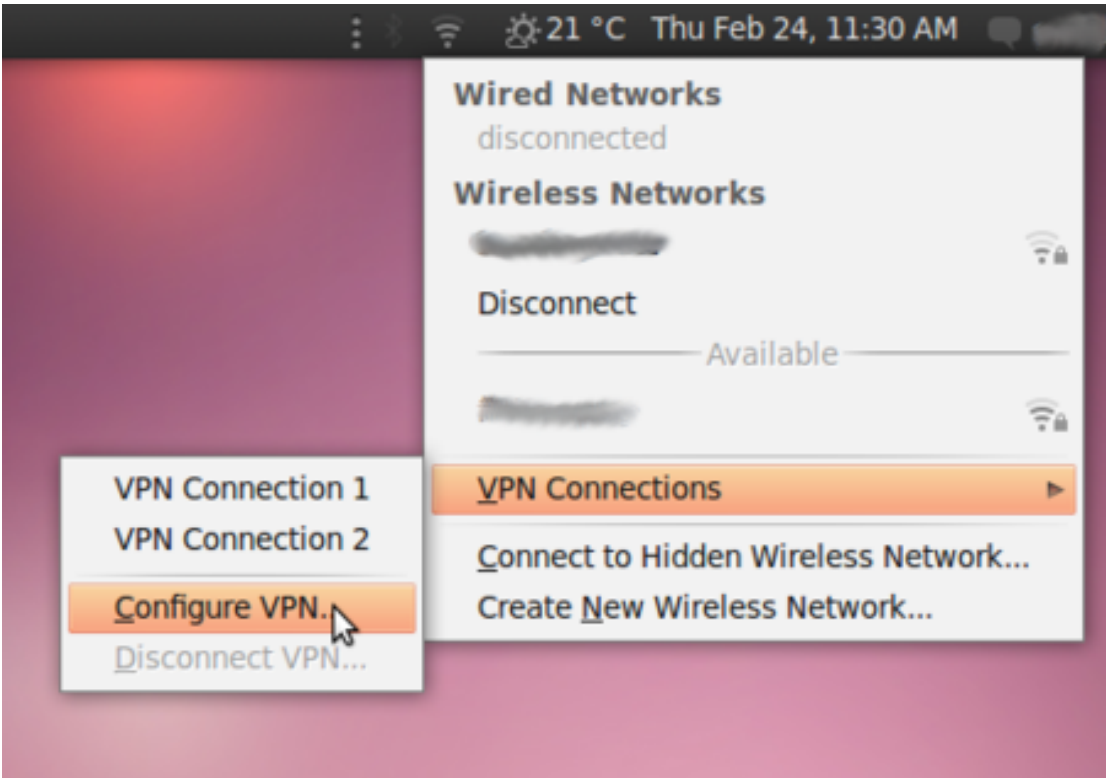


Figure 10.9: VPN on Ubuntu

10 Using Vpn

2. To import the configuration file, open NetworkManager and go to VPN Connections > Configure VPN.
3. Under the VPN tab, click Import.

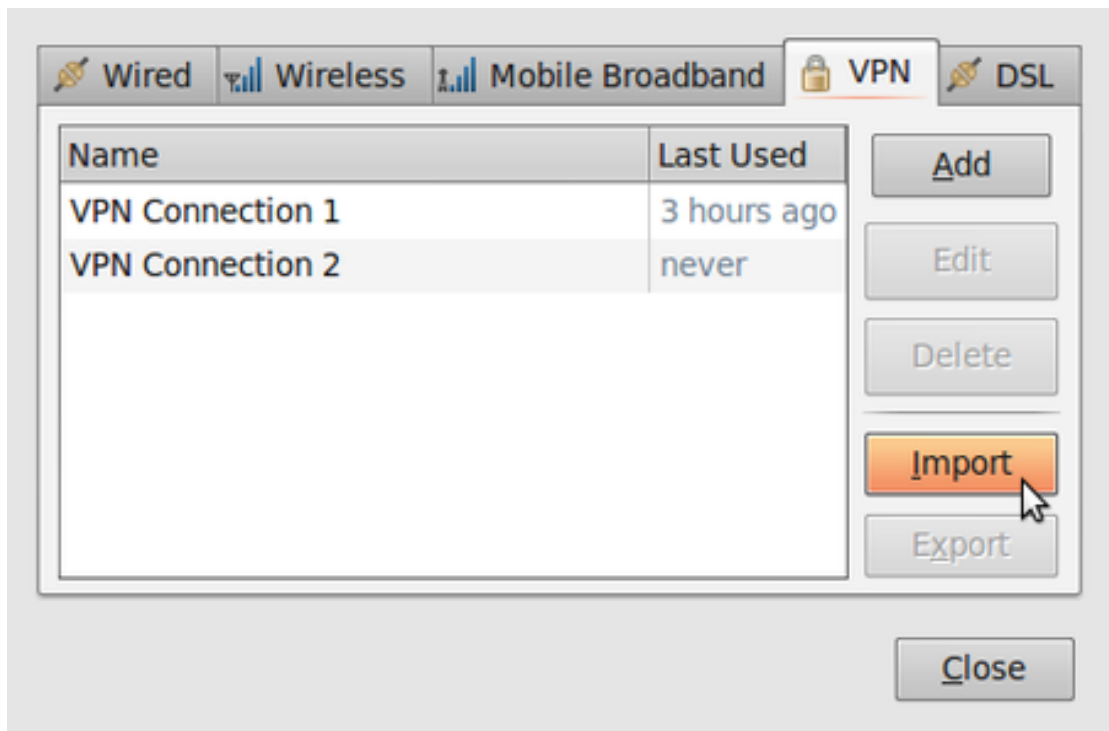


Figure 10.10: VPN on Ubuntu

4. Locate the file air.ovpn that you have just unzipped. Click Open.
5. A new window will open. Leave everything as it is and click Apply.
6. Congratulations! Your VPN connection is ready to be used and should appear on the list of connections under the VPN tab. You can now close NetworkManager.

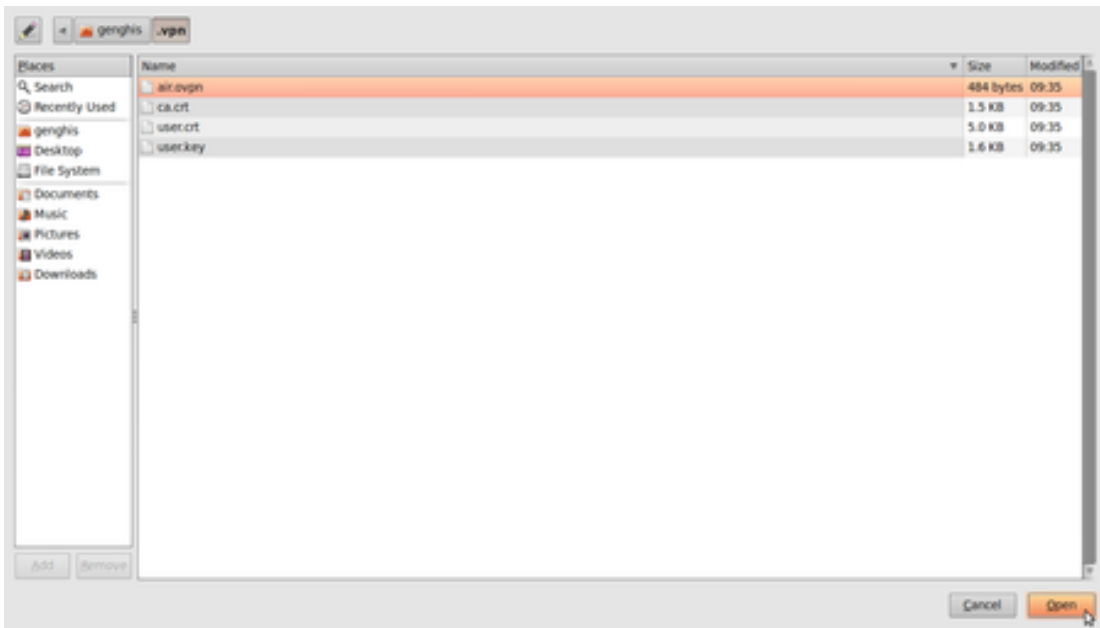


Figure 10.11: VPN on Ubuntu

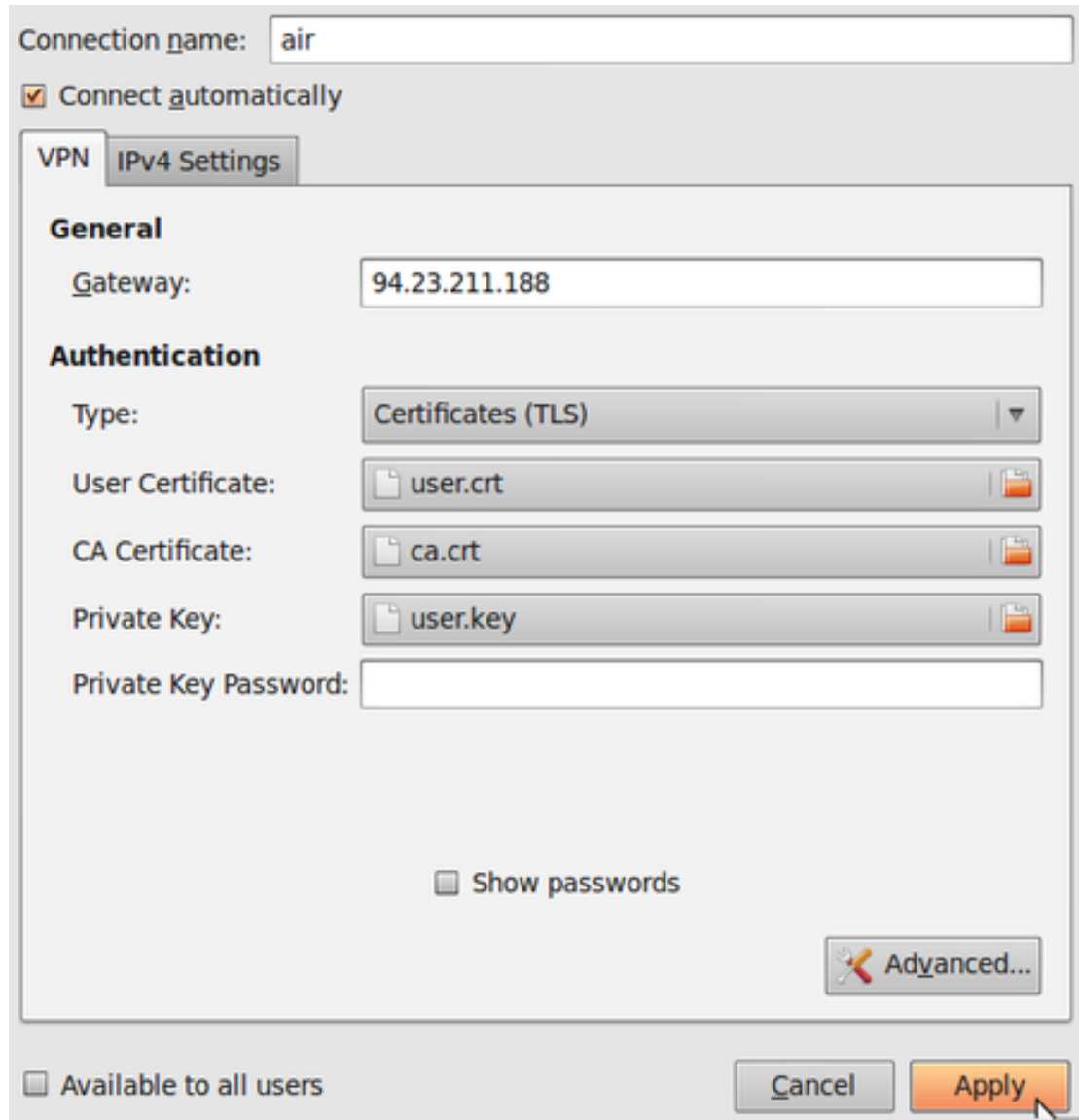


Figure 10.12: VPN on Ubuntu

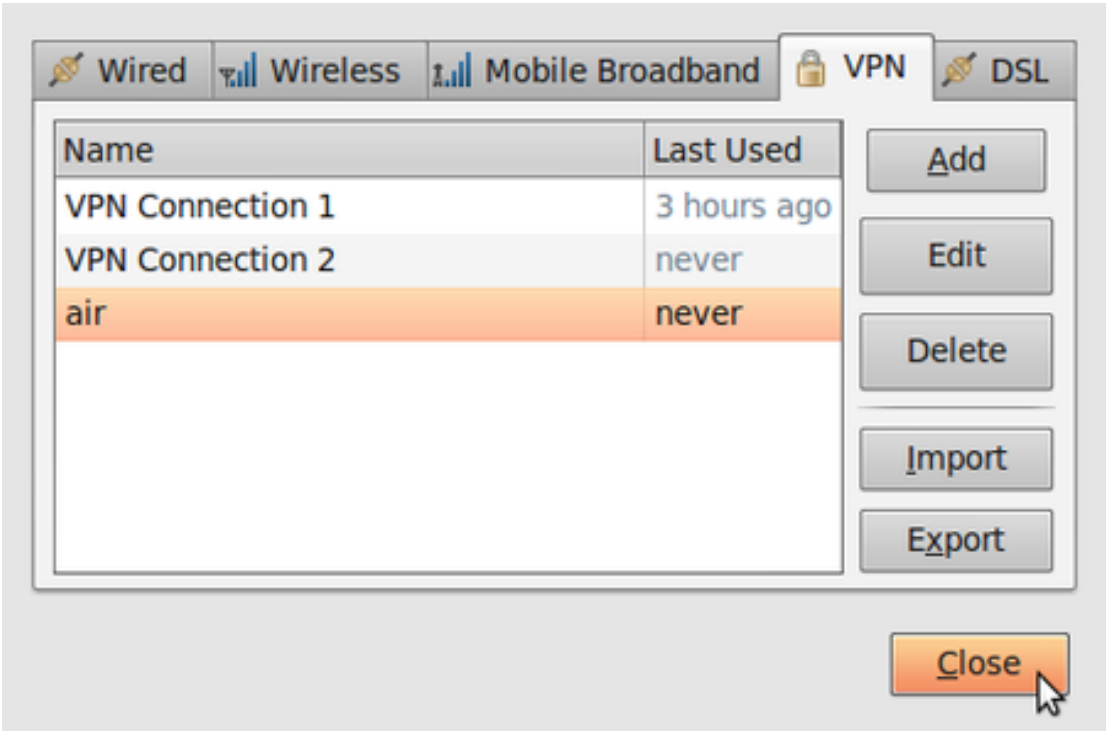


Figure 10.13: VPN on Ubuntu

10.2.3 Using your new VPN connection

Now that you configured NetworkManager to connect to a VPN service using the OpenVPN client, you can use your new VPN connection to circumvent Internet censorship. To get started, follow these steps:

1. In the NetworkManager menu, select your new connection from VPN Connections.

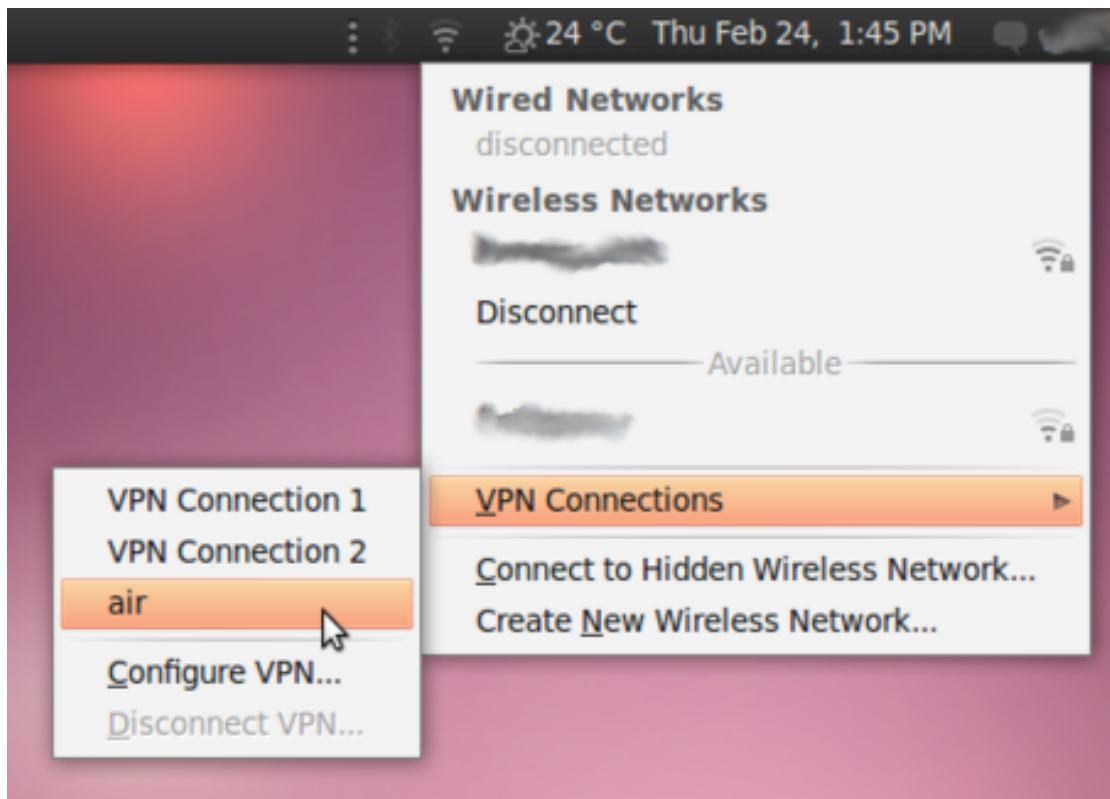


Figure 10.14: VPN on Ubuntu

2. Wait for the VPN connection to be established. When connected, a small padlock should appear right next to your NetworkManager icon, indicating that you are now using a secure connection. Move your cursor over the icon to confirm that the VPN connection is active.
3. Test your connection, using the method described in the “Make sure it works” section of this chapter.
4. To disconnect from your VPN, select VPN Connections > Disconnect VPN in the NetworkManager menu. You are now using your normal connection again.

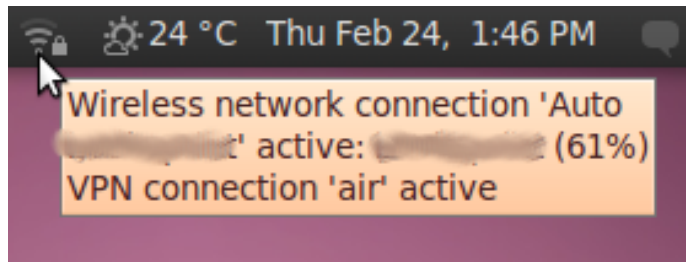


Figure 10.15: VPN on Ubuntu

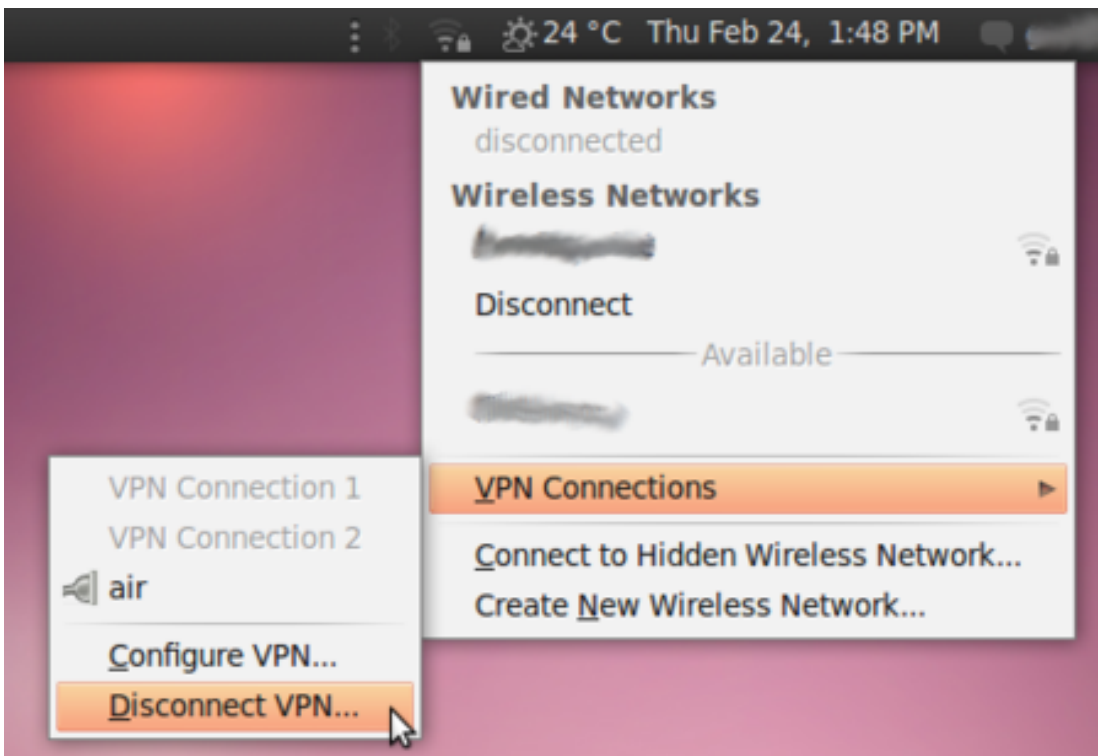


Figure 10.16: VPN on Ubuntu

10.3 VPN on MacOSX

Setting up a VPN on MacOSX is very easy once you have your account details ready, Let's assume have your credentials from your VPN provider for L2TP/IPSec connection ready. This information should contain the following:

- Username, ex. `bill2`
- Password, ex. `verysecretpassword`
- VPN server, ex. `tunnel.greenhost.nl`
- A Pre-Shared-Key or Machine-certificate

10.3.1 Setup

1. Before getting started, please be sure you've read the paragraph "testing before and after account set up", this way you will be able to validate if your connection is actually working after set up.
2. A VPN is configured in the network settings, that are accessible via "System Preferences.." in the Apple menu.
3. Next, open the Network preferences.
4. OSX uses this nifty system to lock windows. To add a VPN it is necessary to unlock the screen: you can do this by clicking on the lock on the left bottom of the screen.
5. Enter our user credentials
6. Now we can add a new network. Do this by clicking on the "+" sign
7. In the pop-up you need to specify the type of connection. In this case choose an VPN interface with L2TP over IPSec. This is the most common system. Also don't forget to give the connection a nice name.
8. Next comes the connection data. Please fill in the provided server name and user name (called 'Account Name'). If this is done, click on the "Authentication Settings..." button

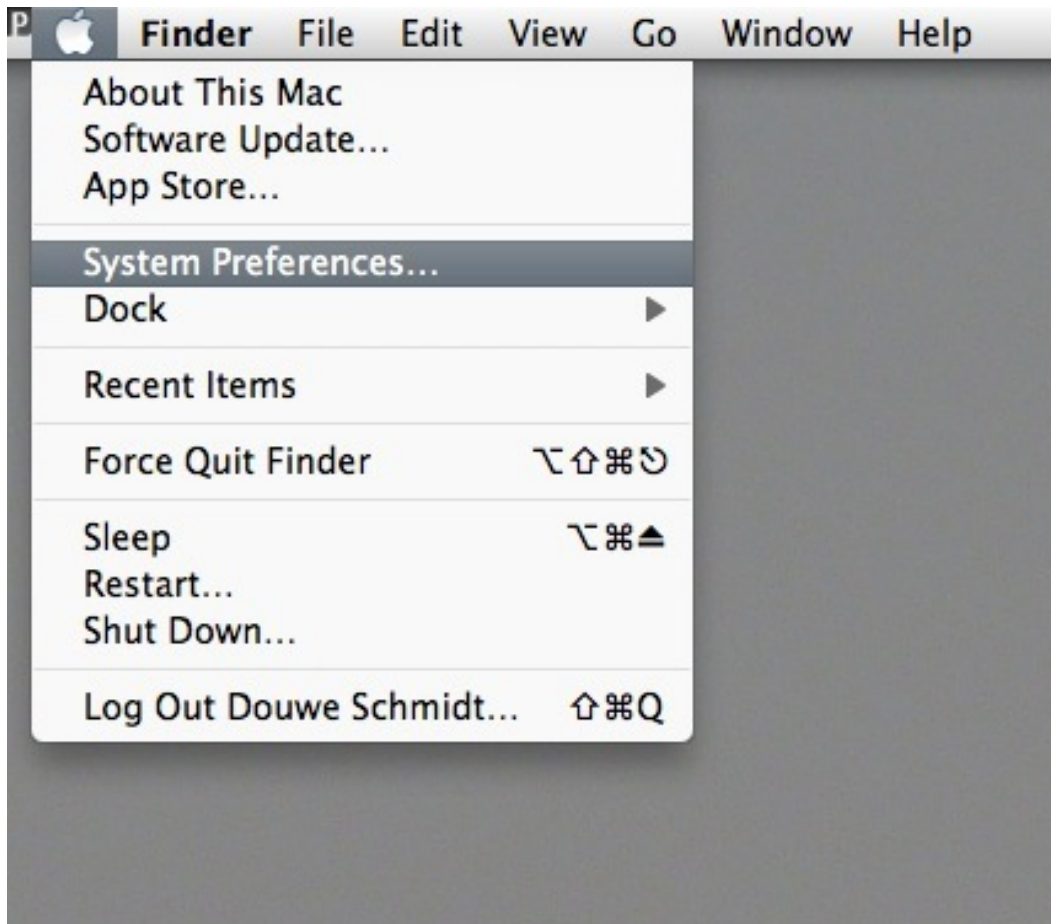


Figure 10.17: VPN on Mac OS X

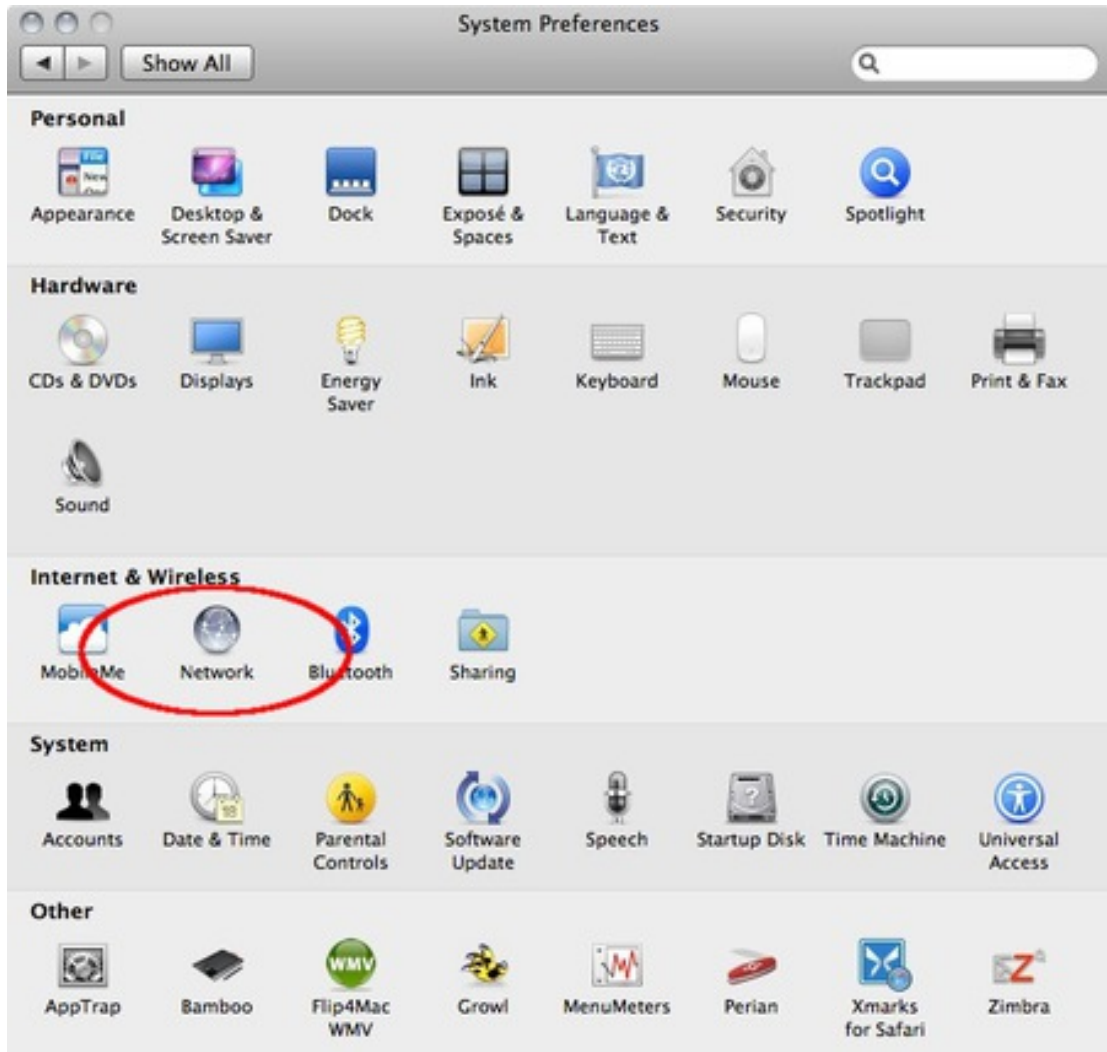


Figure 10.18: VPN on Mac OS X



Figure 10.19: VPN on Mac OS X

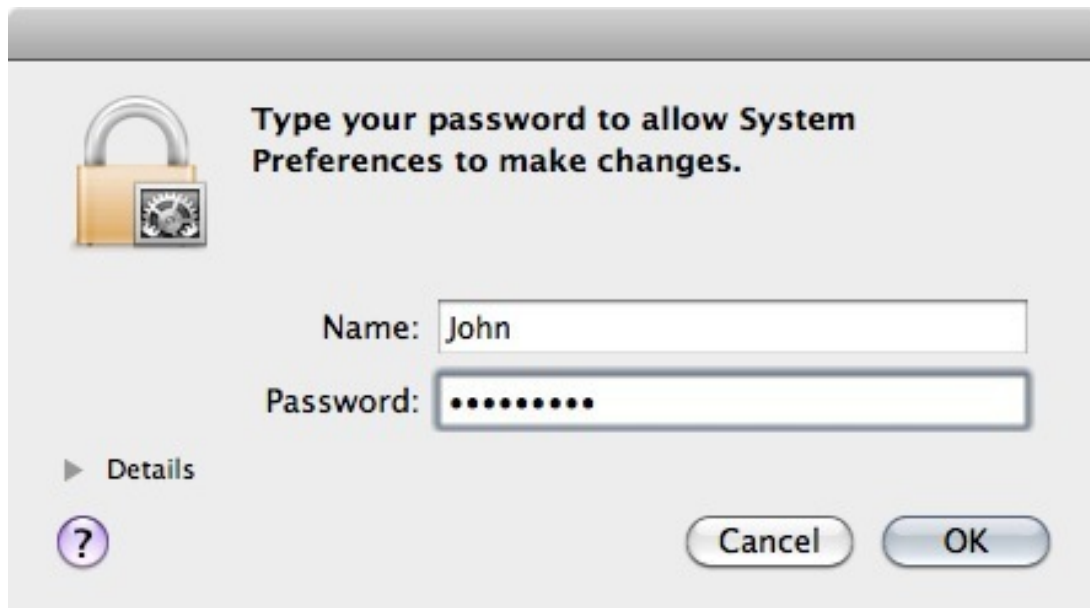


Figure 10.20: VPN on Mac OS X

9. In the new pop-up you can specify connection specific information. This is the way the user is authenticated and how the machine is authenticated. The user is very commonly authenticated by using a password, although other methods are possible. Machine authentication is often done by a Shared Secret (Pre-Shared-Key/PSK), but also quite often by using a certificate. In this case we use the Shared Secret method. When this is done click OK.
10. Now you return back to the network screen. The next step is very important, so click on “Advanced...”
11. In the new pop up you will see an option to route all traffic through the VPN connection. We want to enable this, so all our traffic is encrypted.
12. Well, all is done. Now hit the Connect button!
13. A pop-up appears. You need to confirm your changes, just hit “Apply”
14. After a few seconds, on the left side the connection should turn green. If so, you are connected!
15. Ok, now test your connection!

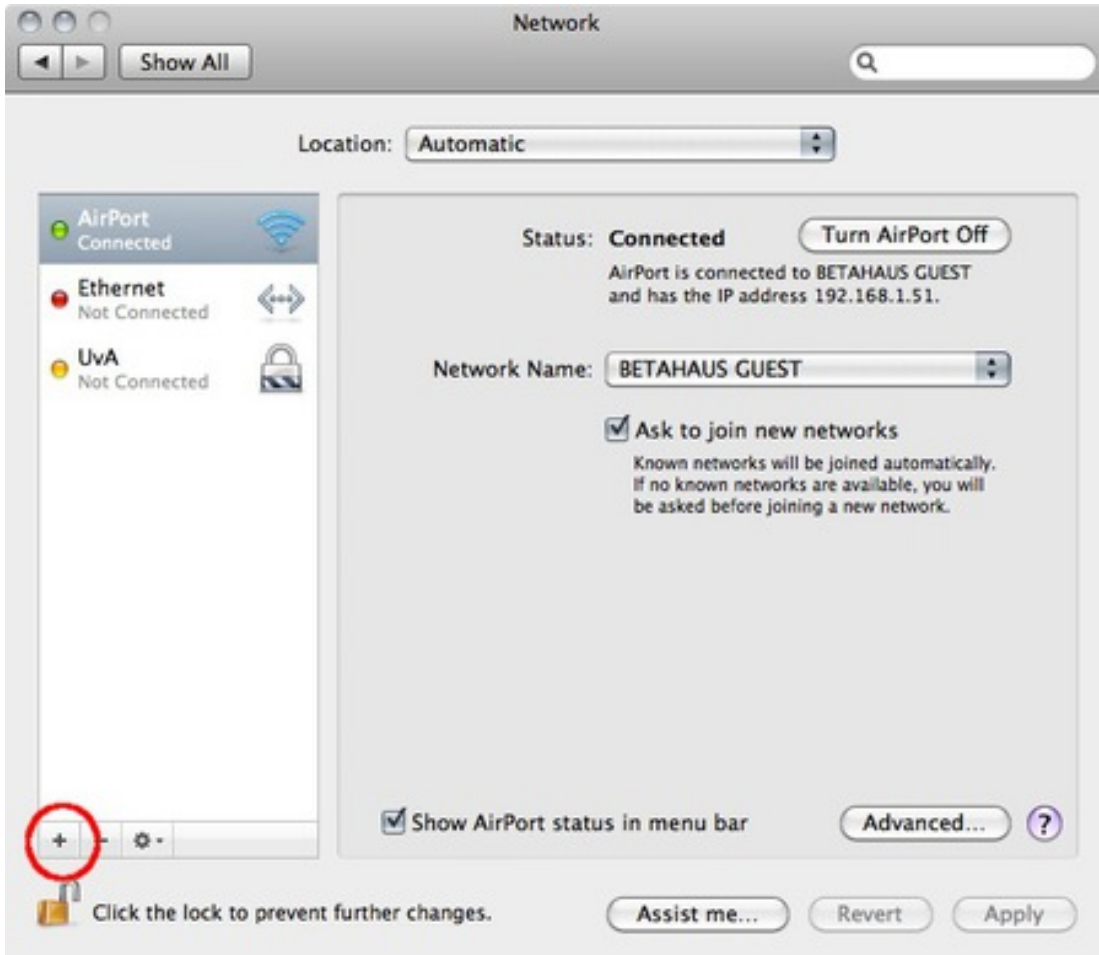


Figure 10.21: VPN on Mac OS X

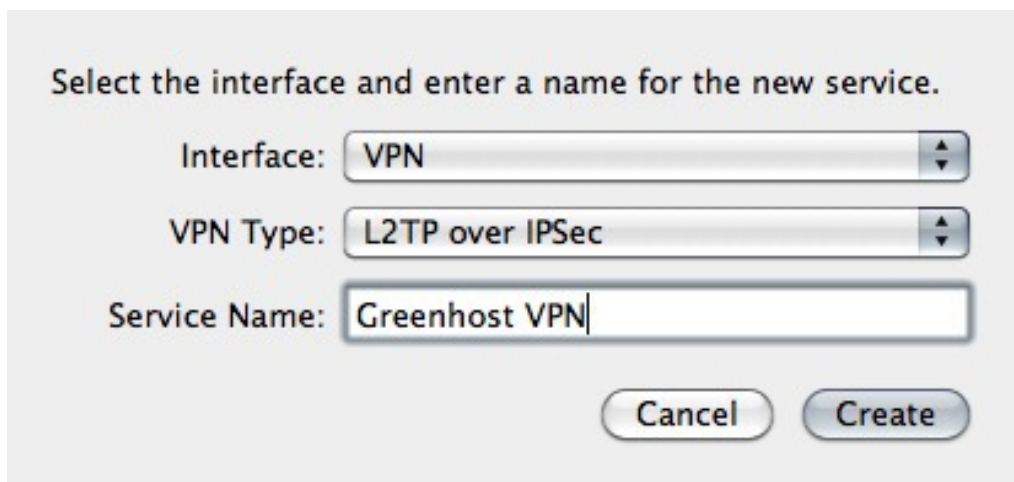


Figure 10.22: VPN on Mac OS X

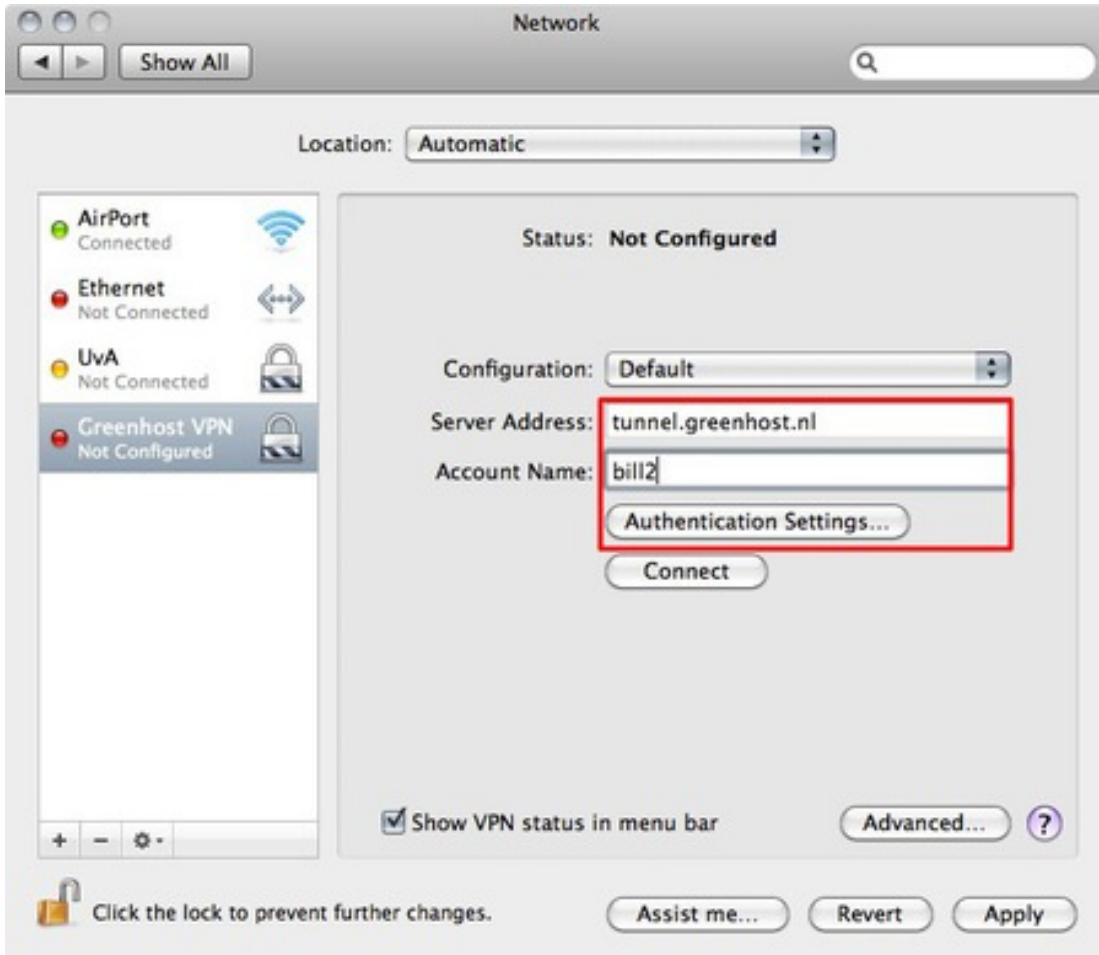


Figure 10.23: VPN on Mac OS X



Figure 10.24: VPN on Mac OS X

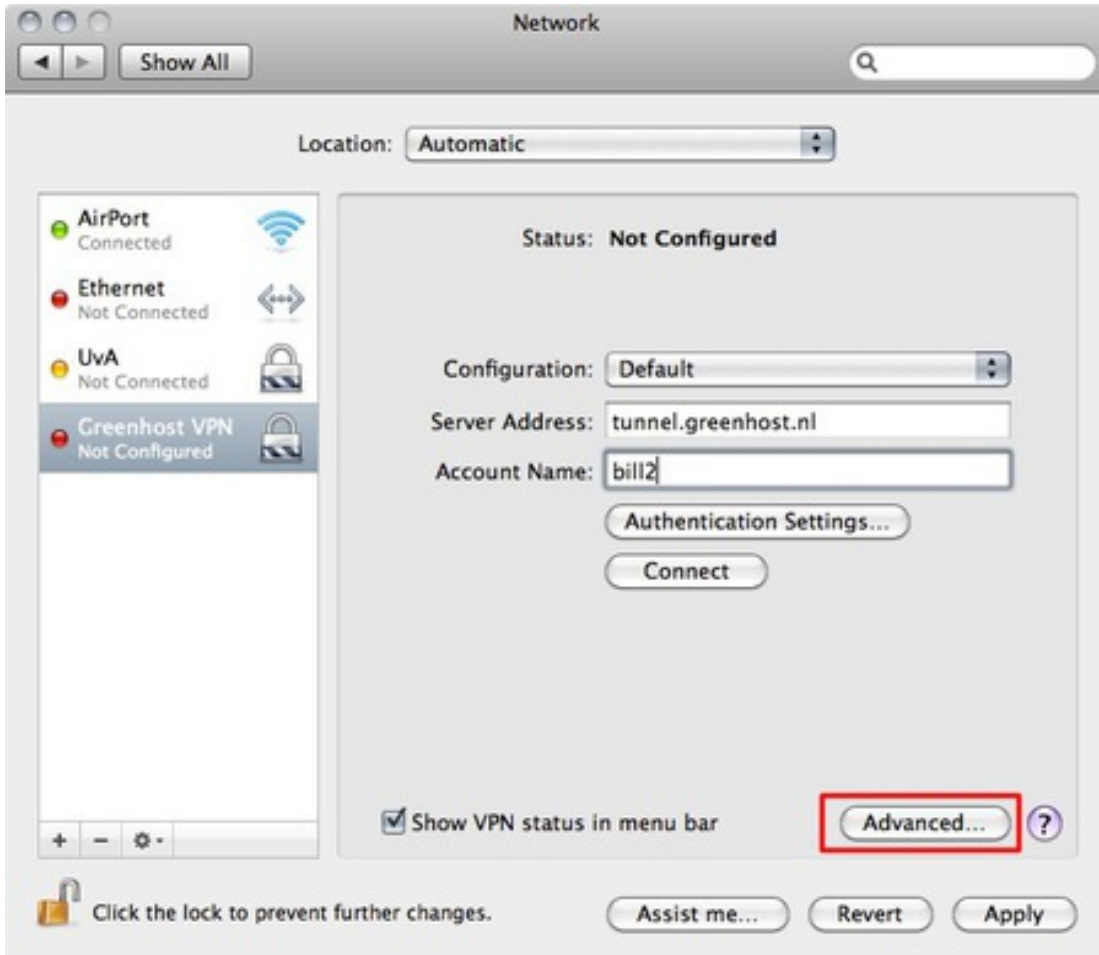


Figure 10.25: VPN on Mac OS X

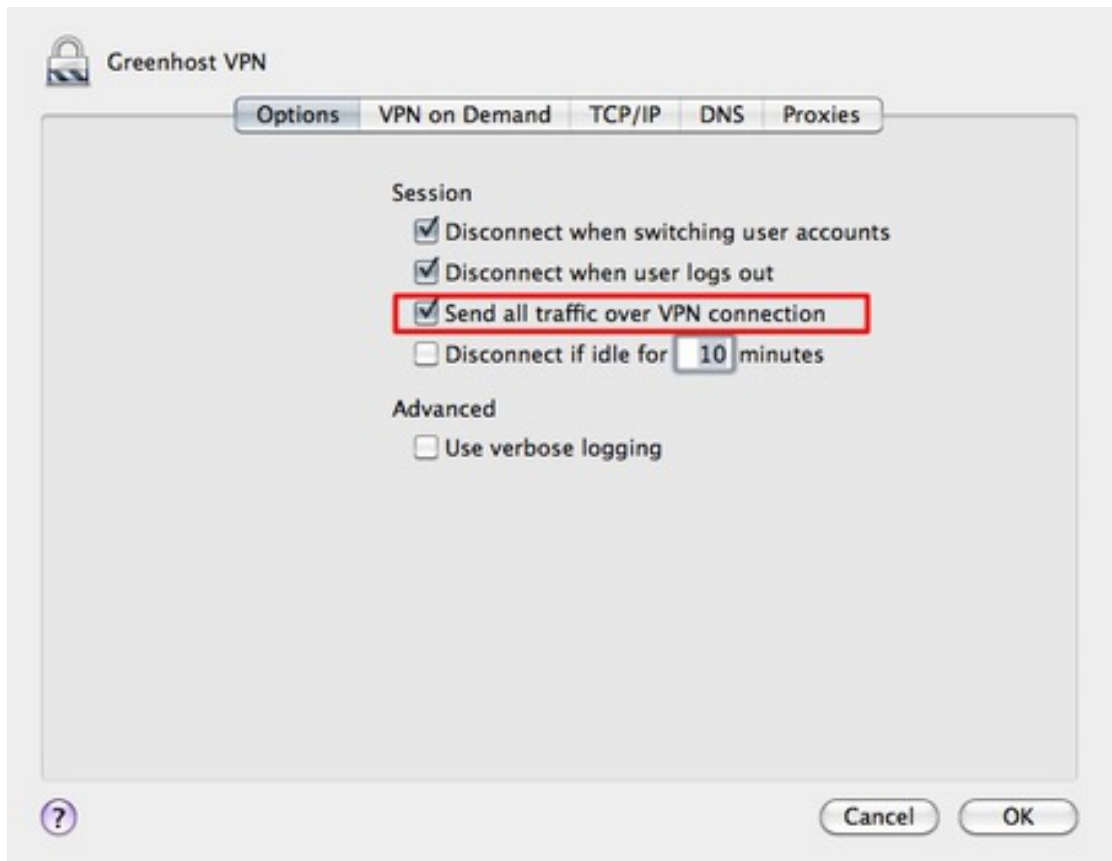


Figure 10.26: VPN on Mac OS X

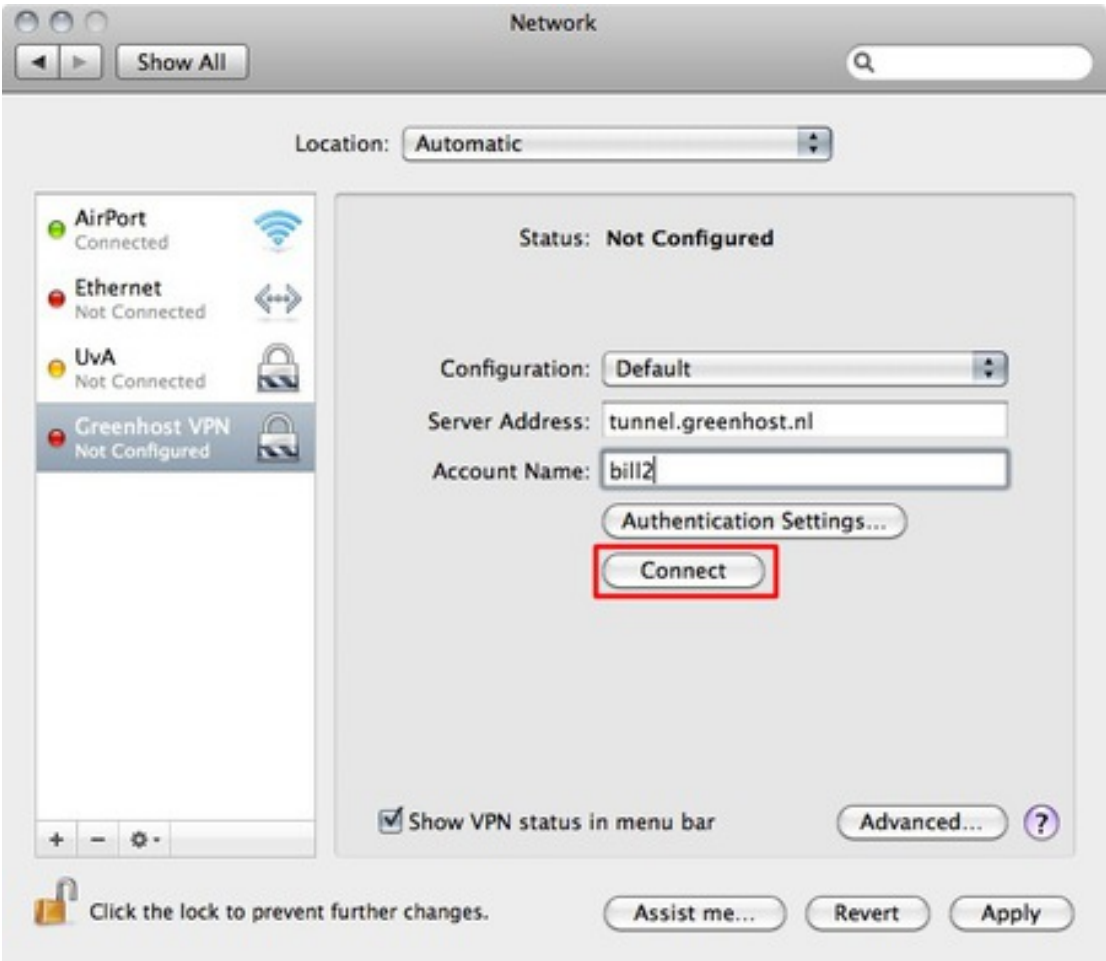


Figure 10.27: VPN on Mac OS X



Figure 10.28: VPN on Mac OS X

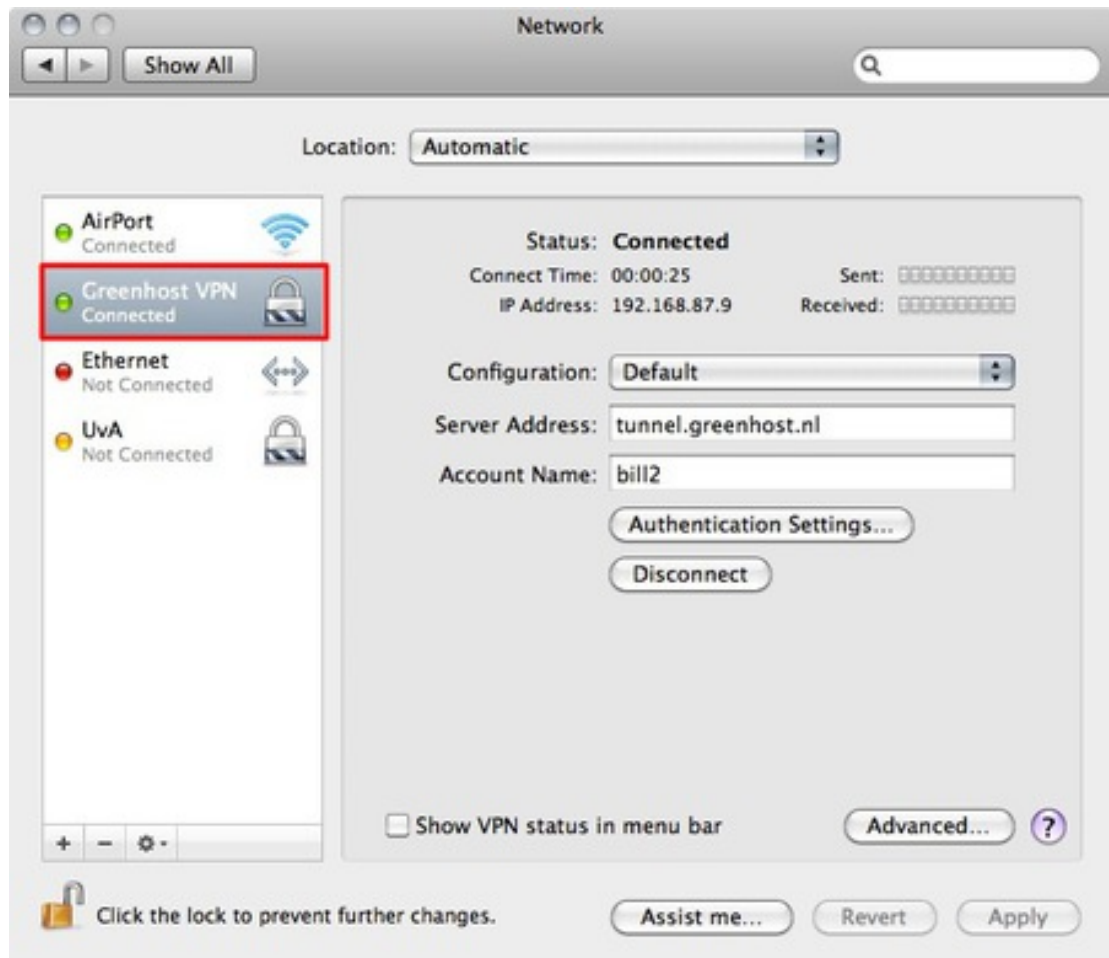


Figure 10.29: VPN on Mac OS X

10.4 VPN on Windows

Setting up a VPN on Windows is very easy once you have your account details ready. Let's assume have your credentials from your VPN provider for L2TP/IPSec connection ready. This information should contain the following:

- Username, ex. `bill12`
- Password, ex. `verysecretpassword`
- VPN server, ex. `tunnel.greenhost.nl`
- A Pre-Shared-Key or Machine-certificate

10.4.1 Setup

1. Before getting started, please be sure you've read the paragraph "testing before and after account set up", this way you will be able to validate if your connection is actually working after set up.
2. We need to go to the "Network and Sharing Center" of Windows to create a new VPN connection. We can access this center easily by clicking on the network icon next to the systemclock en click on "open Network and Sharing Center"

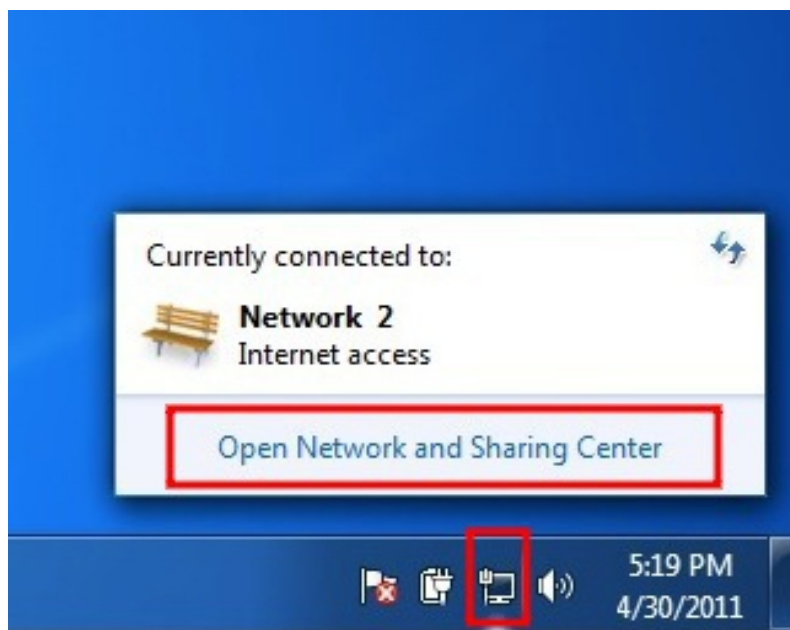


Figure 10.30: VPN on Windows

3. The "Network and Sharing Center" will popup. You will see some information about your current network. Click on "Connect to a network" to add a VPN connection.

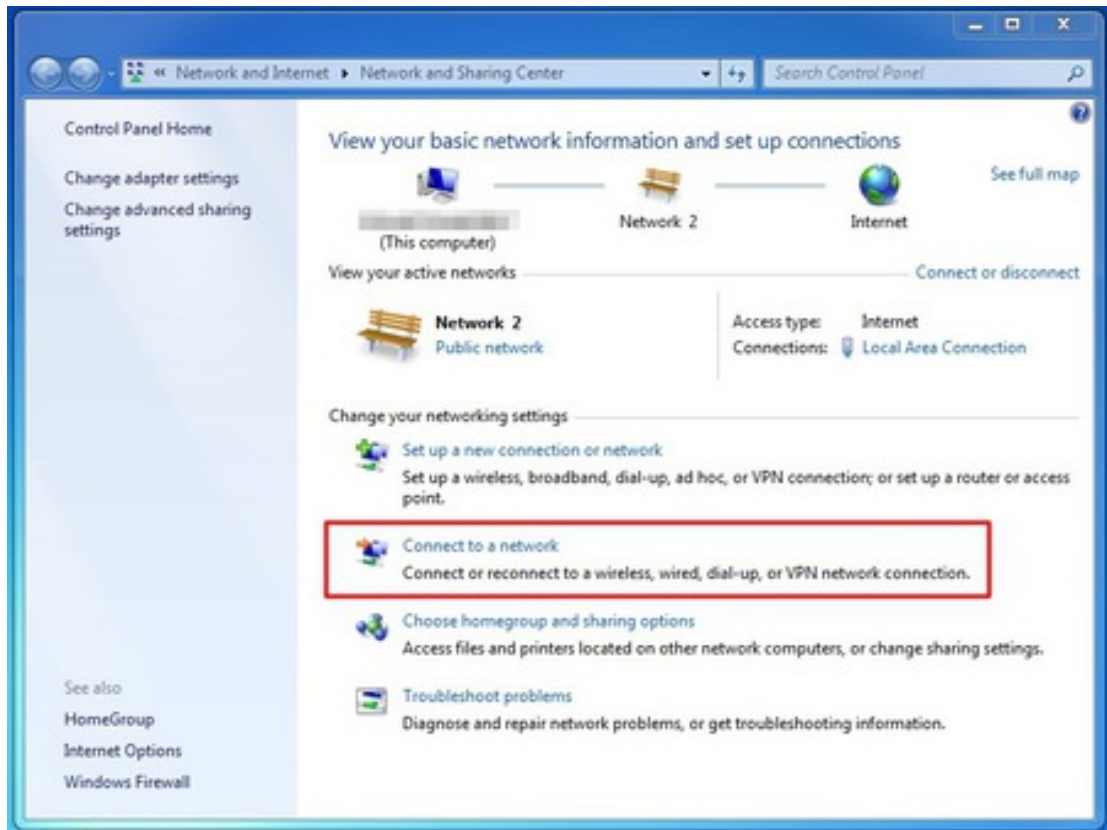


Figure 10.31: VPN on Windows

4. The wizard to setup a connection will popup. Choose the option to “connect to a workplace”, which is Microsoft’s way of naming a VPN connection.

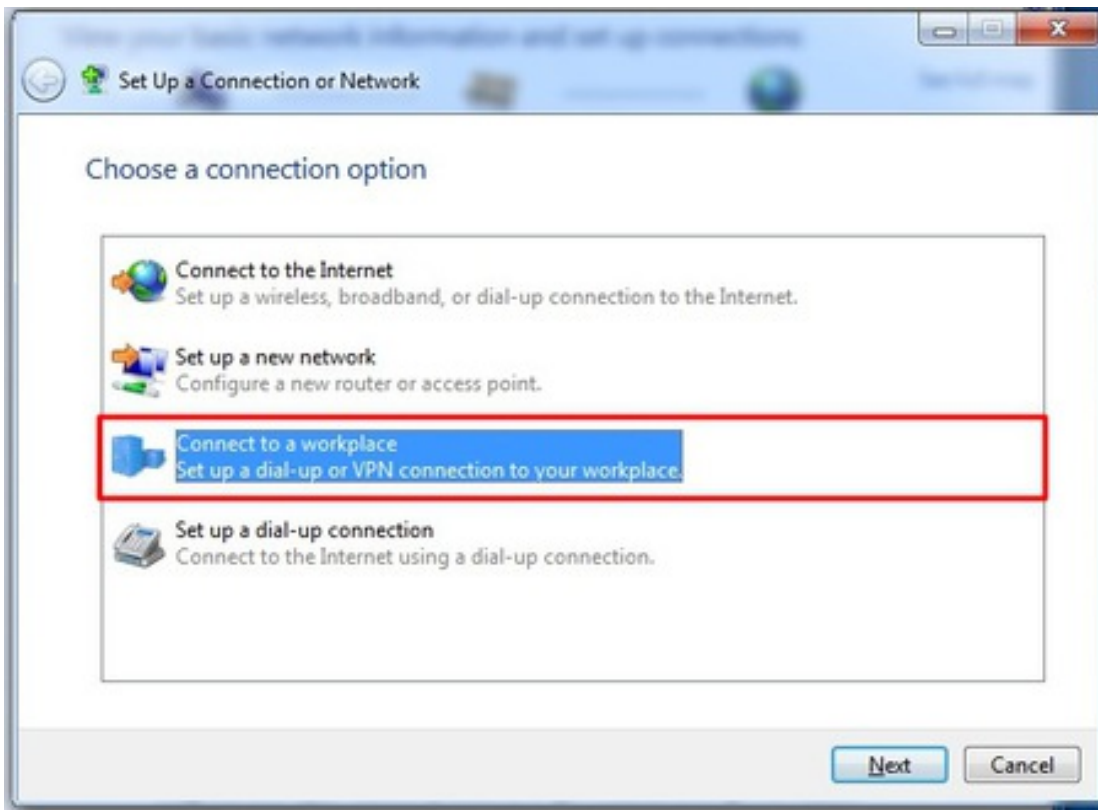


Figure 10.32: VPN on Windows

5. The next screen asks us if we want to use our Internet connection or an old-school phone line to connect to the VPN. Just choose the first option then.
6. The next screen asks for the connection details. Enter here the server of your VPN-provider (called “Internet address” in this dialog). On the bottom please check the box “Don’t connect now; just set it up”. Using this option the connection will be automatically saved and it’s easier to control extra settings. If this is all done, hit the “next” button
7. Next up are your username and password. Just give them like you received them from your VPN-provider. If the connection fails, Windows forgets them. So keep them with you, you maybe need them later. If this is done. Click “create”.



Figure 10.33: VPN on Windows

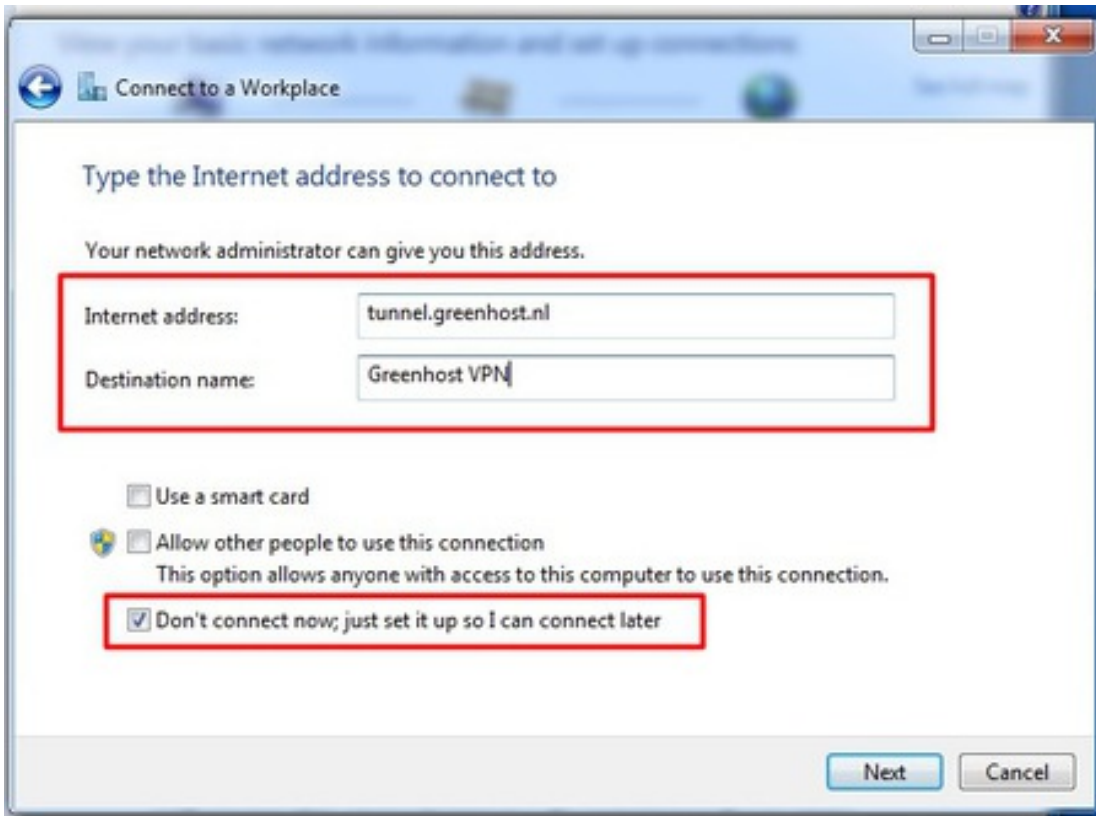


Figure 10.34: VPN on Windows



Figure 10.35: VPN on Windows

8. Your connection is now available, if you click the the network icon again, you will see a new option in the network menu, the name of your VPN connection, just click it to connect.



Figure 10.36: VPN on Windows

9. And click “connect”
10. A VPN connection dialog appears. This give us the opportunity to review our settings and to connect. You can try to connect, Windows will try to discover all

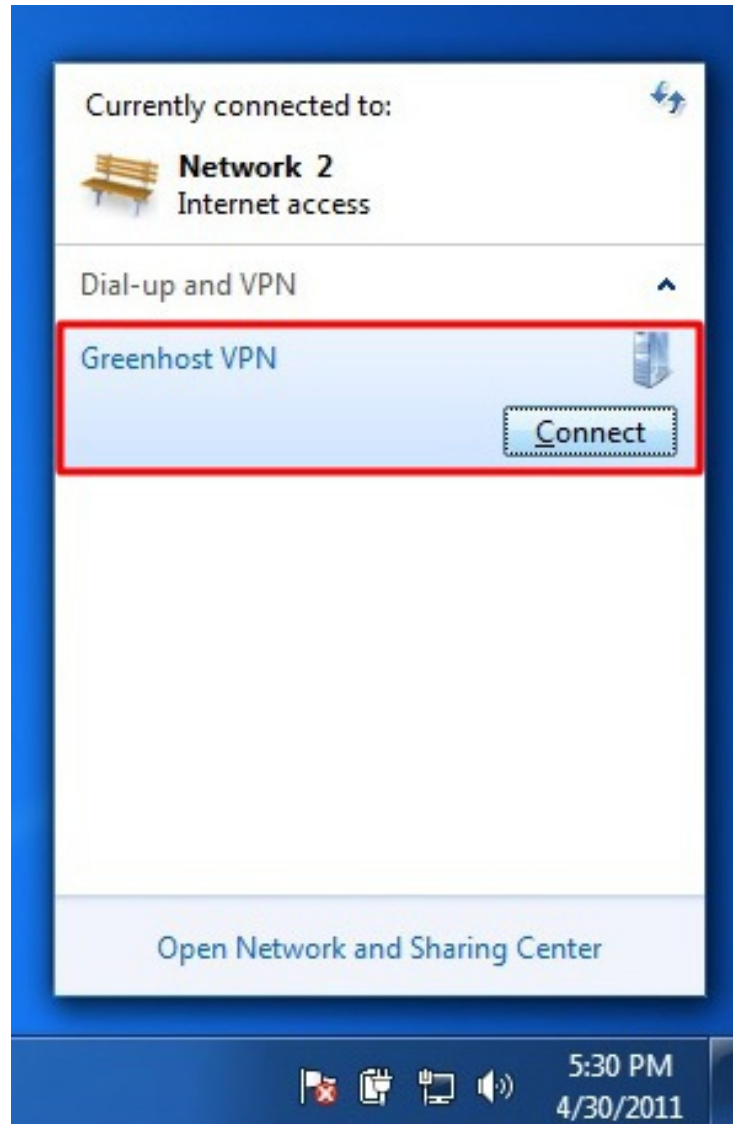


Figure 10.37: VPN on Windows

other settings automatically. Unfortunately, this does not always work, so if this is not working for you, hit the “properties” button.

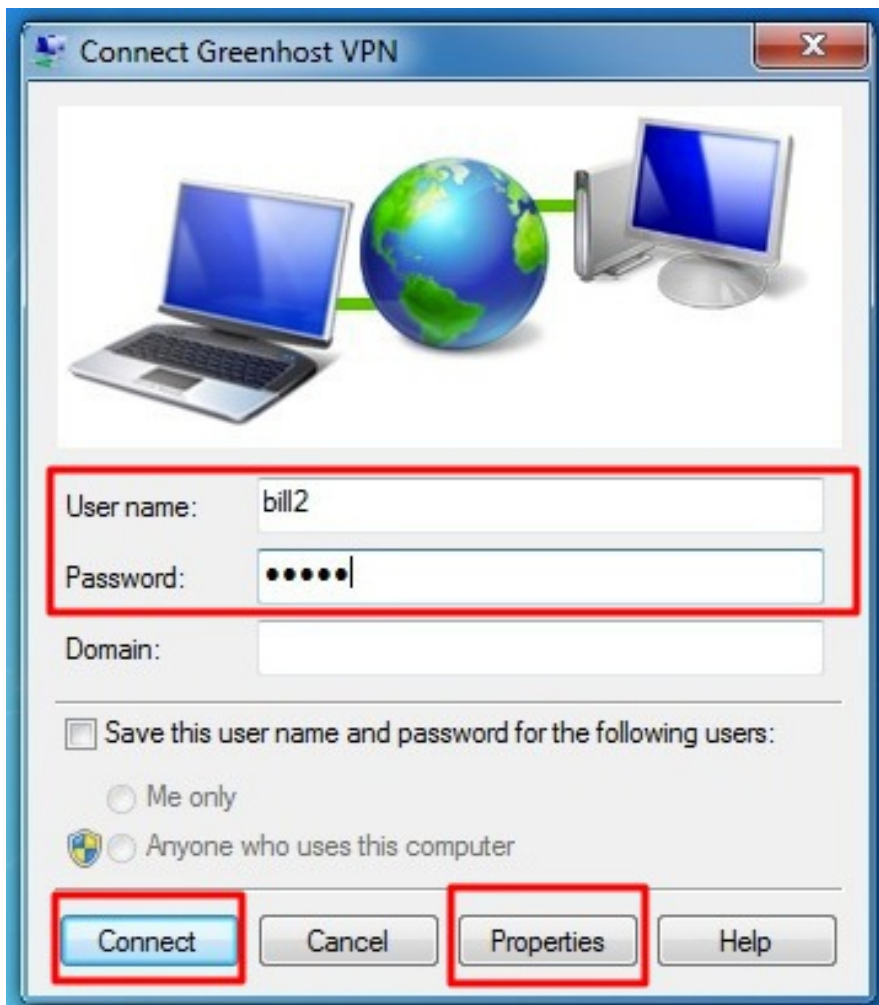


Figure 10.38: VPN on Windows

11. The properties windows appear. The most important page is the “Security” page, click on the Security tab to open it.
12. In the security tab you can specify VPN type, normally L2TP/IPSec. Do not use PPTP as it has several security vulnerabilities. For L2TP/IPSec also have a look at the Advanced settings.

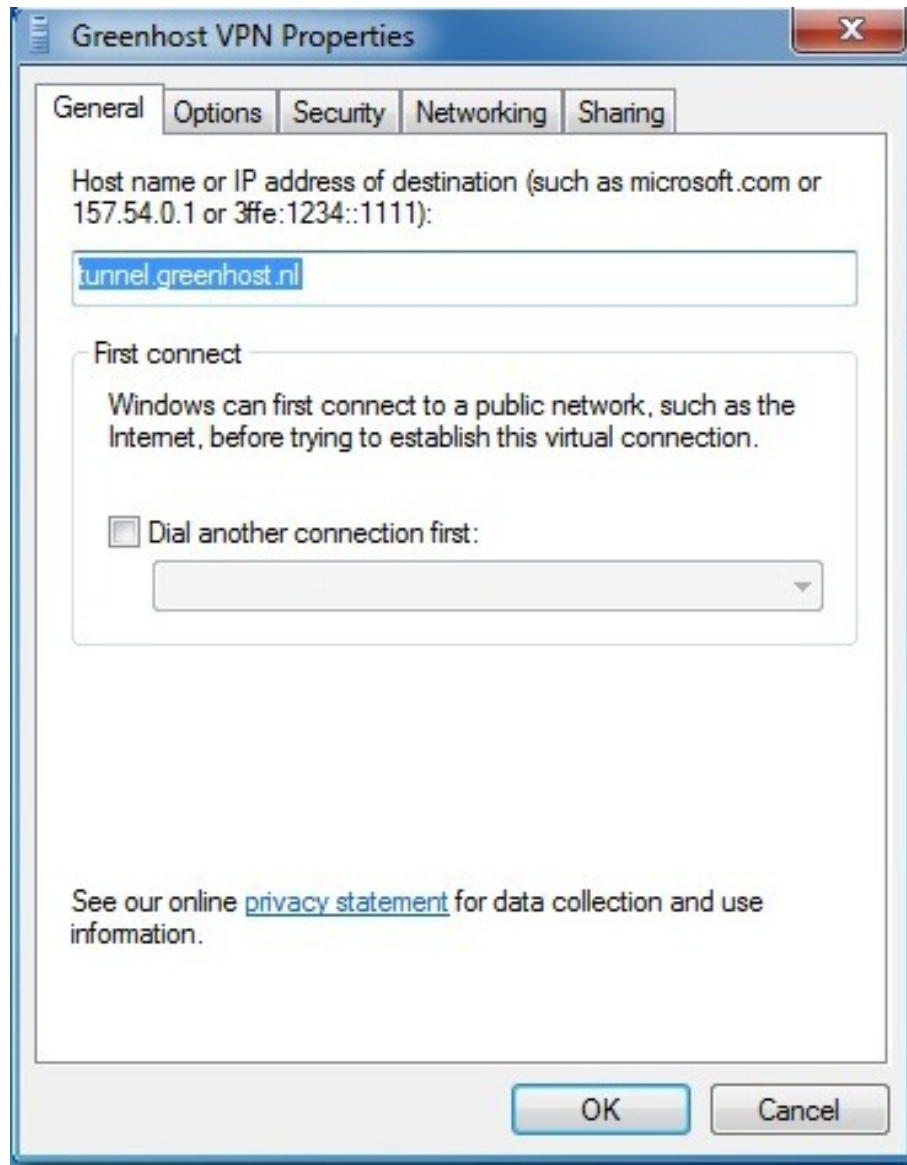


Figure 10.39: VPN on Windows



Figure 10.40: VPN on Windows

13. In the Advanced Settings window, you can specify if you are using a pre-shared key or a certificate. This depends on your VPN-provider. If you have received a pre-shared-key, Select this option and fill in this key. Hit ok afterwards. You will return to the previous window, click ok there also

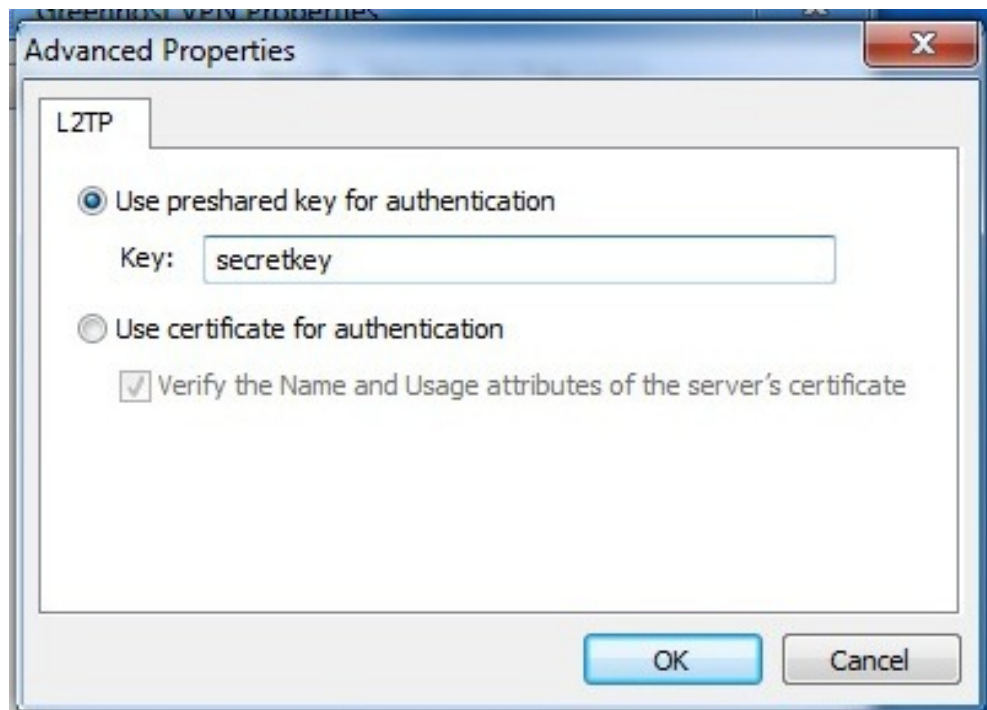


Figure 10.41: VPN on Windows

14. Back in to connection window try to connect now. Please be sure your username and password are filled out.
15. A connection popup will appear
16. Online! Don't forget to check if your VPN is working properly.



Figure 10.42: VPN on Windows



Figure 10.43: VPN on Windows

10.5 Making Sure Your VPN Works

Once you're done setting up your VPN, one of the first things you should do is test whether your data is actually being transferred through your VPN network. The simplest way to test this is to check your public IP address, which is the IP address you're exposing to the internet.

There are numerous websites that will tell you what your IP address is, and where that IP address is located (also known as its geolocation). Many search engines will report your IP address if you search for "My IP," but you can also use dedicated services like <http://www.myip.se> and <http://www.ipchicken.com>.

Check your IP address before connecting to your VPN. Once you connect to your VPN, your computer's public IP address should change to match that of your VPN server, and your geolocation should change to wherever your VPN server is located.

Once your external IP is the same as the IP of your VPN server, you can rest assured your communication is encrypted.

11 Disk Encryption

11.1 Installing TrueCrypt

TrueCrypt can be installed on Windows, Linux, or Mac OSX. The installation files are available here: <http://www.truecrypt.org/downloads>

The following three sections give complete details on how to install TrueCrypt for each of these Operating Systems, starting with Ubuntu and Debian.

11.1.1 Installing on Ubuntu/Debian

TrueCrypt is not available in the standard Ubuntu repositories. This means you cannot use the Ubuntu Software Center or *apt-get* (a command line method for installing software on Ubuntu) to install it. Instead you must first visit the TrueCrypt downloads page (<http://www.truecrypt.org/downloads>).

You will see a drop-down menu under the heading Linux.

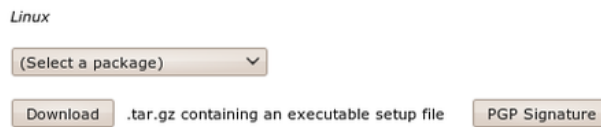


Figure 11.1: Dropdown menu on the download page

From the '(Select a package)' drop down menu you can choose from four options:

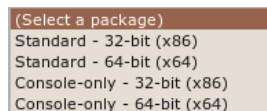


Figure 11.2: Choosing the correct package to download

This is a little technical - the console version is the one you choose if you are either very technical and don't like Graphical User Interfaces or you wish to run this on a machine that you have only a terminal (command line or 'shell') access to (like a remote server for example).

Assuming you are running this in your laptop its best to choose the easy 'standard' option - this will give you a nice user interface to use. From these two options you need to choose the one most suitable for the *architecture* of your machine. Don't know what this means? Well, it basically comes down to the type of hardware (processor) running

11 Disk Encryption

on your computer, the options are 32-bit or 64-bit. Unfortunately Ubuntu does not make it easy for you to find this information if you don't already know it. You need to open a 'terminal' from the Applications->Accessories menu and type the following, followed by the [enter] key

```
uname -a
```

The output will be something like `Linux bigsy 2.6.32-30-generic #59-Ubuntu SMP Tue Mar 1 21:30:46 UTC 2011 x86_64 GNU/Linux`. In this instance you can see the architecture is 64-bit (`x86_64`). In this example I would choose the 'Standard - 64-bit (x64)' option. If you see `i686` somewhere in the output of the `uname` command then you would choose the other standard option to download.

Once selected press the 'download' button and save the file to somewhere on your computer.

So the installation process is still not over. The file you downloaded is a compressed file (to make downloading it faster) and you need to first de-compress the file before you install it. Fortunately Ubuntu makes this easy - simply browse to the file on your computer and right click on it and choose 'Extract Here'.

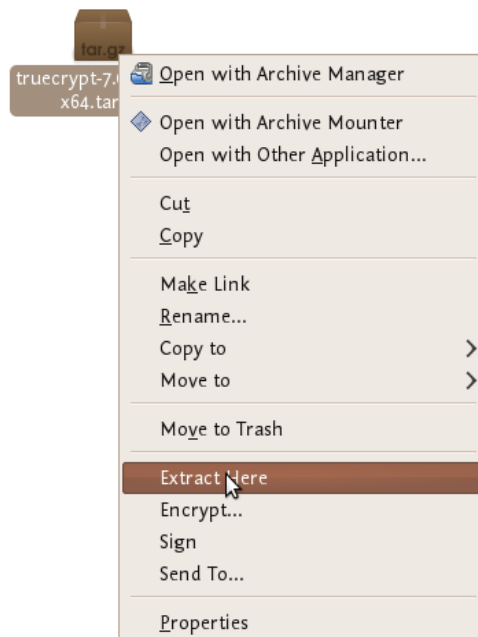


Figure 11.3: Right click and 'extract here'

You will see a new file appear next to the compressed file:
Nearly done! Now right click on the new file and choose 'open':
If all is well you will see a window open like this:
Choose 'run' and you see the following:

11.1 Installing TrueCrypt

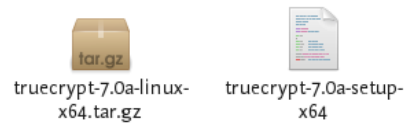


Figure 11.4: The extracted file

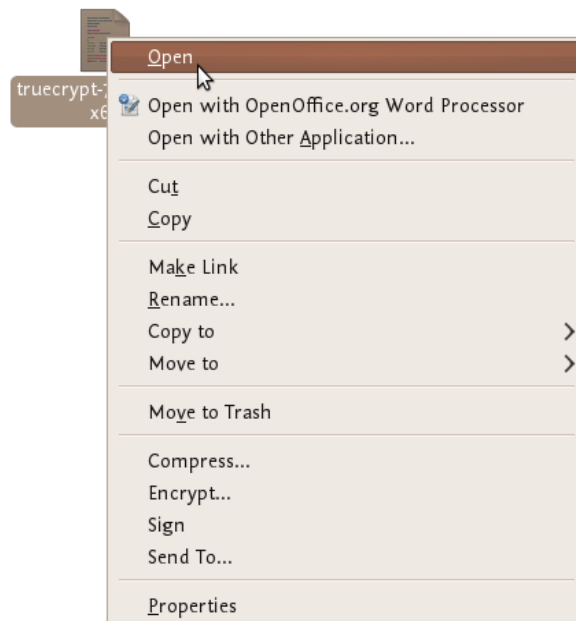


Figure 11.5: Right click and 'open'



Figure 11.6: Window opens to confirm you want to 'run' the file

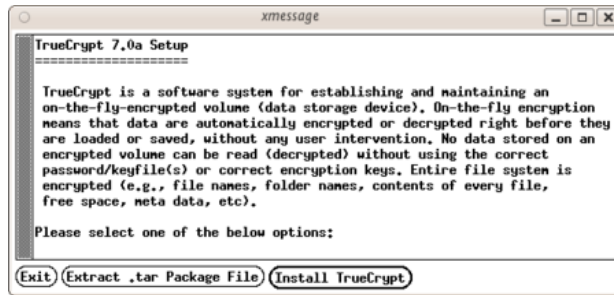


Figure 11.7: Truecrypt installer starts...

Now we are getting somewhere... press 'Install TrueCrypt'. You will be displayed a user agreement. At the bottom press 'I accept and agree to be bound by the license terms' (sounds serious). You will then be shown another info screen telling you how to uninstall TrueCrypt. Press 'OK' then you will be asked for your password to install software on your computer. Enter your password and then you will finally see a screen like this:

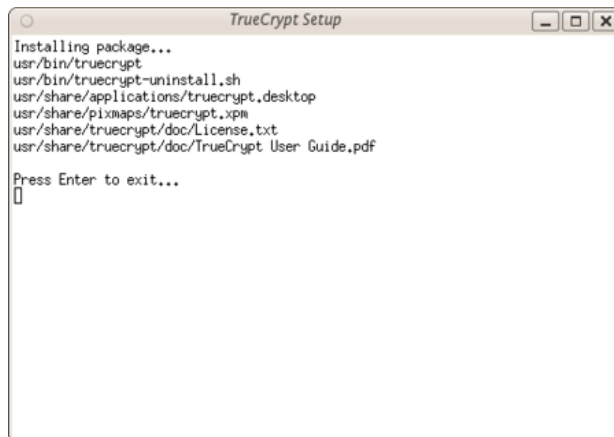


Figure 11.8: Truecrypt install finished... 'press Enter to exit'

Believe it or not you are done... TrueCrypt is installed and you can access it from the Applications->accessories menu... close the setup window. Now proceed to the chapter on Using TrueCrypt.

11.1.2 Installing on OSX

1. To install TrueCrypt on OSX first visit the download page (<http://www.truecrypt.org/downloads>) and press the download button under the OSX section.
2. Download this to your computer find the .dmg file and open it to access the installation package.

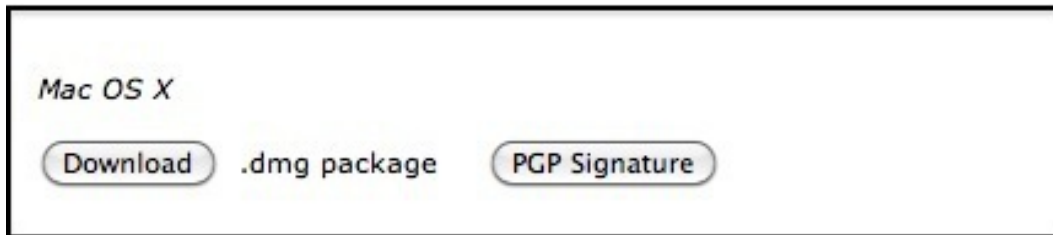


Figure 11.9: Download button

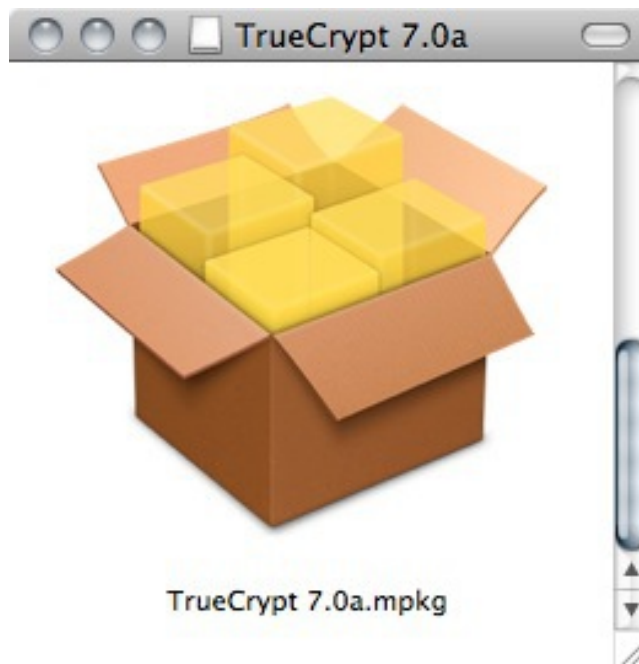


Figure 11.10: Open the .dmg file

3. Open the installation package, and click through the dialogues.
4. Choose the standard installation. You can choose to do a customized installation and deselect FUSE, but why would you? You need it!
5. After the installation finishes you can find the program in your 'Applications' folder.



Figure 11.11: Click through the dialogues

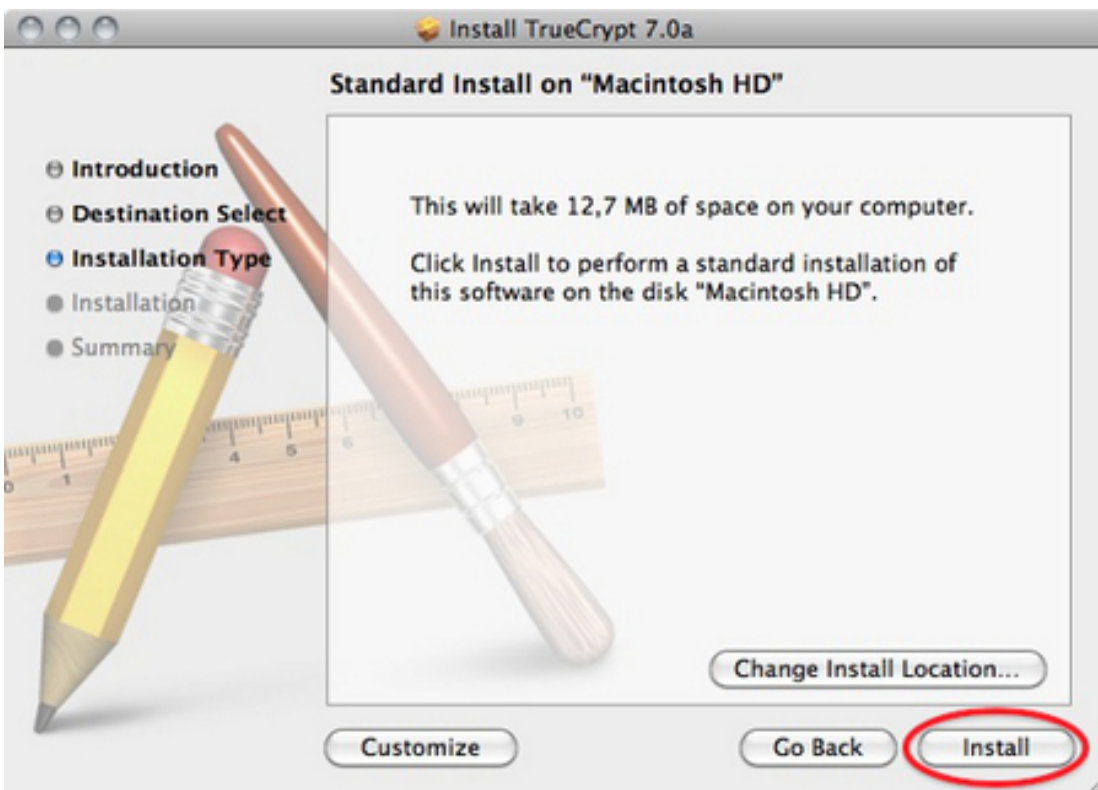


Figure 11.12: Choose standard installation



Figure 11.13: Truecrypt launcher now in Applications

11.1.3 Installing on Windows

To install TrueCrypt on Windows first visit the download page (<http://www.truecrypt.org/downloads>) and press the download button under the Windows section.

Download this to your computer and then double click on the file. You will see a license agreement.

Click on 'I accept and agree to be bound by the license terms' and then click 'Accept'.

Leave the above screen with the defaults and press 'Next >' and you will be taken to the Setup Options window:

You can leave this with the defaults. If you want to set up TrueCrypt just for yourself then consider not selecting the 'Install for all users'. However if you are installing this on your own machine and no one else uses the computer then this is not necessary. You may also wish to consider installing TrueCrypt in a folder other than the default. In which case click 'Browse' and choose another location. When you are done click 'Install' and the process will proceed:

When the installation is complete you will get a verification popup that it was successful. Close this window and click 'Finish' and all is done. Now proceed to the chapter on Using TrueCrypt.

11.2 Using TrueCrypt

The following are step-by-step instructions on how to create, mount, and use a TrueCrypt volume.

11.2.1 Creating a TrueCrypt Container

1. Install TrueCrypt. Then launch TrueCrypt by
 - double-clicking the file TrueCrypt.exe in Windows
 - opening Applications->Accessories->TrueCrypt in Ubuntu
 - on MacOSX open it by clicking Go > Applications. Find TrueCrypt in the Applications folder and double click on it.
2. When the main TrueCrypt window appears. Click Create Volume.
3. You should see the TrueCrypt Volume Creation Wizard window appear on screen.

Where do you want to create the TrueCrypt volume? You need to choose now. This can be in a file, which is also called a container, in a partition or drive. The following steps will take you through the first option creating a TrueCrypt volume within a file.

You can just click Next, as the option is selected by default,

4. Next you need to choose whether to create a standard or hidden TrueCrypt volume. We will walk you through the former option and create a standard TrueCrypt volume.

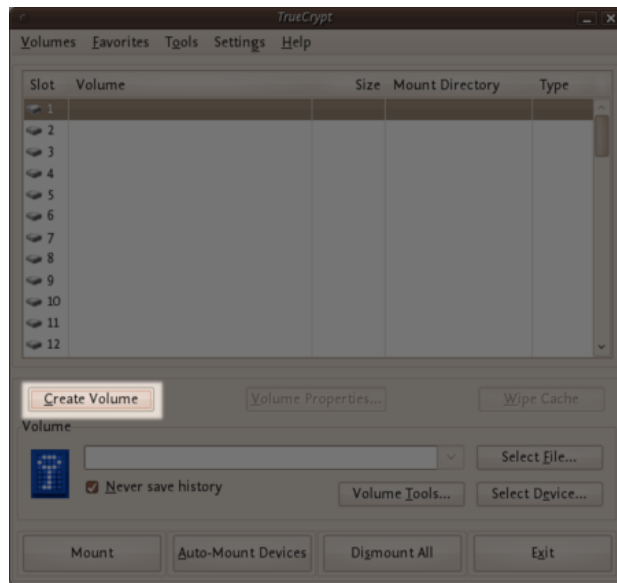


Figure 11.14: Using TrueCrypt



Figure 11.15: Using TrueCrypt



Figure 11.16: Using TrueCrypt

You can just click Next, as the option is selected by default.

5. Now you have to specify where to have the TrueCrypt volume (file container) created. Note that a TrueCrypt container behaves like any normal file. It can be moved or deleted as any normal file.



Figure 11.17: Using TrueCrypt

Click Select File.

The standard file selector will now appear on screen (the TrueCrypt Volume Creation Wizard remains open in the background). You need to browse to the folder that the file should be created in and then type into the 'name' field the name for the file you wish to create.

We will create our TrueCrypt volume in the folder 'adam/true' and the filename of the volume (container) will be 'myencryptedfile'. You may, of course, choose any other filename and location you like (for example, on a USB stick). Note that the file 'myencryptedfile' does not exist yet - TrueCrypt will create it. Press 'Save' when you are ready. The file selector window should close.

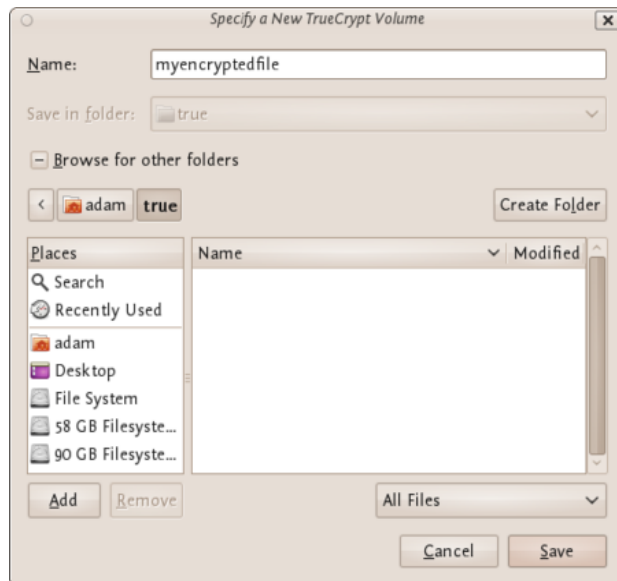


Figure 11.18: Using TrueCrypt

IMPORTANT: Note that TrueCrypt will not encrypt any existing files. If an existing file is selected in this step, it will be overwritten and replaced by the newly created volume (the contents of the existing file will be lost). You will be able to encrypt existing files later on by moving them to the TrueCrypt volume that we are creating now.

6. In the Volume Creation Wizard window (which was previously running in the background), click Next.
7. Here you can choose an encryption algorithm and a hash algorithm for the volume.



Figure 11.19: Using TrueCrypt

11 Disk Encryption

The TrueCrypt manual suggests that if you are not sure what to select here, you can use the default settings and click Next (for more information about each setting have a look at the TrueCrypt documentation website).

8. Now choose the size of your container. You should be fine with 1 megabyte but for this example we will enter '20' into the available field.

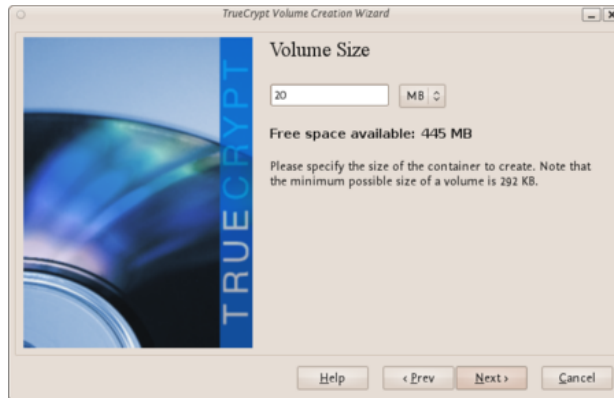


Figure 11.20: Using TrueCrypt

You may, of course, specify a different size. After you type the desired size in the input field, click Next.

9. This step is really important, choosing a password.

The information displayed in the Wizard window about what is considered a good password, should be read carefully.

Choose a strong password, type it in the first input field. Then re-type it in the input field below the first one.

When you are done click Next.

10. Now you must choose the format of your partition (this step may not be available for you under windows or OSX). If using Ubuntu you can choose a Linux file type or FAT (Windows) for simplicity leave it at the default.

Then press Next.

11. Next TrueCrypt tries to generate random information to help encrypt your container. For 30 seconds move your mouse as randomly as possible within the Volume Creation Wizard window. Move the mouse as much as possible for up to a minute. This significantly increases security by increasing the cryptographic strength of the encryption keys. security). Move your mouse around until you are bored.

11.2 Using TrueCrypt



Figure 11.21: Using TrueCrypt

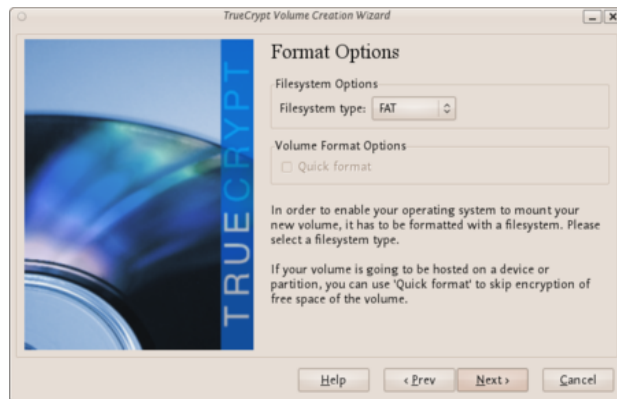


Figure 11.22: Using TrueCrypt

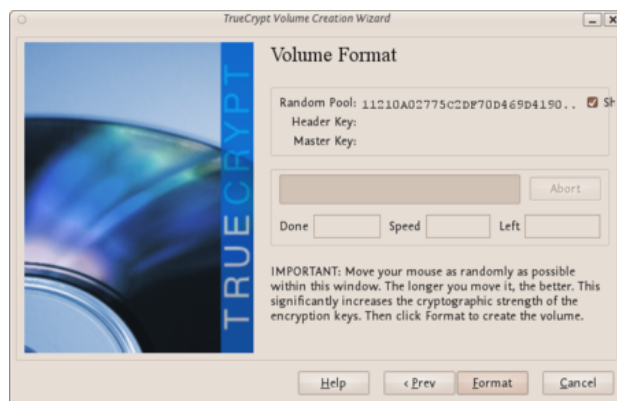


Figure 11.23: Using TrueCrypt

11 Disk Encryption

Then Click Format.

TrueCrypt will now create a file in the folder you selected with the name you chose. This file will be a TrueCrypt container, containing the encrypted TrueCrypt volume. This may take some time depending on the size of the volume. When it finishes this should appear:

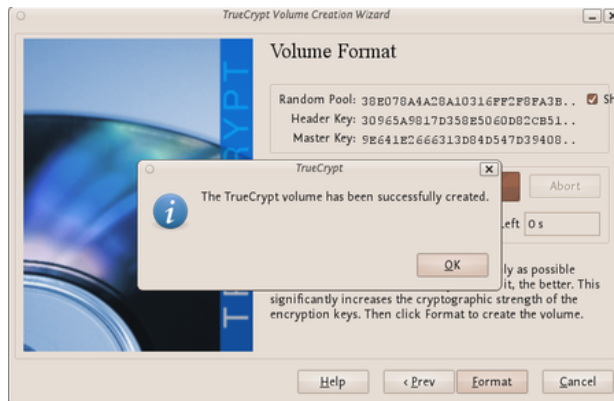


Figure 11.24: Using TrueCrypt

Click OK to close the dialog box.

12. Well done! You've just successfully created a TrueCrypt volume (file container).

In the TrueCrypt Volume Creation Wizard window, click Exit.

11.2.2 Mounting the Encrypted Volume

1. Open up TrueCrypt again.
2. Make sure one of the 'Slots' is chosen (it doesn't matter which - you can leave at the default first item in the list). Click Select File.

The standard file selector window should appear.

3. In the file selector, browse to the container file (which we created earlier) and select it.

Click Open (in the file selector window).

The file selector window should disappear.

4. In the main TrueCrypt window, click Mount.

Password prompt dialog window should appear.

5. Type the password in the password input field.

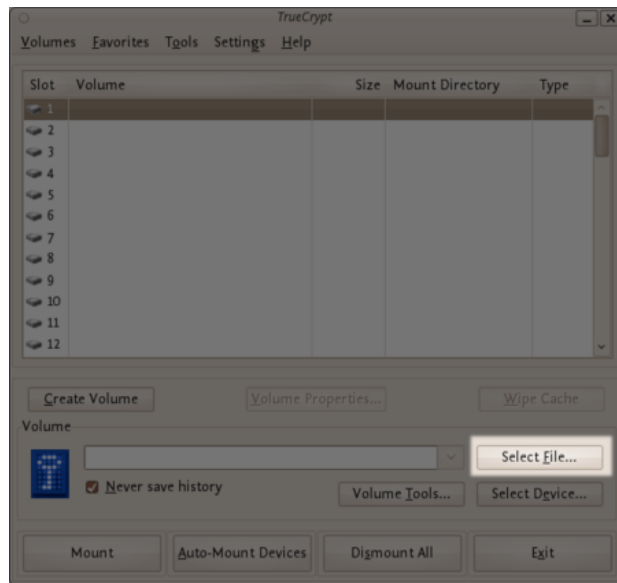


Figure 11.25: Using TrueCrypt

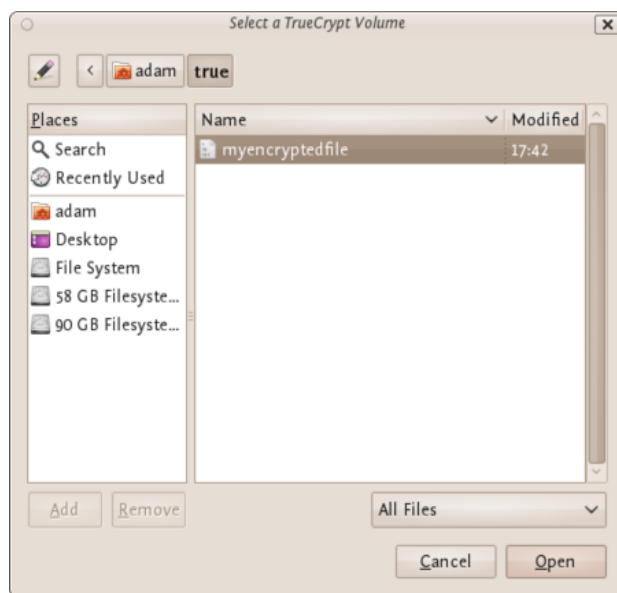


Figure 11.26: Using TrueCrypt

11 Disk Encryption

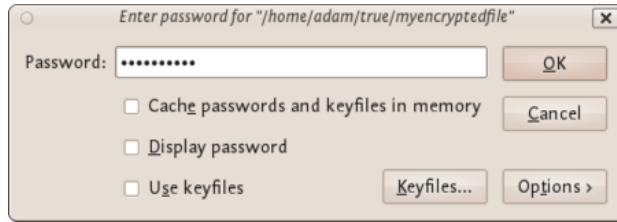


Figure 11.27: Using TrueCrypt

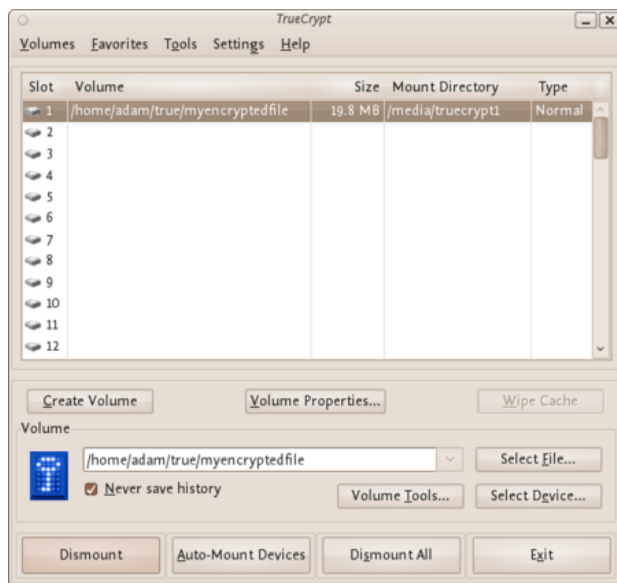


Figure 11.28: Using TrueCrypt

6. Click OK in the password prompt window.

TrueCrypt will now attempt to mount the volume. If the password is correct, the volume will be mounted.

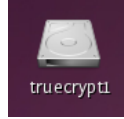


Figure 11.29: Using TrueCrypt

If the password is incorrect (for example, if you typed it incorrectly), TrueCrypt will notify you and you will need to repeat the previous step (type the password again and click OK).

7. We have just successfully mounted the container as a virtual disk 1. The container will appear on your Desktop or you will see it in your file browser.

11.2.3 What does this mean?

The disk that you have just created is completely encrypted and behaves like a real disk. Saving (moving, copying, etc) files to this disk will allow you to encrypt files on the fly.

You'll be able to open a file which is stored on a TrueCrypt volume, which will automatically be decrypted to RAM while it is being read, and you won't need to enter your password each time. You'll only need to enter this when your mounting the volume.

11.2.4 Remember to dismount!

To do this right click on the drive and select unmount. This will automatically happen when you turn off your computer but will not happen if you just put the computer on sleep.

11.3 Setting up a hidden volume

A TrueCrypt hidden volume exists within the free space of a typical TrueCrypt volume. Given then the 'outer volume' is accessed it is (almost) impossible to determine if there is a hidden volume within it. This is because TrueCrypt *always* fills the empty space of an encrypted volume with random data. So a hidden volume looks the same as an empty TrueCrypt volume.

To create and use a hidden volume you need two passwords - one each for the outer and inner (hidden) volumes. When you mount (open) the volume you can use either password and that will determine which of the two is opened. If you want to open just the hidden volume you use one password, and if you want to access just the non-hidden encrypted volume you use the other password.

11 Disk Encryption

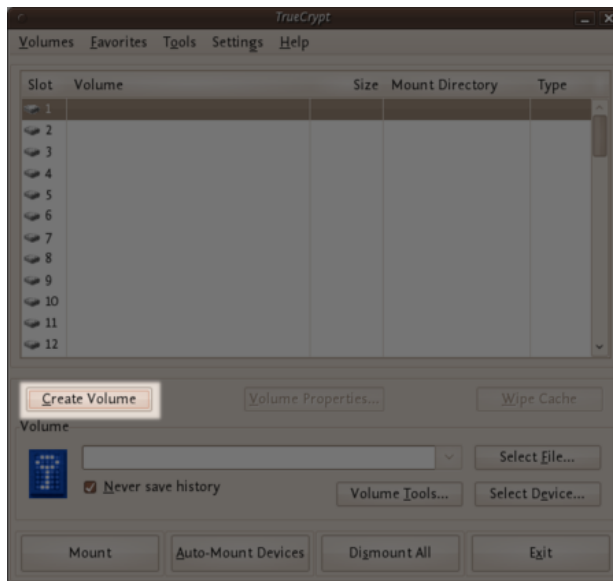


Figure 11.30: Hidden volumes

To create a hidden volume open TrueCrypt and press the ‘Create Volume’ button:

The options for half of this process are almost the same as for setting up a standard TrueCrypt volume and then the process continues for setting up the hidden volume but lets go through the entire process step by step anyway. In the screen shown below you just want to stay with the default setting ‘Create an encrypted file container’:



Figure 11.31: Hidden volumes

Press ‘Next >’ and continue to the next screen.

In the above screen you want to be sure that you choose the second option ‘Hidden TrueCrypt Volume’. Select this and click on ‘Next >’ you will then be asked to choose the location and name of the TrueCrypt *outer* volume.

Click ‘Select File...’ and browse to a location for a new TrueCrypt volume. We will

use the name ‘myencryptedfile’ in this example. Its the same name as we used in the last example so be aware that if you have just followed those instructions you must now create a new volume with a new name.

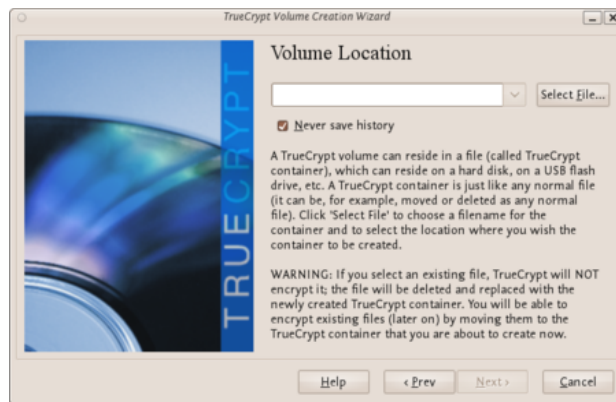


Figure 11.32: Hidden volumes

Browse to the directory where you want to put the outer volume and enter the name of the volume in the field named ‘Name’ as in the example above. When you are satisfied all is well click on ‘Save’. The file browser will close and you return to the Wizard. Click ‘Next >’. Here you are presented with some very technical choices. Don’t worry about them. Leave them at the defaults and click ‘Next >’. The next screen asks you to determine the size of the outer volume. Note that when you do this the maximum inner ‘hidden’ volume size is determined by TrueCrypt. This maximum size will of course be smaller than the size you are setting on this screen. If you are not sure what the ratio of outer volume size to inner (hidden) volume size is then go through the process now as a ‘dummy’ run - you can always trash the encrypted volume and start again (no harm done).

So choose the size of the outer volume, I will choose 20MB as shown below:

You cannot set the outer volume size to be larger than the amount of free space you have available on your disk. TrueCrypt tells you the maximum possible size in bold letters so create a volume size smaller than that. Then click ‘Next >’ and you will be taken to a screen asking you to set a password for the outer (not the hidden, this comes later) volume.

Enter a password that is strong (see the chapter on creating good passwords) and press ‘Next >’. Next TrueCrypt wants you to help it create the random data it will fill the volume up with. So wave your mouse around, browse the web, and do whatever you want for as long as you can. When you feel TrueCrypt should be happy then press ‘Format’. You will see a progress bar zip by and then you will be presented with the next screen:

You can open the outer volume if you like but for this chapter we will skip that and go ahead to create the hidden volume. Press ‘Next >’ and TrueCrypt will work out how the maximum possible size of the hidden volume.

When you see the above screen just press ‘Next >’. Now you must choose the encryp-

11 Disk Encryption

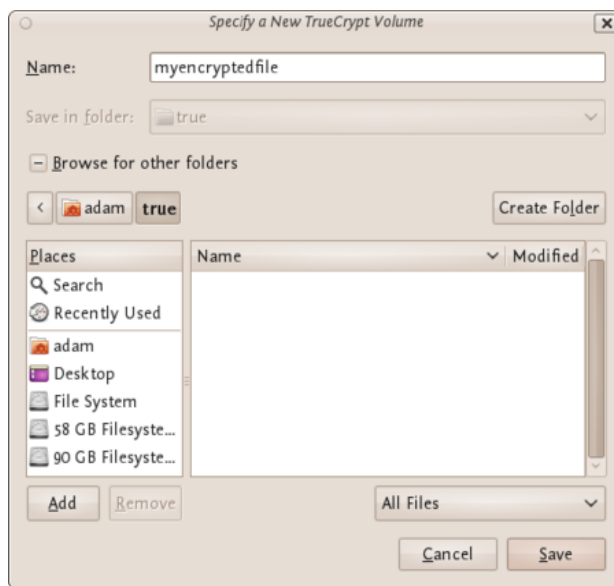


Figure 11.33: Hidden volumes



Figure 11.34: Hidden volumes

tion type for the hidden volume. Leave it at the defaults and press 'Next >'.

Now you will be asked to choose the size of the hidden volume.

I have set (as you see above) the maximum size as 10MB. When you have set your maximum size press 'Next >' and you will be prompted to create a password for the hidden volume.

When creating the password for the hidden volume make sure you make it substantially different fro the password for the outer volume. If someone really does access your drive and finds out the password for the outer volume they might try variations on this password to see if there is also a hidden volume. So make sure the two passwords are not alike.

Enter your password in the two fields and press 'Next >'.

Leave this window at the defaults and press 'Next >' and you will be presented with the same screen you have seen before to generate random data for TrueCrypt. When you are happy click 'Format' and you should see the following :



Figure 11.35: Hidden volumes

The TrueCrypt manual it is referring to is not this manual. They mean this manual : <http://www.truecrypt.org/docs/>

Click 'OK' and keep and exit TrueCrypt. You can now mount the volume as noted in the previous chapter.

11.4 Securely destroying data

Just hit the delete button and you are done! No it's not that easy. To understand how to securely delete data, we have to understand how data is stored. In an analogy to the real world, an explanation of how data is stored follows:

Assume you have a small notebook with 10 pages and you want to write some data in this notebook. You just start writing on the first page up to the end of the notebook. Maybe you decide the information on page 5 must be destroyed. Probably you will just take out the page and burn it.

Unfortunately data on a harddisk doesn't work this way. A harddisk contains not ten but thousands or maybe even millions of pages. Also it's impossible to take out a "page" of a harddisk and destroy it. To explain how a harddisk work, we will continue with our 10-page notebook example. But now we will work a little bit different with it. We will work in a way similar to how a harddisk works.

This time we use the first page of our notebook as an index. Assume we write a piece about "WikiLeaks", then on the first page we write a line "piece about WikiLeaks: see page 2". The actual piece is then written on page 2.

For the next document, a piece about "Goldman Sachs" we add a line on page 1, "Goldman Sachs: see page 3". We can continue this way till our notebook is full. Let's assume the first page will look like this:

- WikiLeaks -> see page 2
- Goldman Sachs -> see page 3
- Monstanto scandal -> see page 4
- Holiday pictures -> see page 5
- KGB Investigation -> see page 6
- Al Jazeera contacts -> see page 7
- Iran nuclear program -> see page 8
- Sudan investigation -> see page 9
- Infiltration in EU-politics -> see page 10

Now, let's decide you want to wipe the "Goldman Sachs" piece, what a harddisk will do, it will only remove the entry on the first page, but not the actual data, your index will be:

- WikiLeaks -> see page 2
- Monstanto scandal -> see page 4
- Holiday pictures -> see page 5
- KGB Investigation -> see page 6
- Al Jazeera contacts -> see page 7
- Iran nuclear program -> see page 8
- Sudan investigation -> see page 9
- Infiltration in EU-politics -> see page 10

What we did, we removed only the reference to the article, but if we open page 3, we will still be able to read the Goldman Sachs piece. This is exactly the way what a harddisk does when you “delete” a file. With specialized software it is still able to “recover” page 3.

To securely delete data, we should do the following:

1. Open the “Goldman Sachs” page (page 3)
2. Use an eraser to remove the article there, if done return to page 1
3. Delete the reference in the index on page 1

Well you will be surprised by the similarity between this example and the real world. You know when you removed the article on page 3 with an eraser, it is still possible to read the article slightly. The pencil leaves a track on the paper because of the pressure of the pencil on the paper and also you will be unable to erase all of the graphite. Small traces are left behind on the paper. If you really need this article, you can reconstruct (parts) of it, even if it’s erased.

With a harddisk this is very similar. Even if you erased every piece of data, it is sometimes possible with (very) specialized hardware to recover pieces of the data. If the data is very confidential and must be erased with the greatest care, you can use software to “overwrite” all pieces of data with random data. When this is done multiple times, this will make the data untraceable.

11.4.1 A note on Solid State Hard Drives

The instructions below explain how to use file deletion tools to securely delete files from your hard drives. These tools rely on the Operating System you are using being able to directly address every byte on the hard drive in order to tell the drive “set byte number X to 0”. Unfortunately, due to a number of advanced technologies used by Solid State Drives (SSDs) such as TRIM, it is not always possible to ensure with 100% certainty that every part of a file on an SSD has been erased using the tools below.

11.4.2 Securely delete data under Windows

For Windows there is a good open source tool called “File Shredder”. This tool can be downloaded from <http://www.files shredder.org>

The installation is very straightforward, just download the application and install it by hitting the next button. After installation this application will automatically start. You can then start using it for shredding files. However the best part of the program is that you can use it from within windows itself by right clicking on a file.

1. Click right on the file you want to shred, and choose File Shredder -> Secure delete files
2. A pop-up asks if you really want to shred this file
3. After confirming, there your file goes. Depending on the size of the file this can take a while

11 Disk Encryption

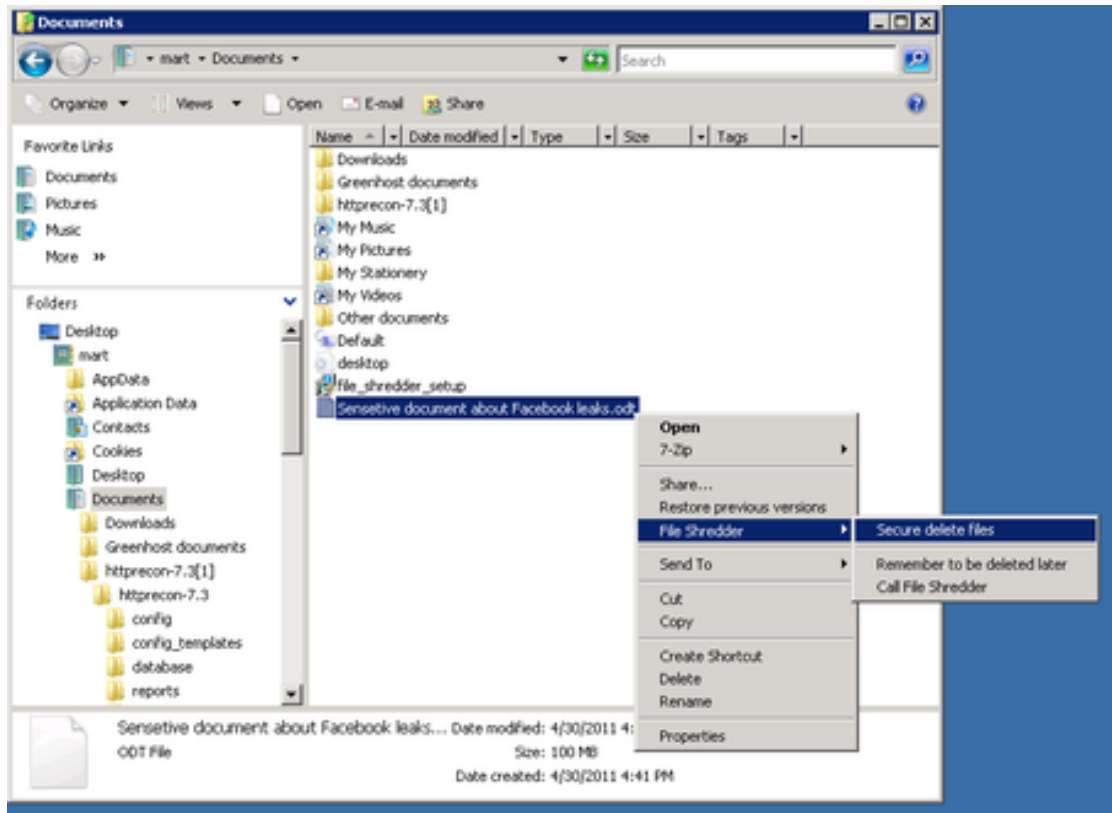


Figure 11.36: Destroying data

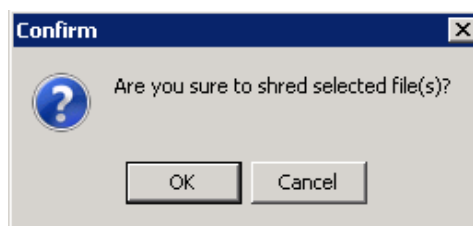


Figure 11.37: Destroying data



Figure 11.38: Destroying data

11.4.3 Securely delete data under MacOSX

There are basically two build-in steps to make to securely delete your data on Mac OSX.

1. Erase the free-space on your hard-drive containing all the data of items which are deleted in an insecure way.
2. Make sure that every file from then on is always securely deleted.

We start with the first one:

Erasing Free Space

1. Open Disk-Utility which resides in the Utilities folder inside the Applications folder.
2. Select your hard drive and click on 'Erase Free Space'.
3. Three options will appear, from top to bottom more secure, but also they take much more time to complete. Read the descriptions on each one of them to get an idea from what will happen if you use them and then choose which one might suite your needs the best and click 'Erase free Space'.

If time is no issue, then use the most secure method and enjoy your free time to get a good coffee while you Mac crunches away on this task. If the crooks are already knocking on your front-door you might want to use the fastest way.



Figure 11.39: Destroying data

Securely Erasing Files

Now that your previously deleted data is once and for ever securely erased you should make sure that you don't create any new data that might be recovered at a later date.

1. To do this open the finder preferences under the Finder Menu.
2. Go to the advanced tab and tick 'Empty trash securely'. This will make sure that every time you empty your trash all the items in it will be securely deleted and are really gone!

Note: Deleting your files securely will take longer than just deleting them. If you have to erase big portions of unimportant data (say your movie and mp3 collection) you may want to untick this option before doing so.

11.4 Securely destroying data

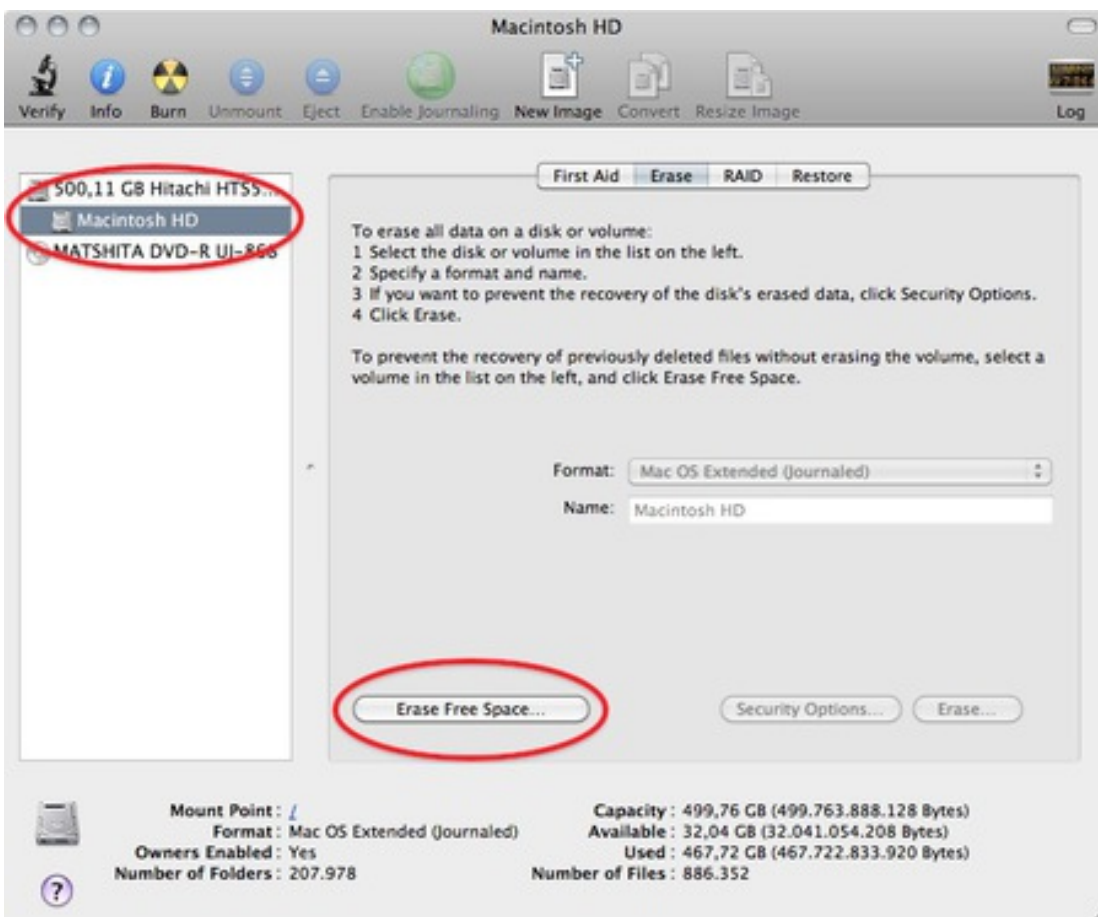


Figure 11.40: Destroying data

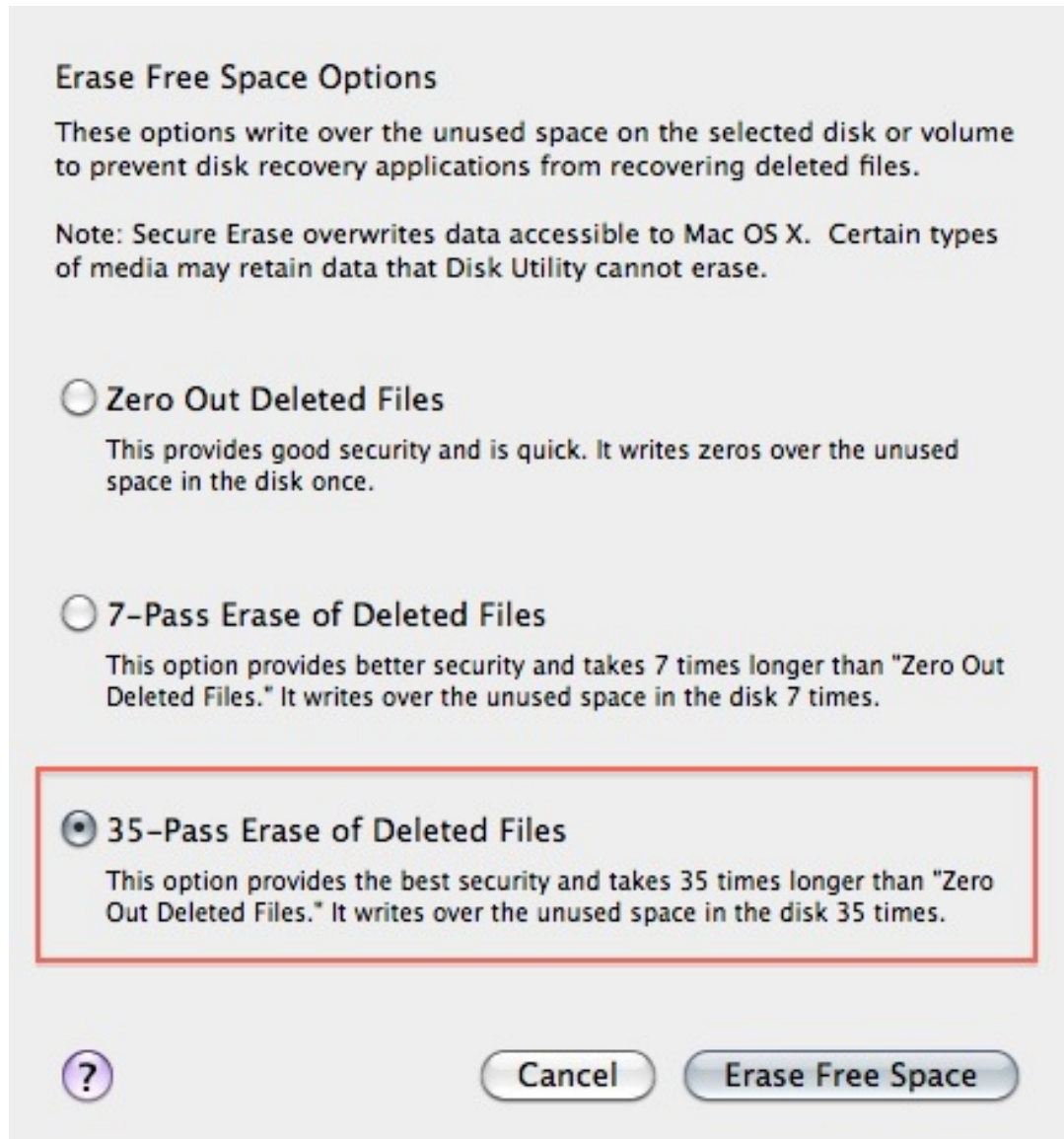


Figure 11.41: Destroying data



Figure 11.42: Destroying data



Figure 11.43: Destroying data

11.4.4 Securely delete data under Ubuntu/Linux

Unfortunately currently there is no graphical user interface available for Ubuntu to delete files secure. There are two command-line programs available though:

- `shred`
- `wipe`

`Shred` is installed in Ubuntu by default and can delete single files. `Wipe` is not installed by default but can easily be installed with using Ubuntu Software Center or if you understand the command line you can install it with `apt-get install wipe`. `Wipe` is a little more secure and has nicer options.

It is possible make access to these program's easy by adding it as an extra menu option

1. We assume you are familiar with the Ubuntu Software Center. To add the securely wipe option, it's required to install these two programs `wipe` and `nautilus-actions`

If the two programs are installed follow the following steps. If they are not installed use the Ubuntu Software Center to install them or on the command line simply type `apt-get install nautilus-actions wipe`

2. Open the "Nautilus Actions Configuration" from the System -> Preferences menu
3. We have to add a new action. To do this, start clicking on the "create new action button", the first option in the toolbar
4. Next is describing the new action. You can give the action every name you wish. Fill out this title in the "Context label" field. In this example we used "Delete file securely"
5. Click on the second tab ("Command"), here is how we specify the action we want. In the field "Path", type "wipe", in the field parameters type "`-rf %M`", please be sure about the capitalisation of all characters here, this is very important.
6. Next is specifying the conditions, click on the conditions tab and choose the option "Both" in the "Appears if selection contains..." box. With this option you can wipe both files and folders securely. If done, click the save button (second item on the icon bottom toolbar) or use the menu File->Save
7. Now close the Nautilus Actions Configuration tool. Unfortunately, after this, you have to re-login into your system, so ether reboot or login.

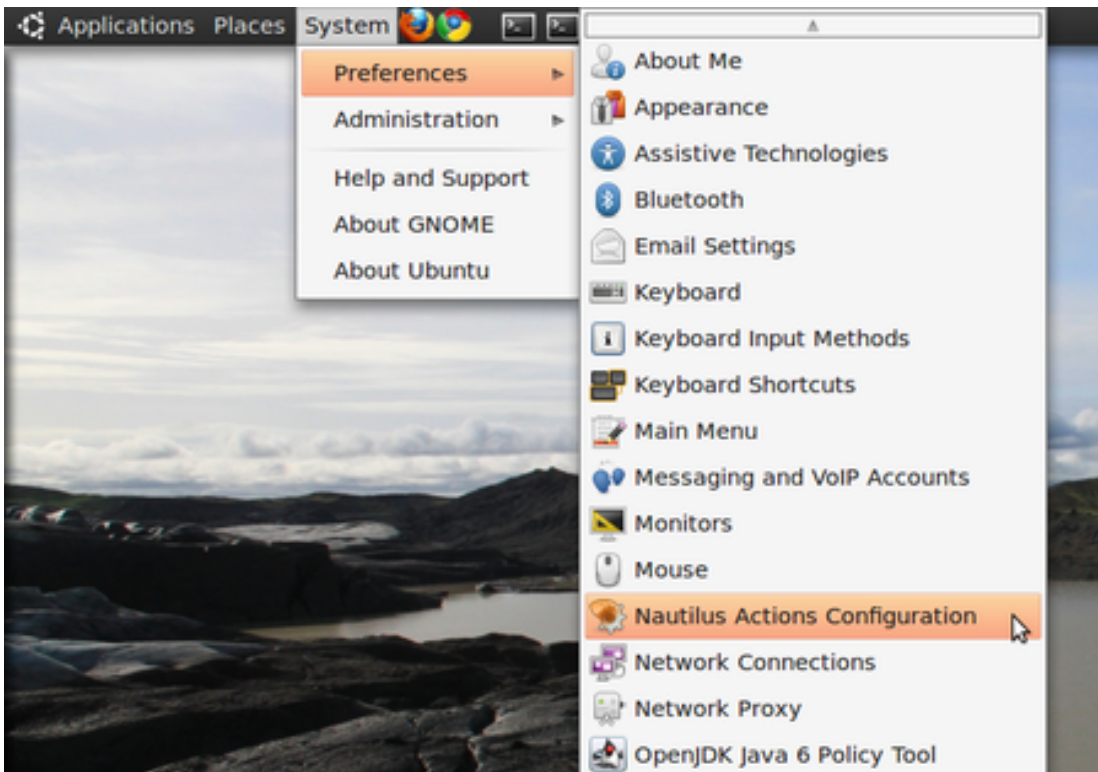


Figure 11.44: Destroying data

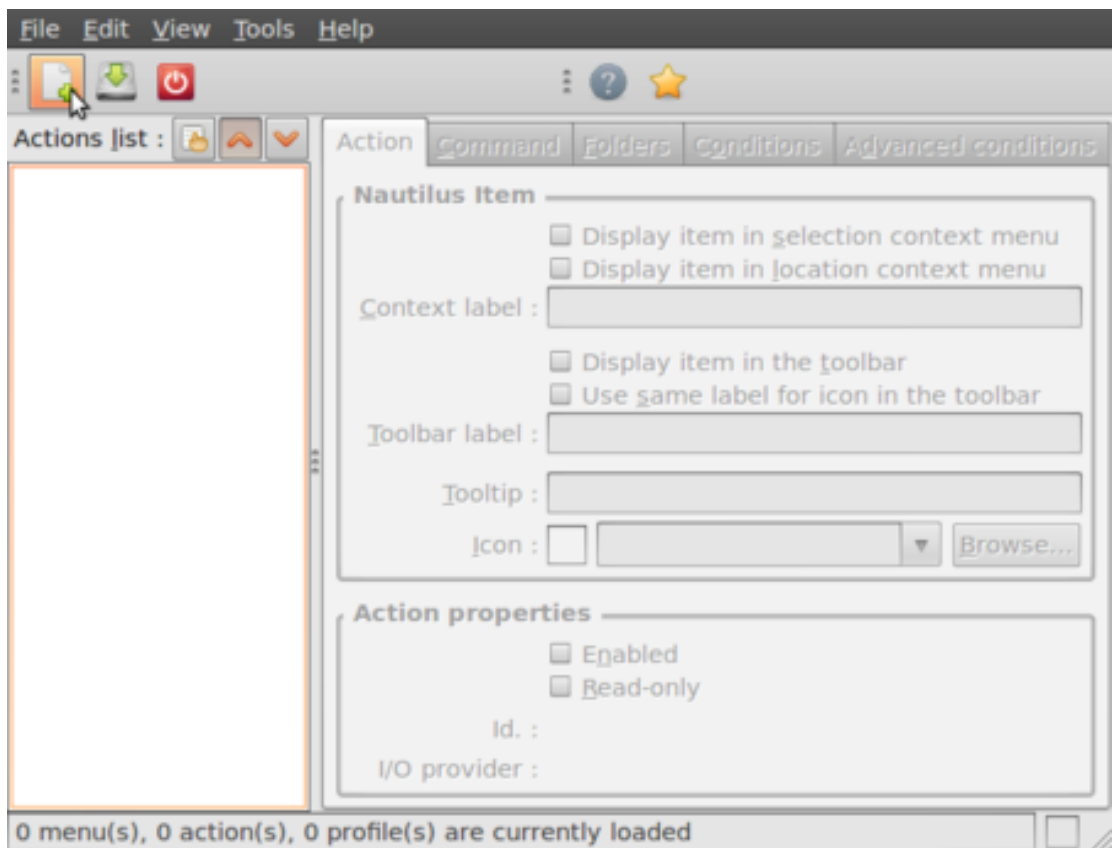


Figure 11.45: Destroying data

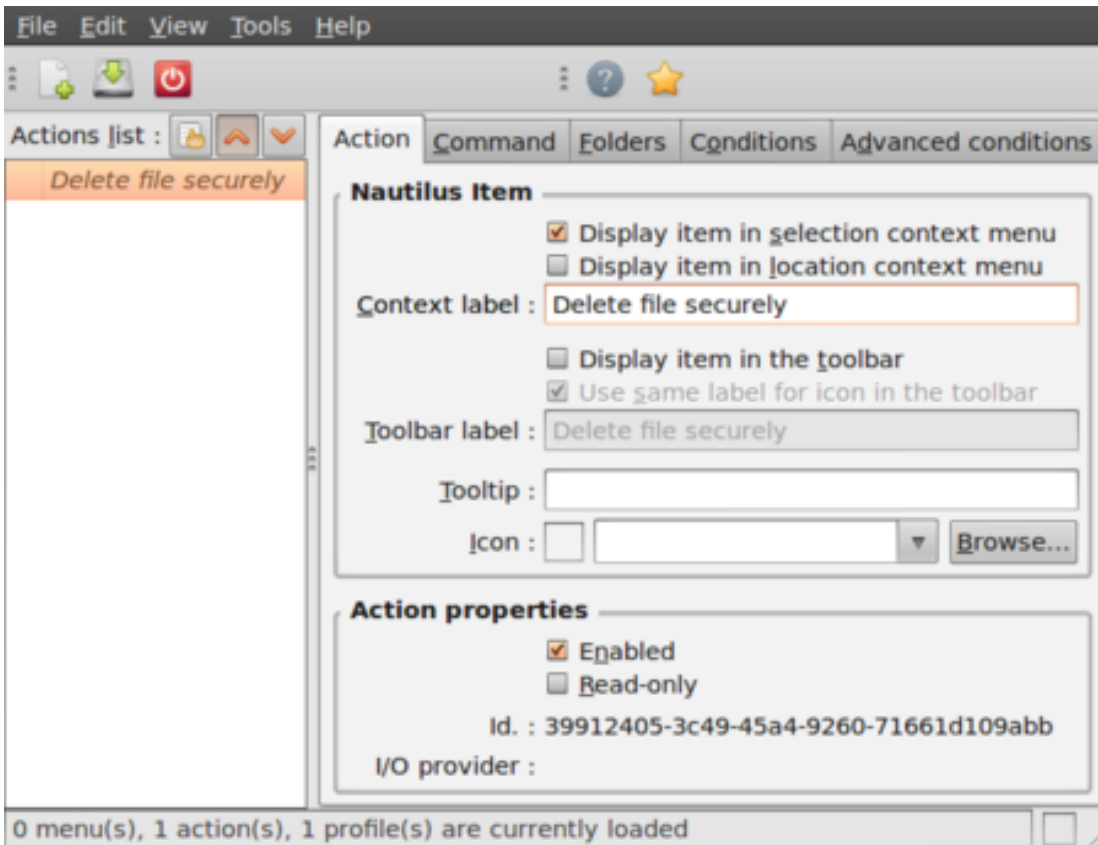


Figure 11.46: Destroying data

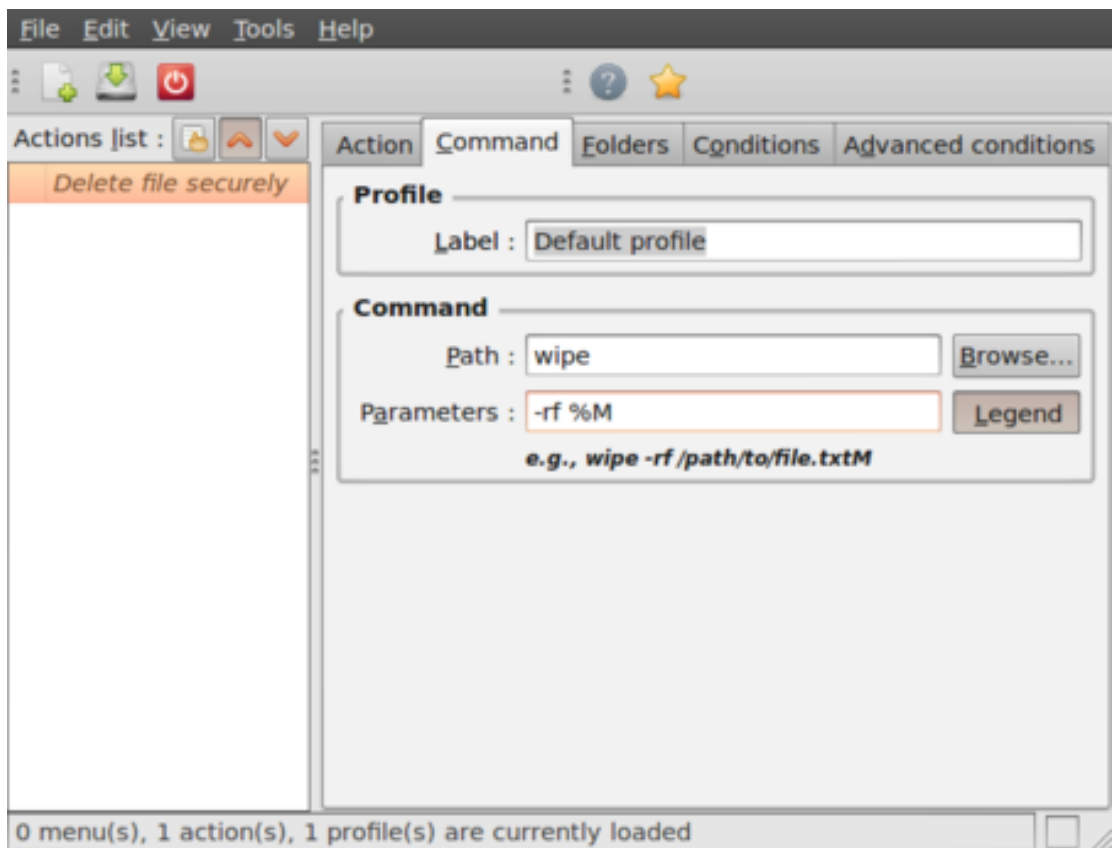


Figure 11.47: Destroying data

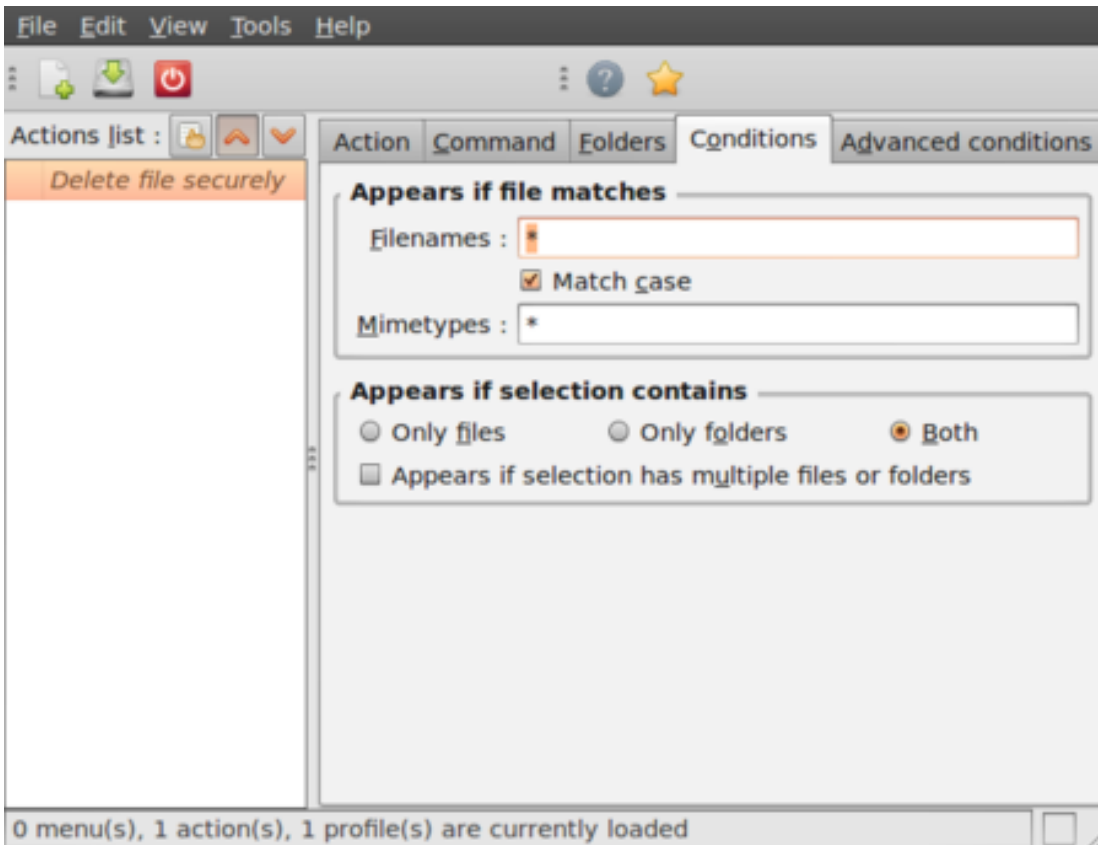


Figure 11.48: Destroying data

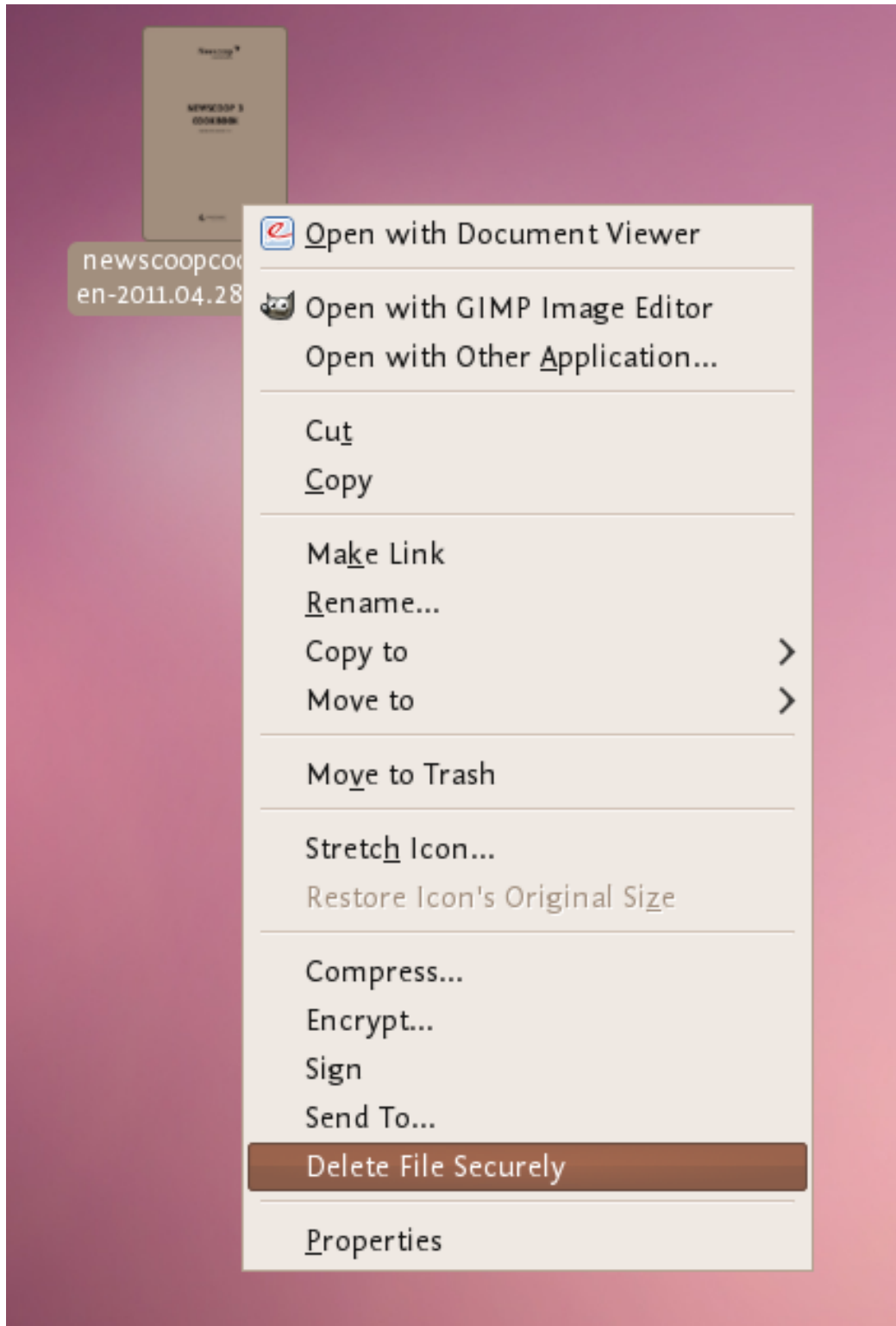


Figure 11.49: Destroying data

8. Now browse to the file you want to securely delete and right click:

Choose ‘Delete File Securely’. The file will then be wiped ‘quietly’ - you do not get any feedback or notice that the process has started or stopped. However the process is underway. It takes some time to securely delete data and the bigger the file the longer it takes. When it is complete the icon for the file to be wiped will disappear. If you would like to add some feedback you can change the parameters field in Nautilus Actions Configuration tool to this:

```
-rf %M | zenity --info --text "your wipe is underway, please be patient.  
The file to be wiped will disappear shortly."
```

The above line will tell you the process is underway but you will not know the file is deleted until the icon disappears.

11.5 About LUKS

LUKS, short for *Linux Unified Key Setup*, is the default method for disk encryption on Linux. It can be used to enable *Full Disk Encryption* during installation with a single click, or to encrypt individual partitions on external hard disks or usb sticks later on. Please note that *Full Disk Encryption* is hard to enable **after** the installation as it requires moving all existing files temporarily as encrypting a device requires formatting it.

- Advantages: LUKS is available through dm-crypt which is part of the Linux kernel, so it doesn't need any further software to be installed.
- Disadvantages: Unlike with Truecrypt, it is not possible to use it with other Operating Systems (yet), so if you use LUKS to encrypt a USB drive, you can only use it on Linux machines, but not on Windows or Mac OS.

If you want to encrypt a device after the Linux installation completed, you can use the *Disks* utility which can be found in most Linux distribution's *System Settings*.

11.5.1 Starting *Disks*

On Ubuntu, start *Disks* by pressing the Windows key and A, typing “disks” and selecting the corresponding program as shown below:

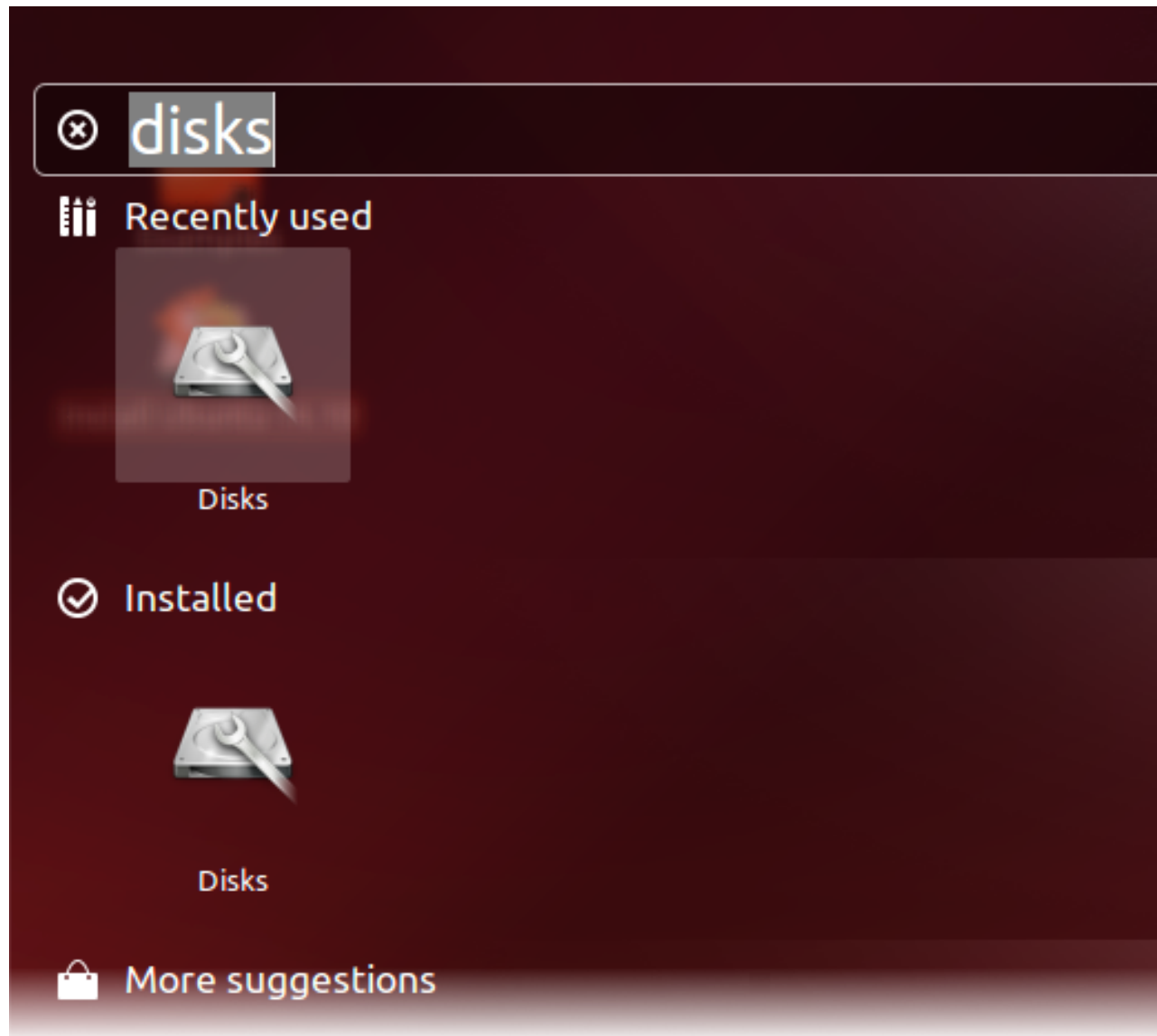


Figure 11.50: Launching Disks

11.5.2 Encrypting a device

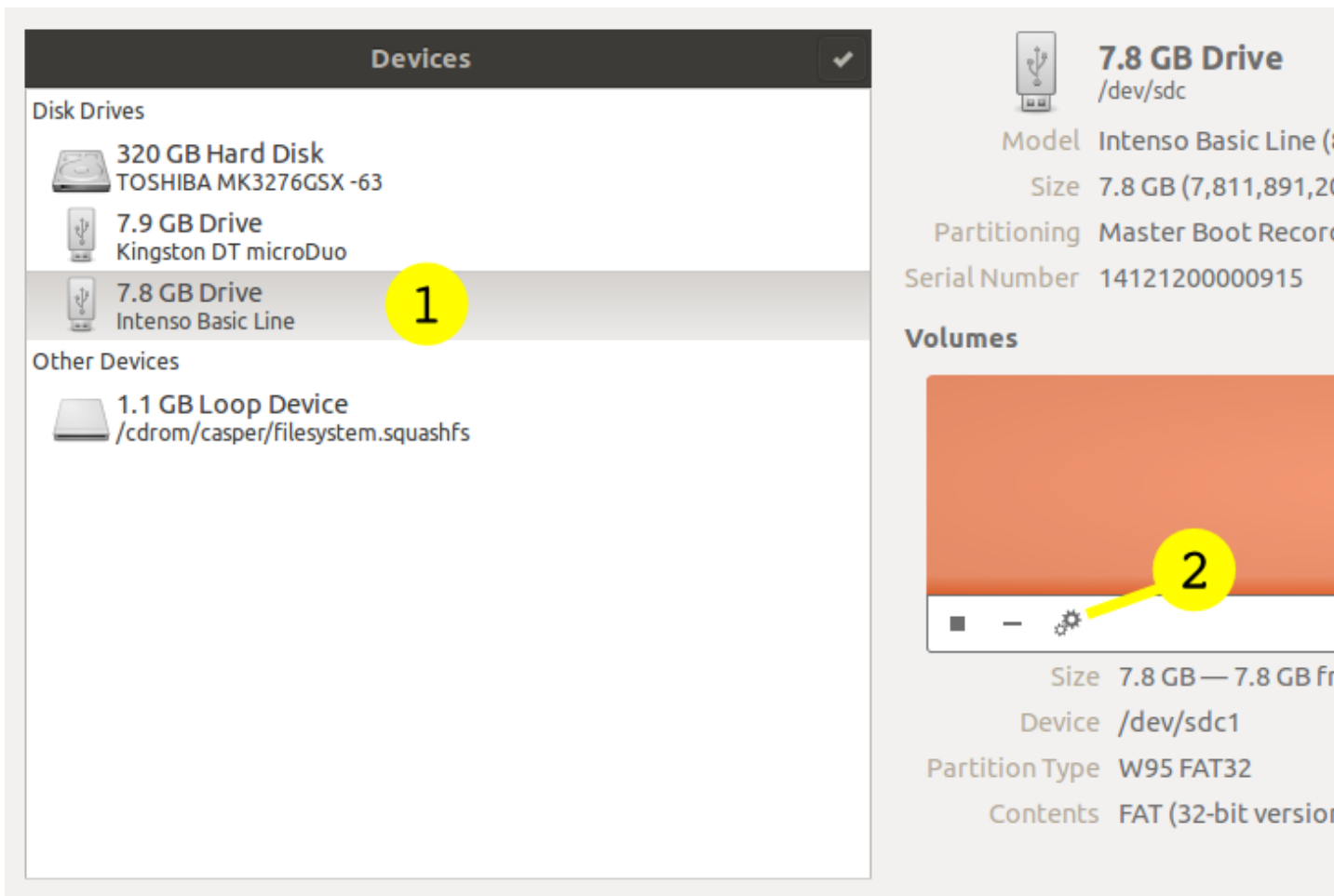


Figure 11.51: Disks main window

On the left hand side you will find a list of all storage devices plugged into your computer.

Select the one you want to encrypt (step 1) (in this case a usb stick), and then on the right hand side, click on the cog wheels and “Format...”. A dialog will appear where you can select if the existing data on the device shall be completely overwritten (that can take up to several hours depending on the size and performance of the device) or just formatted. Please note that even if you choose to encrypt the device, data, that was present before will be recoverable if you don’t choose to overwrite it completely.

No matter what you choose for the field *Erase*, select “Encrypted, compatible with Linux systems (LUKS+Ext4)” for *Type*, give it a name and a strong passphrase (see chapter 8 on that matter), and click *Format...*

On the confirmation screen make sure you selected the correct device as data recovery

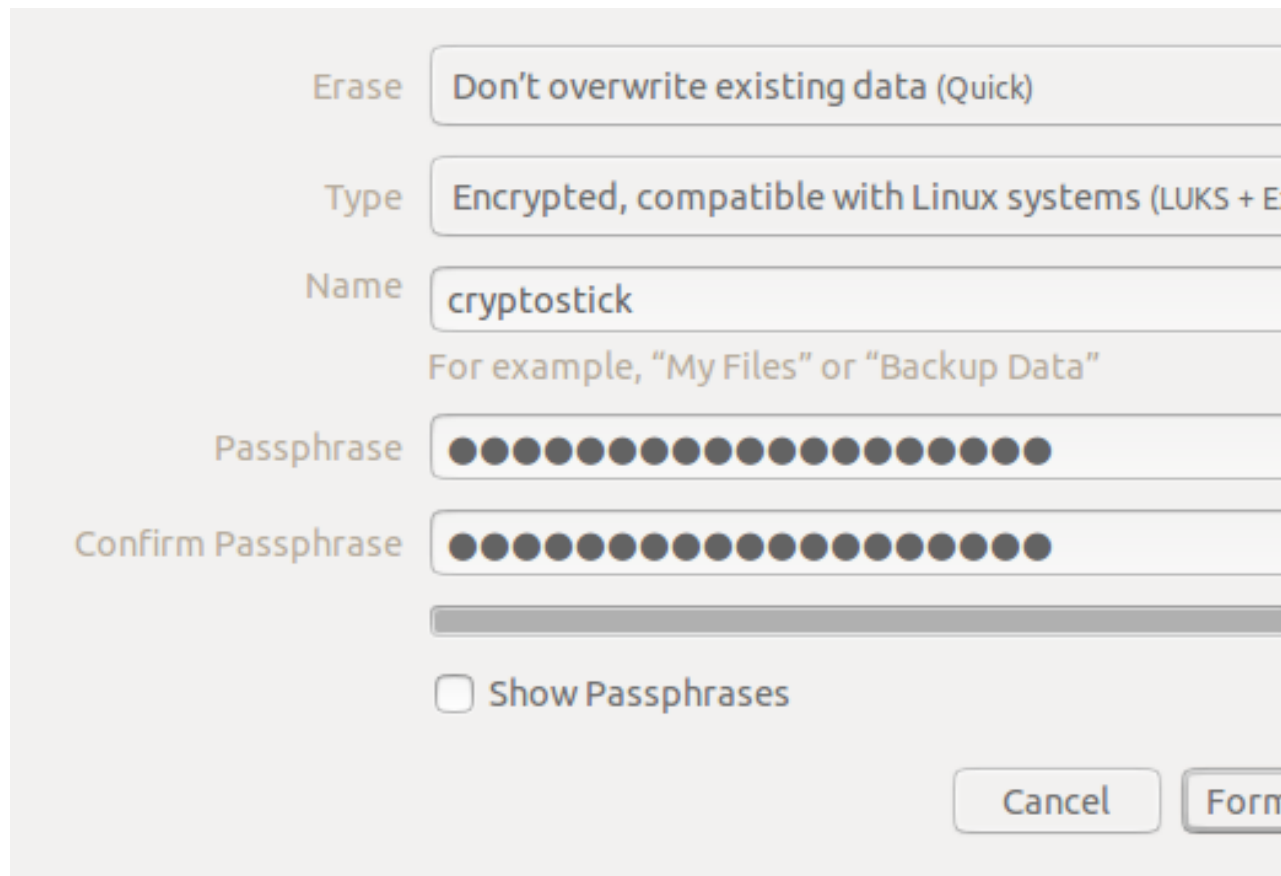


Figure 11.52: “Format...” dialog

is a cumbersome tasks – if possible at all.

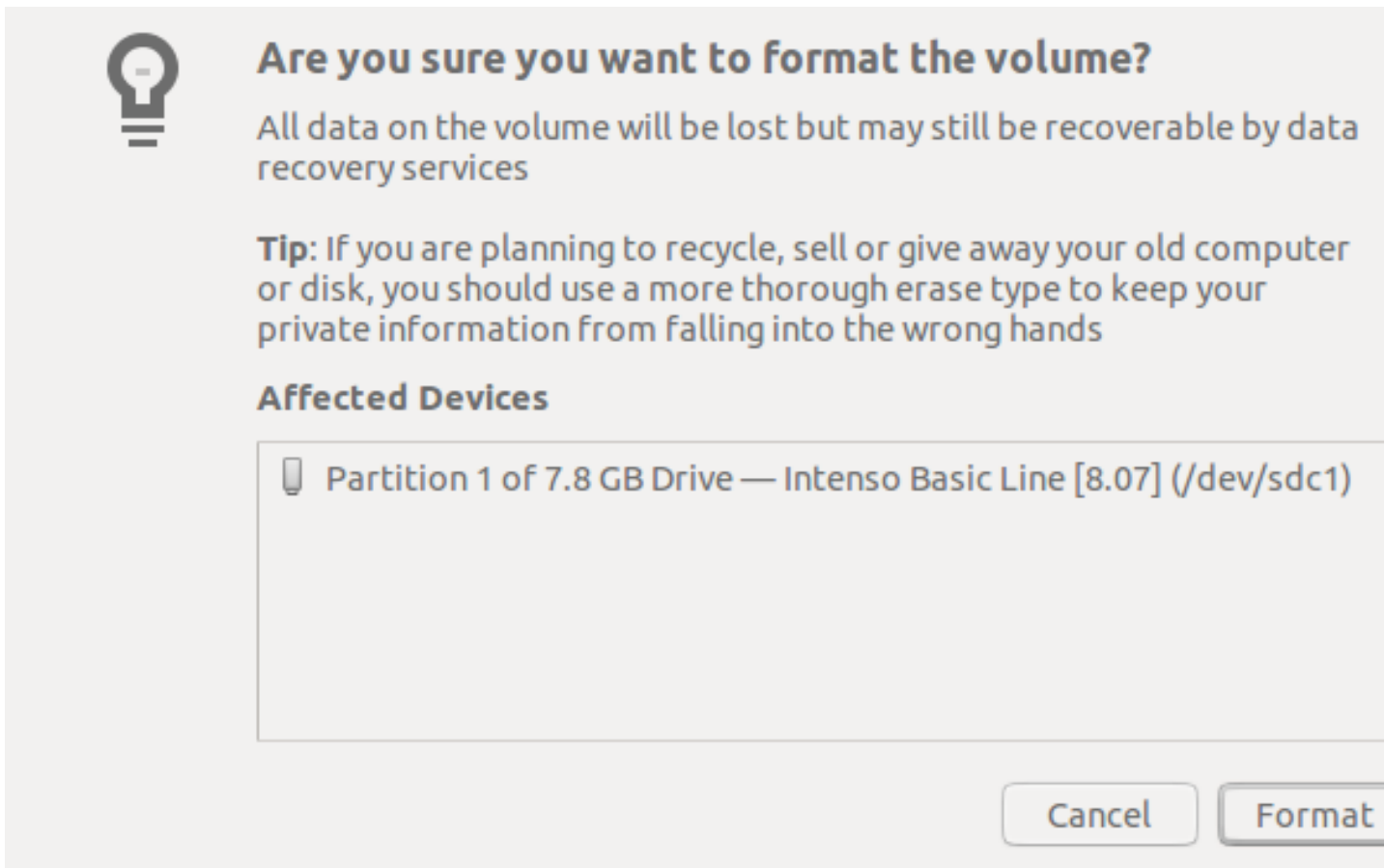


Figure 11.53: Confirmation step

Back on the main window the device now consists of two layers. One is the physical storage (here called “Partition 1”) and the other a virtual device which is created by the LUKS system to give you access to the encrypted device (here called “cryptostick”). The pad lock on “Partition 1” is open as the *Disks* utility needed to open it in order to create a file system (how would you store files on a device without a file system?). You can click on the (other) pad lock as shown below to close the decryption channel and the *eject* button in the upper right corner to safely remove the device.

11 Disk Encryption

The screenshot displays a system's disk management interface. On the left, a 'Devices' panel lists hardware components: a 320 GB Hard Disk (TOSHIBA MK3276GSX -63), a 7.9 GB Drive (Kingston DT microDuo), a 7.8 GB Drive (Intenso Basic Line), and a 1.1 GB Loop Device (/cdrom/casper/filesystem.squashfs). The 7.8 GB Drive is selected. On the right, detailed information for the 7.8 GB Drive (/dev/sdc) is shown, including its model (Intenso Basic Line (8.07)), size (7.8 GB), partitioning scheme (Master Boot Record), and serial number (14121200000915). Below this, the 'Volumes' section shows a partitioning diagram with an orange bar for 'Partition 1' (7.8 GB LUKS) and a grey bar for 'cryptostick' (7.8 GB Ext4). A yellow circle with the number '1' highlights a lock icon in the partitioning controls, indicating that the partition is encrypted.

Devices ✓

Disk Drives

- 320 GB Hard Disk
TOSHIBA MK3276GSX -63
- 7.9 GB Drive
Kingston DT microDuo
- 7.8 GB Drive**
Intenso Basic Line

Other Devices

- 1.1 GB Loop Device
/cdrom/casper/filesystem.squashfs

7.8 GB Drive
/dev/sdc

Model Intenso Basic Line (8.07)
Size 7.8 GB (7,811,891,200 bytes)
Partitioning Master Boot Record
Serial Number 14121200000915

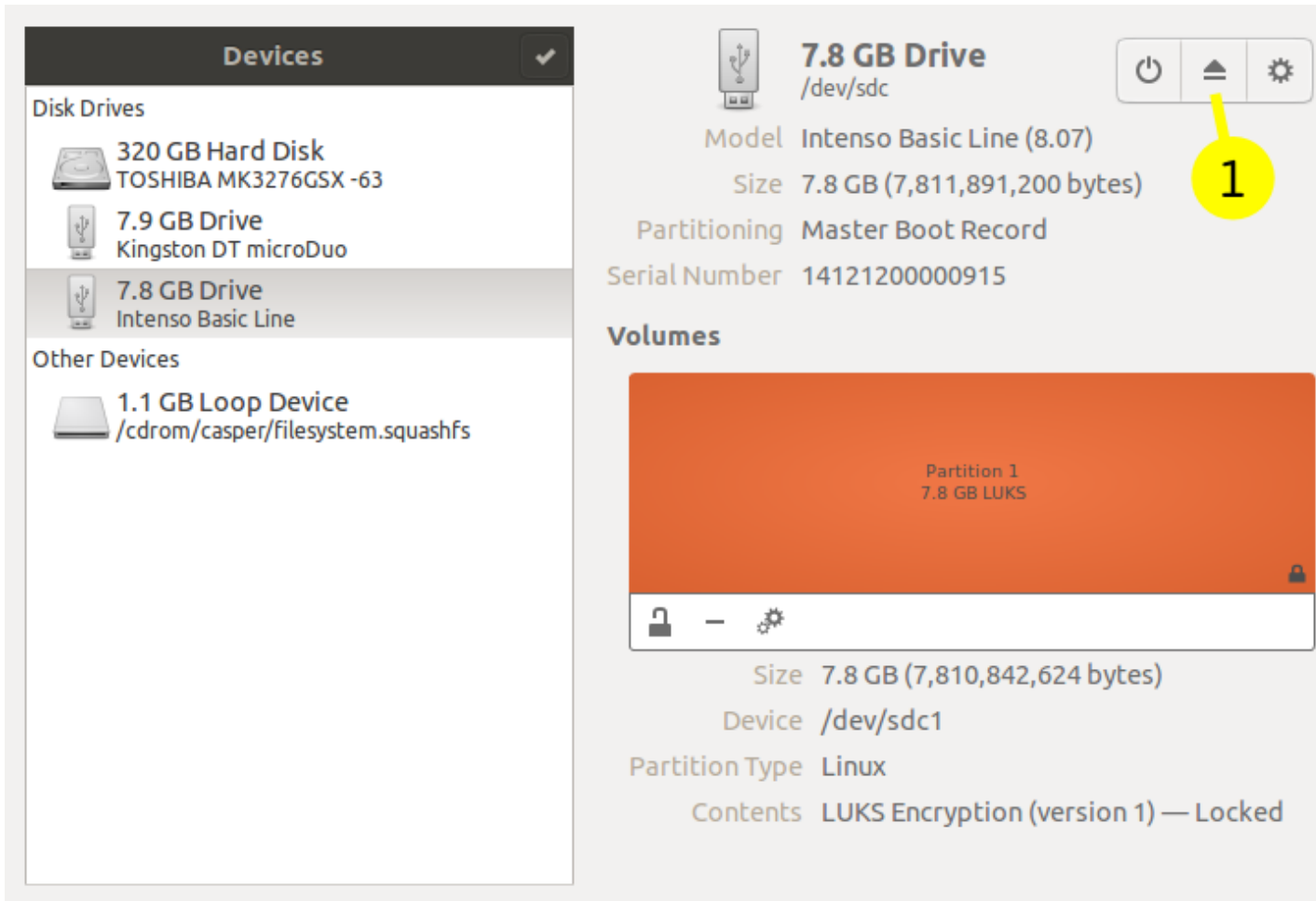
Volumes

Partition 1
7.8 GB LUKS

cryptostick
7.8 GB Ext4

1

Size 7.8 GB (7,810,842,624 bytes)
Device /dev/sdc1
Partition Type Linux
Contents LUKS Encryption (version 1)



11.5.3 Using an encrypted device

This is quite straight-forward. Plug it in, enter the passphrase and click *Connect*. If the file manager does not open automatically, the device will be available when you do.

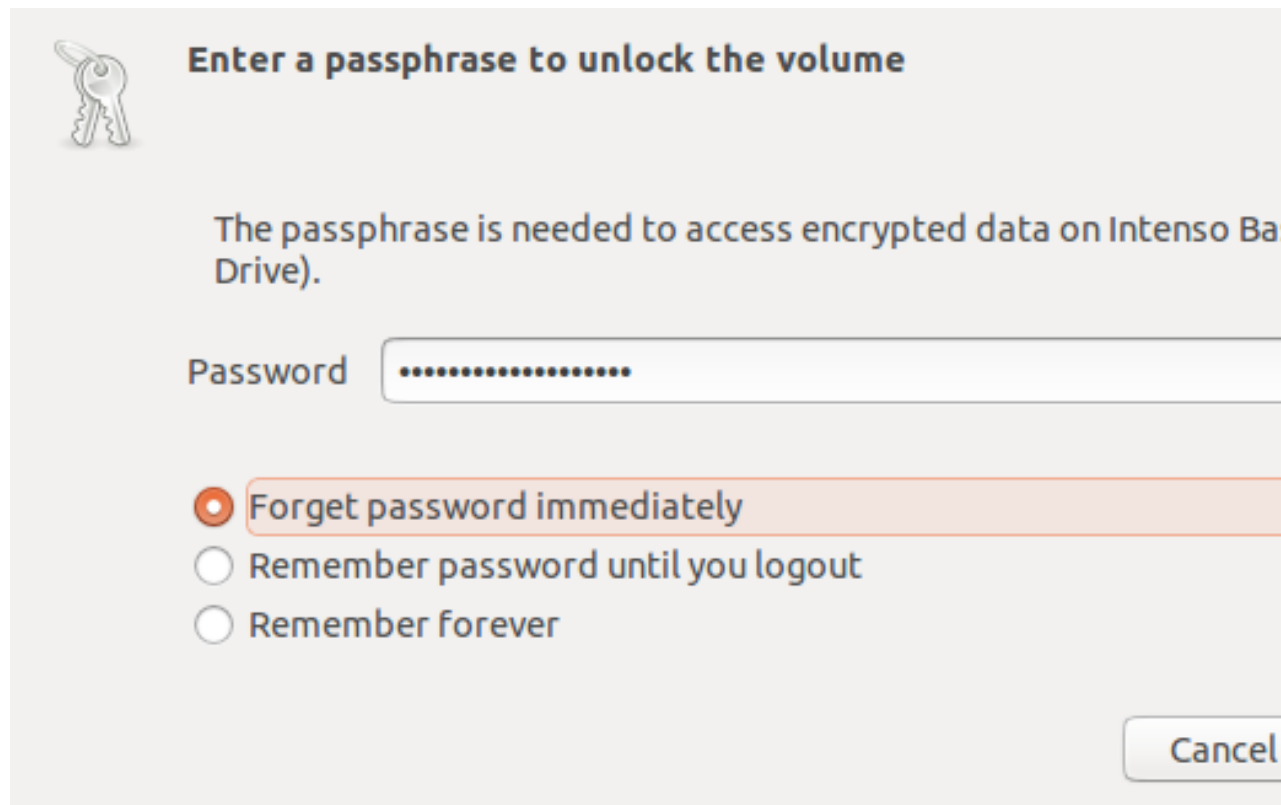


Figure 11.54: Eject the LUKS device

12 Call Encryption

12.1 Installing CSipSimple

CSipSimple is a program for Android devices that allows for making encrypted calls. Naturally the calling software isn't enough on its own and we need a communication network to enable us to make calls.

12.1.1 Introducing The OSTN Network

If you already know about OSTN and have an account, you can skip this section.

The Guardian Project's OSTN (Open {Secure, Source, Standards} Telephony Network - <https://guardianproject.info/wiki/OSTN>) is an attempt to define a standard Voice over IP (VoIP) setup using the Session Initiation Protocol (SIP) that enables end-to-end encrypted calls. Similar to e-mail, SIP allows people to choose their service provider while still being able to call each other even if they are not using the same provider. Yet, not all SIP providers offer OSTN and both providers have to support OSTN for the call to be secure. Once a connection between two people is established, the audio data is exchanged directly between the two parties. Data is encrypted according to the Secure Real-time Transport Protocol (SRTP).

A majority of encrypting VoIP applications currently use Session Description Protocol Security Descriptions for Media Streams (SDES) with hop-by-hop Transport Layer Security (TLS) to exchange secret master keys for SRTP. This method is not end-to-end secure as the SRTP keys are visible in plaintext to any SIP proxy or provider involved in the call.

ZRTP is a cryptographic key-agreement protocol to negotiate the keys for encryption between two parties. ZRTP end points use the media stream rather than the signaling stream to establish the SRTP encryption keys. Since the media stream is a direct connection between the calling parties, there is no way for the SIP providers or proxies to intercept the SRTP keys. ZRTP provides a useful reassurance to end-users that they have a secure line. By reading and comparing a word pair, users can be certain that the key exchange has completed.

Open Secure Telephony (<https://ostel.me/>) is a testbed for OSTN that worked well at the time of writing this book. At https://ostel.me/users/sign_up you can sign up and create an account. You can also check the OSTN page listed above for other providers.

12.1.2 CSipSimple

CSipSimple is a free and open source client for Android that works well with OSTN. You can find it at <https://market.android.com/details?id=com.csipsimple>

To use CSipSimple with ostel.me, select OSTN in the generic wizards when creating an account and enter username, password and server as provided after signing up at https://ostel.me/users/sign_up

Once you call another party with CSipSimple you see a yellow bar with ZRTP and the verification word pair. You now have established a secure voice connection that cannot be intercepted. Still, you should be aware that your phone or the phone of the other party could be set up to record the conversation.

Basic steps:

1. Install CSipSimple from Google Play store or other trusted source
2. Start it up and choose if you want to make SIP calls via data connection or only WiFi
3. Configure your account

To use CSipSimple with ostel.me, select OSTN in the Generic Wizards section when creating an account. You can toggle off the “United States” providers by clicking on “United States”. Now select *OSTN*:

Now you can enter your username (number), password and server (ostel.me) as provided after signing up at https://ostel.me/users/sign_up.

Now you can make a call. The first time you connect to someone with ZRTP you have to verify that the key exchange was successful. In the example below the confirmation word is “cieh”, you can already talk to the other party and make sure you both see the same word. Once done, press ok.

You now have established a secure voice connection that cannot be intercepted. Beware that your or the phone of the other party could be recording your conversation.

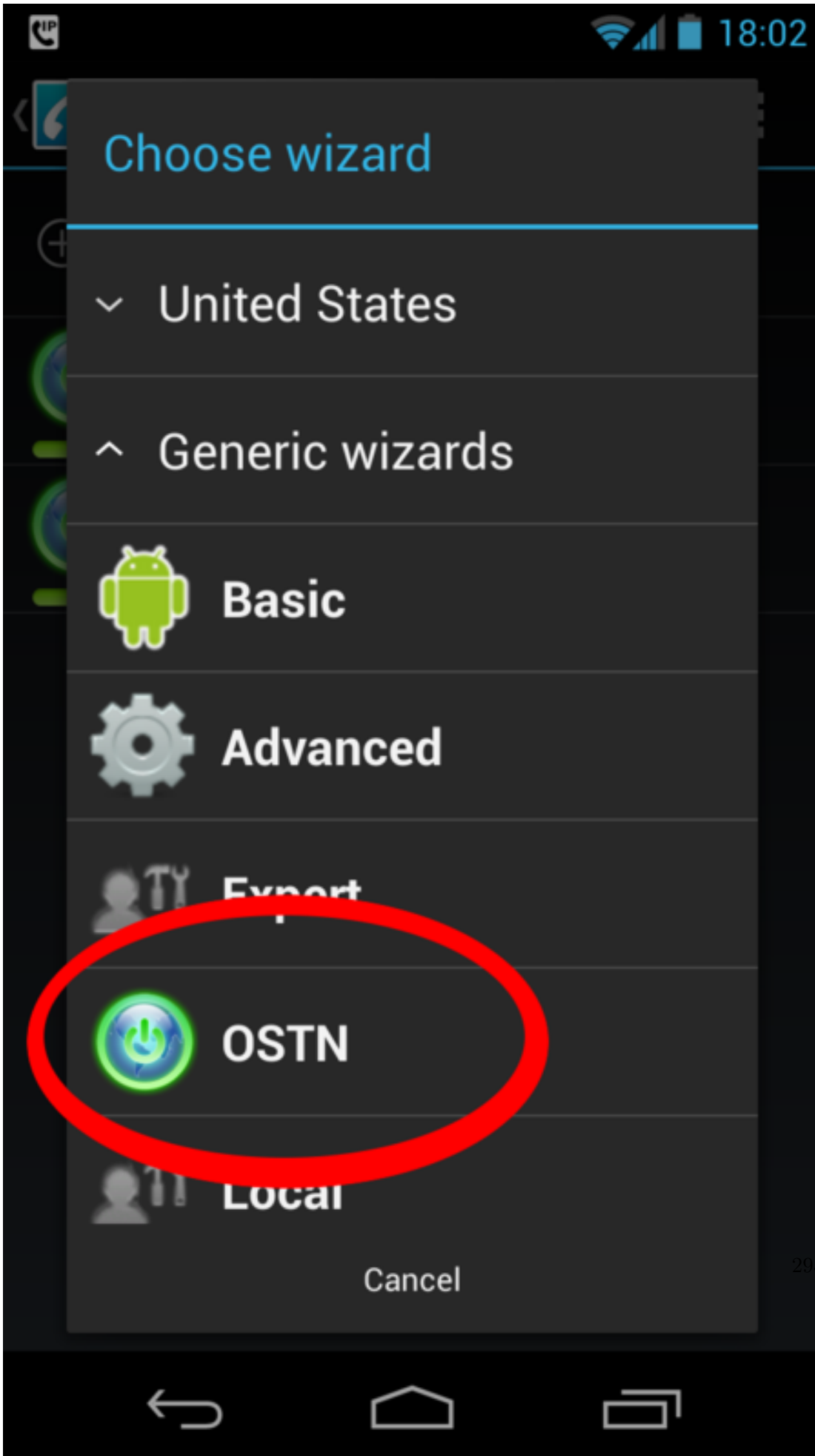
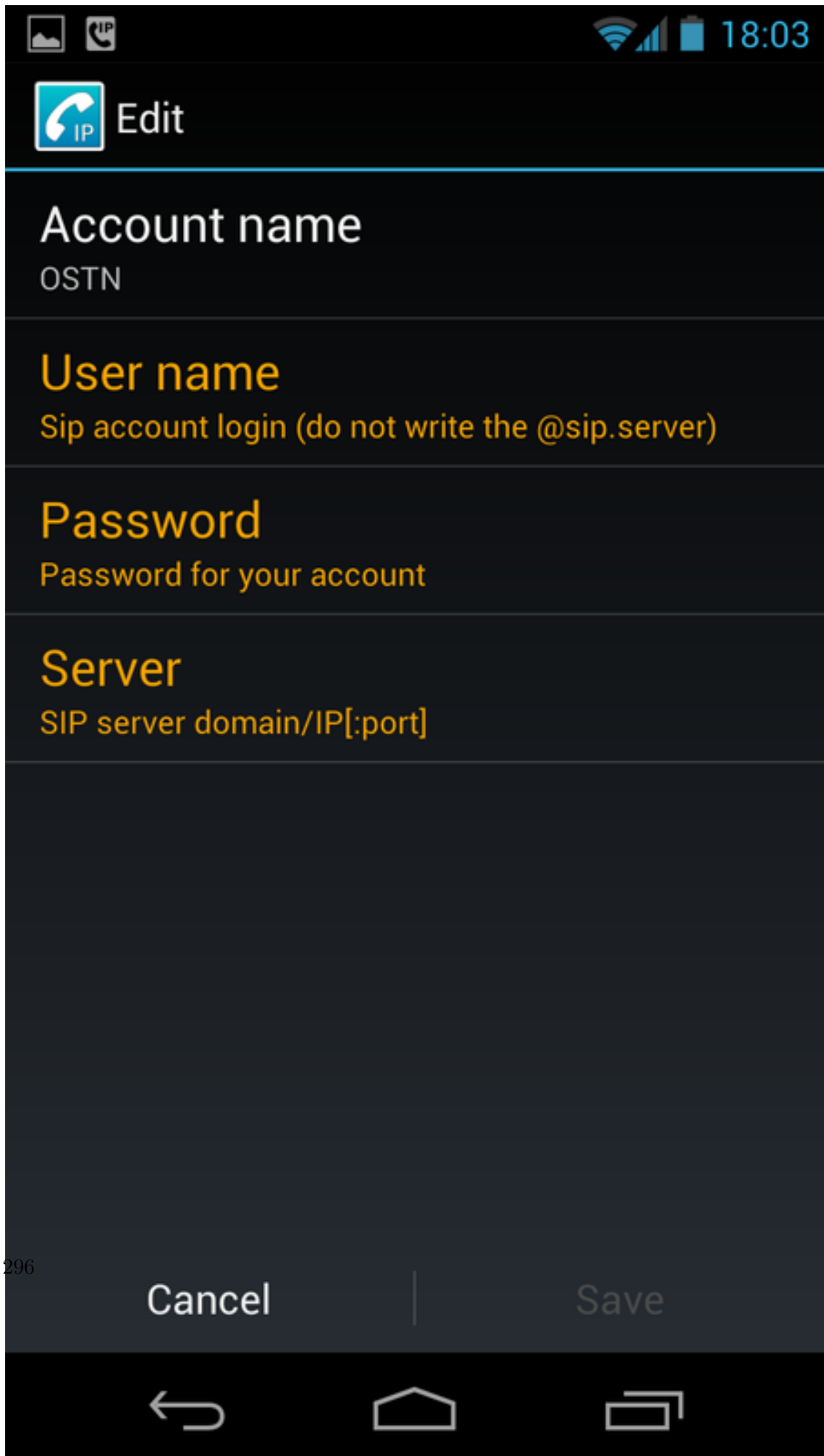


Figure 12.1: OSTN



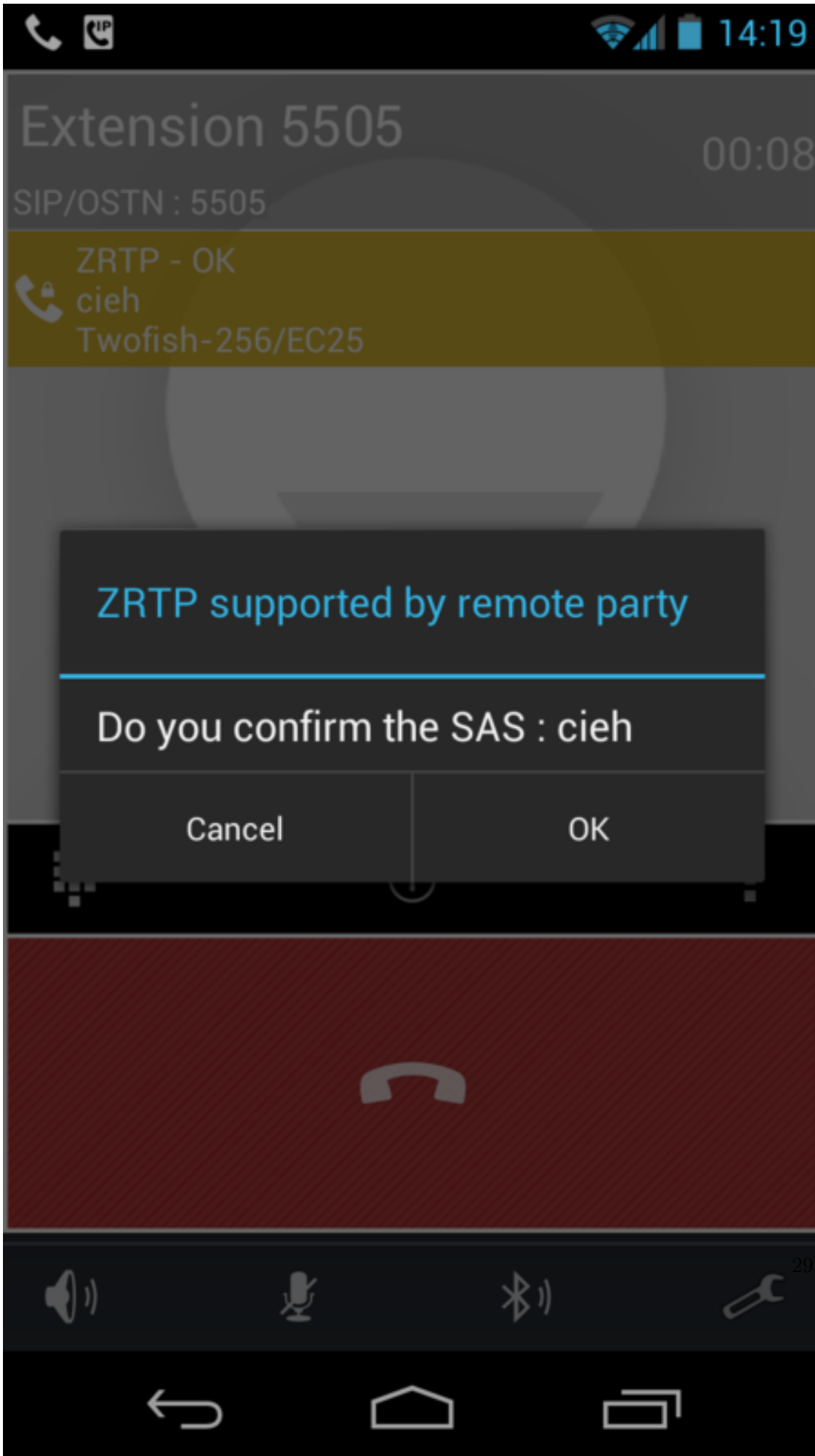


Figure 12.3: OSTN

13 Instant Messaging Encryption

13.1 Setting up Encrypted Instant Messaging

13.1.1 Android - Installing Gibberbot

<https://guardianproject.info/apps/gibber/>

Gibberbot is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. Gibberbot uses the Off-The-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

You can install Gibberbot through the Google Play store or from another trusted source.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

13.1.2 iOS - Installing ChatSecure

<http://chrisballinger.info/apps/chatsecure/>

ChatSecure is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. ChatSecure uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

You can install ChatSecure through the iTunes store

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

13.1.3 Ubuntu - Installing Pidgin

<http://pidgin.im/>

Pidgin is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. Pidgin uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

You can install via Ubuntu Software Center, search for pidgin-otr to install pidgin and the pidgin otr plugin.

Once installed you can enable otr for any account you setup in pidgin.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

13.1.4 OS X - Installing Adium

<http://www.adium.im/>

Adium is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. Adium uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

Installing Adium is similar to installing most Mac OS X applications.

1. Download the Adium disk image from <http://www.adium.im/>.
2. If an Adium window does not open automatically, double click the downloaded file
3. Drag the Adium application to your Applications folder.
4. “Eject” the Adium disk image, which has an icon of a drive
5. The Adium disk image will still be present in your download folder (probably on your desktop). You can drag this file to the trash, as it is no longer needed.
6. To load Adium, locate it in the Applications folder and double click.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

13.1.5 Windows - Installing Pidgin

<http://pidgin.im/>

Pidgin is a secure chat client capable of end-to-end encryption. It works with Google, Facebook, any Jabber or XMPP server. Pidgin uses the Off-the-Record encryption standard (OTR) to enable true verifiable end-to-end encrypted communications.

To use Pidgin with OTR on Windows, you have to install Pidgin and the OTR plugin for Pidgin.

1. Download the latest version of Pidgin for Windows from <http://www.pidgin.im/download/windows/>
2. Run the Pidgin Installer
3. Download the latest version of “OTR plugin for Pidgin” at <http://www.cypherpunks.ca/otr/#downloads>
4. Run the OTR Plugin Installer

Now you can use OTR with any account you setup in Pidgin.

You can securely chat with other programs with OTR support such as Adium, Pidgin on the desktop, Gibberbot on Android or ChatSecure on iOS.

13.1.6 All OS - `crypto.cat`

<https://crypto.cat>

Cryptocat is an open source web application intended to allow secure, encrypted online chatting. Cryptocat encrypts chats on the client side, only trusting the server with data

that is already encrypted. Cryptocat is delivered as a browser extension and offers plugins for Google Chrome, Mozilla Firefox and Apple Safari.

Cryptocat intends to provide means for impromptu, encrypted communications that offer more privacy than services such as Google Talk, while maintaining a higher level of accessibility than other high-level encryption platforms, and furthermore allows for multiple users in one chat room.

13.1.7 Chat Log Files

Some of the Chat Clients listed above e.g. Adium, store plaintext, unencrypted Chat Logs, often by default, even when the OTR “security / privacy” plug-in is installed.

If you are taking OTR precautions to protect your chats from snoopers over the wire or over the air, you should either double check that you have manually switched off Chat Session Logging, or ensure that the Chat Logs you deliberately intend to keep are created on an encrypted disk drive or volume, in case your computer is lost, stolen or seized. It is also worth asking the person you are chatting with if they are inadvertently logging the chat with their own Chat Client software.

14 Secure File Sharing

14.1 Installing I2P on Ubuntu Lucid Lynx (and newer) and derivatives like Linux Mint & Trisquel

1. Open a terminal and enter:

```
sudo apt-add-repository ppa:i2p-maintainers/i2p
```

This command will add the PPA to `/etc/apt/sources.list.d` and fetch the gpg key that the repository has been signed with. The GPG key ensures that the packages have not been tampered with since being built.

2. Notify your package manager of the new PPA by entering

```
sudo apt-get update
```

This command will retrieve the latest list of software from each repository that is enabled on your system, including the I2P PPA that was added with the earlier command.

3. You are now ready to install I2P!

```
sudo apt-get install i2p
```

4. Your browser should open up with your local I2P router console, to browse i2p domains you have to configure your browser to use the i2p proxy. Also check your connection status on the left side on the router console. If your status is **Network: Firewalled** your connection will be rather slow. The first time you start I2P it may take a few minutes to integrate you into the network and find additional peers to optimize your integration, so please be patient.

From the Tools menu, select Options to bring up the Firefox settings panel. Click the icon labelled Advanced, then click on the Network tab. In the Connections section, click on the Settings button. You'll see a Window like the following:

In the Connection Settings window, click the circle next to Manual proxy configuration, then enter 127.0.0.1, port 4444 in the HTTP Proxy field. Enter 127.0.0.1, port 4445 in the SSL Proxy field. Be sure to enter localhost and 127.0.0.1 into the "No Proxy for" box.

For more information and proxy settings for other browsers check <https://www.i2p2.de/htproxyports.htm>

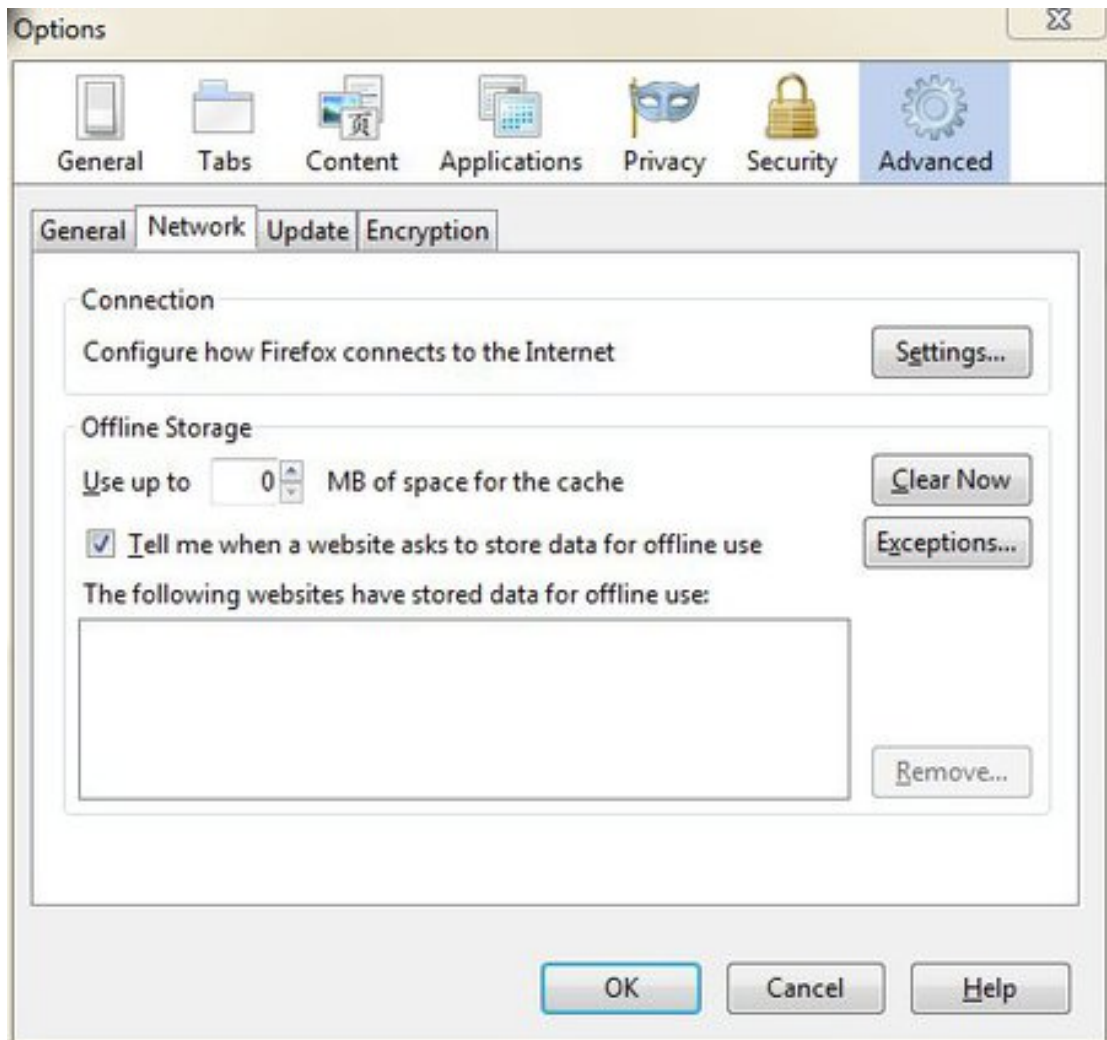


Figure 14.1: I2P

14.1 Installing I2P on Ubuntu Lucid Lynx (and newer) and derivatives like Linux Mint & Trisquel

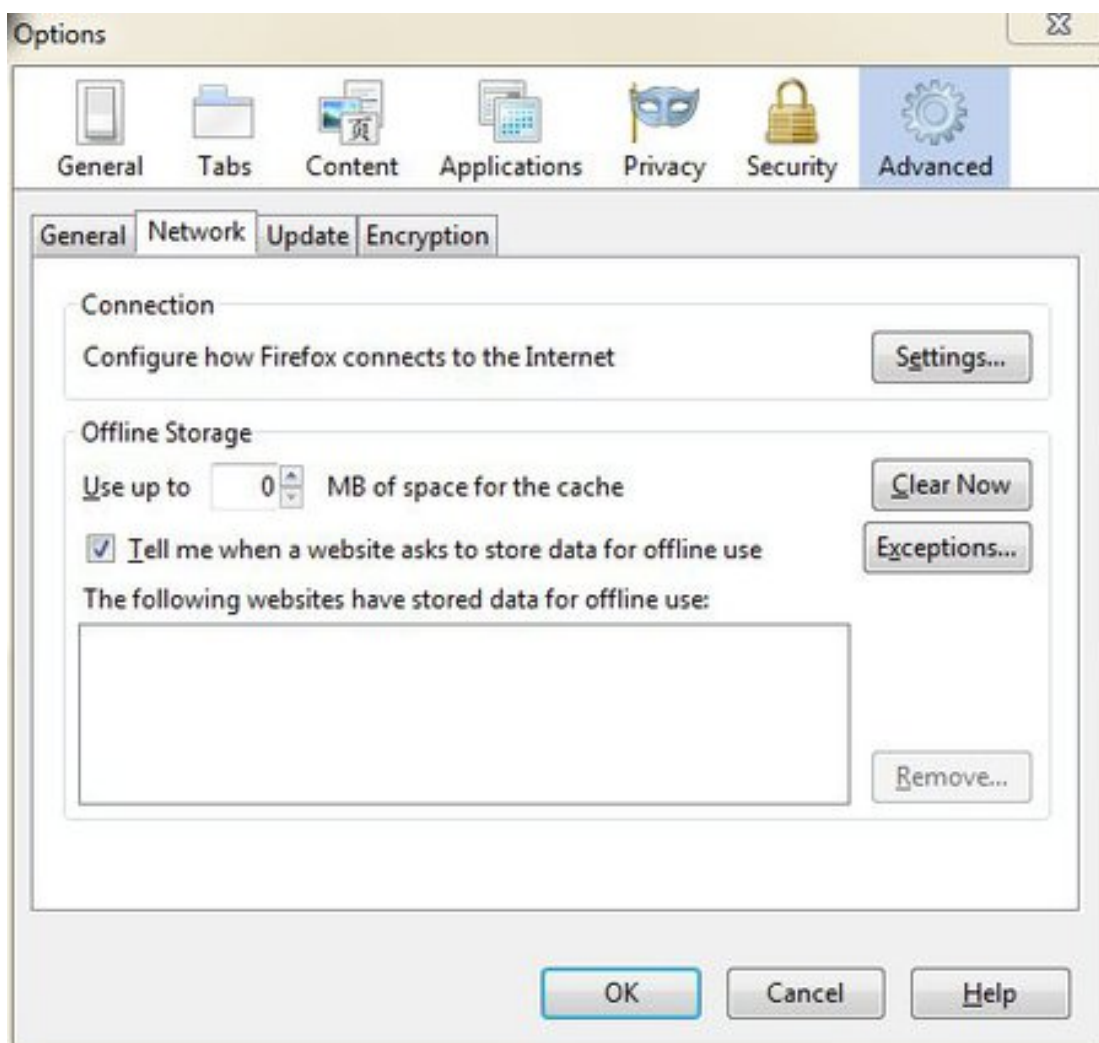


Figure 14.2: I2P

14.2 Instructions for Debian Lenny and newer

For more information visit this page <https://www.i2p2.de/debian.html>

14.3 Starting I2P

Using these I2P packages the I2P router can be started in the following three ways:

- “on demand” using the `i2prouter` script. Simply run “`i2prouter start`” from a command prompt. (Note: Do not use `sudo` or run it as root!).
- as a service that automatically runs when your system boots, even before logging in. The service can be enabled with “`dpkg-reconfigure i2p`” as root or using `sudo`. This is the recommended means of operation.

14.4 Anonymous Bittorrent with I2PSnark

We can use the I2P network to share and download files without the entire world knowing who is sharing them. or even the fact that you are running a torrent client, since i2p network is end-to-end encrypted the only thing known to outsider is you are running I2P.

I2p come with a built-in torrent client that run inside the browser called I2PSnark. You can access it through this direct link:

<http://localhost:7657/i2psnark/>

or through the router console: <http://localhost:7657/> and clicking on the torrent icon. Once started you should see a screen similar to the following:



Figure 14.3: I2P

You can search for a torrent using one of following bittorrent trackers:

- <http://tracker.postman.i2p/>
- <http://diftracker.i2p/>

Copy the torrent or magnet link and past it in the I2PSnark window, and click **Add torrent**. the file will be downloaded inside the `/home/user/.i2p/i2psnark` folder.

NOTE:

- Since I2P is a closed network, you can't download normal torrents found on regular internet with it, and it can't be used to make downloading them anonymous!
- The speed seems to be slightly lower than usual which is caused by the anonymization. I think that the download rates are still acceptable if you consider that you download and share anonymously.

15 Appendices

0xcaca0 Adam Hyde Ahmed Mansour Alice Miller A Ravi Ariel Viera Asher Wolf AT Austin Martin Ben Weissmann Bernd Fix Brendan Howell Brian Newbold Carola Hesse Chris Pinchen Dan Hassan Daniel Kinsman Danja Vasiliev DÃl'vai NaÃl'ndor djmat-tyg007 Douwe Schmidt Edward Cherlin Elemar Emile Denichaud Emile den Tex Erik Stein Erinn Clark Freddy Martinez Freerk Ohling Greg Broiles Haneef Mubarak Helen varley jamieson Janet Swisher Jan Gerber Jannette Mensch Jens Kubieziel jmorahan Josh Datko Joshua Datko Julian Oliver Kai Engert Karen Reilly l3lackEyedAngels leoj3n LiamO Lonneke van der Velden Malte Malte Dik Marta Peirano Mart van Santen mdimitrova Michael Henriksen Nart Villeneuve Nathan Andrew Fain Nathan Houle Niels Elgaard Larsen Petter Ericson Piers Plato Punkbob Roberto Rastapopoulos Ronald Deibert Ross Anderson Sacha van Geffen Sam Tennyson Samuel Carlisle Samuel L. Tennyson Seth Schoen Steven Murdoch StooJ Story89 Ted W Ted Wood Teresa Dillon therealplato Tomas Krag Tom Boyle Travis Tueffel Uwe Lippmann WillMorrison Ximin Luo Yuval Adam zandi Zorrino Zorrinno

15.1 Cryptography and Encryption

Cryptography and encryption are similar terms, the former being the science and latter the implementation of it. The history of the subject can be traced back to ancient civilisations, when the first humans began to organise themselves into groups. This was driven in part by the realisation that we were in competition for resources and tribal organisation, warfare and so forth were necessary, so as to keep on top of the heap. In this respect cryptography and encryption are rooted in warfare, progression and resource management, where it was necessary to send secret messages to each other without the enemy deciphering ones moves.

Writing is actually one of the earliest forms of cryptography as not everyone could read. The word cryptography stems from the Greek words *kryptos* (hidden) and *graphein* (writing). In this respect cryptography and encryption in their simplest form refer to the writing of hidden messages, which require a system or rule to decode and read them. Essentially this enables you to protect your privacy by scrambling information in a way that it is only recoverable with certain knowledge (passwords or passphrases) or possession (a key).

Put in another way, encryption is the translation of information written in plaintext into a non-readable form (ciphertext) using algorithmic schemes (ciphers). The goal is to use the right key to unlock the ciphertext and return it back into its original plaintext form so it becomes readable again.

Although most encryption methods refer to written word, during World War Two, the US military used Navajo Indians, who traveled between camps sending messages in their native tongue. The reason the army used the Navajo tribe was to protect the information they were sending from the Japanese troops, who famously could not decipher the Navajo's spoken language. This is a very simple example of using a language to send messages that you do not want people to listen into or know what you're discussing. Why is encryption important? _____

Computer and telecommunication networks store digital echoes or footprints of our thoughts and records of personal lives.

From banking, to booking, to socialising: we submit a variety of detailed, personalised information, which is driving new modes of business, social interaction and behavior. We have now become accustomed to giving away what was (and still is) considered private information in exchange for what is presented as more personalised and tailored services, which might meet our needs, but cater to our greed.

But how do we protect who sees, controls and uses this information?

Lets consider a scenario whereby we all thought it was fine to send all our communication on open handwritten postcards. From conversations with your doctor, to intimate moments with our lovers, to legal discussions you may have with lawyers or accountants. It's unlikely that we would want all people to be able to read such communications. So instead we have written letters in sealed envelopes, tracking methods for sending post, closed offices and confidential agreements, which help to keep such communication private. However given the shift in how we communicate, much more of this type of interaction is taking place online. More importantly it is taking place through online spaces, which are not private by default and open to people with little technical skills to snoop into the matters that can mean the most to our lives.

Online privacy and encryption is something we therefore need to be aware of and practice daily. In the same way we would put an important letter into an envelope or have a conversation behind a closed door. Given that so much of our private communication is now happening in networked and online spaces, we should consider the interface, like envelopes or seals, which protect this material as a basic necessity and human right.

15.1.1 Encryption examples

Throughout history we can find examples of cipher methods, which have been used to keep messages private and secret.

15.1.2 A Warning!

“There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files” - Bruce Schneier, Applied Cryptography, 1996

This chapter first explains a number of historical cryptographic systems and then provides a summary of modern techniques. The historical examples illustrate how cryp-

tography emerged, but are considered broken in the face of modern computers. They can be fun to learn, but please don't use them for anything sensitive!

15.1.3 Historical ciphers

Classical ciphers refer to historical ciphers, which are now out of popular use or no longer applicable. There are two general categories of classical ciphers: transposition and substitution ciphers.

In a transposition cipher, the letters themselves are kept unchanged, but the order within the message is scrambled according to some well-defined scheme. An example of a transposition cipher is Skytale, which was used in ancient Rome and Greece. A paperstrip was wrapped around a stick and the message written across it. That way the message could not be read unless wound around a stick of similar diameter again.



Figure 15.1: Cryptography

Image: Skytale taken from Wikimedia Commons (3.10.12)

A substitution cipher is a form of classical cipher whereby letters or groups of letters are systematically replaced throughout the message for other letters (or groups of letters). Substitution ciphers are divided into monoalphabetic and polyalphabetic substitutions. The Caesar Shift cipher is common example of amonoalphabetic substitution ciphers, where the letters in the alphabet are shifted in one direction or another.

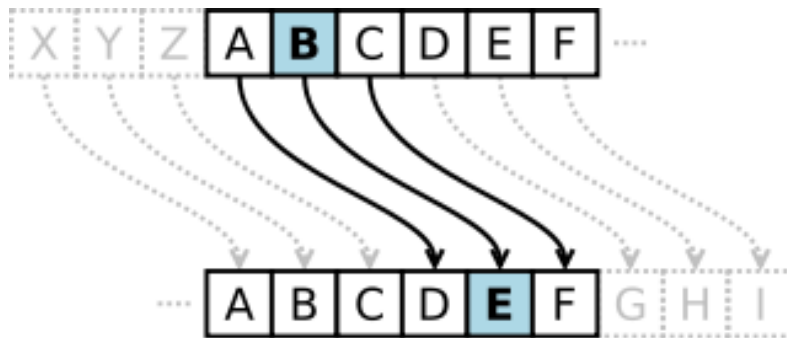


Figure 15.2: Cryptography

Image: Caesar Shift Cipher taken from Wikimedia Commons (3.10.12)

Polyalphabetic substitutions are more complex than substitution ciphers as they use more than one alphabet and rotate them. For example, The Alberti cipher, which was the

first polyalphabetic cipher was created by Leon Battista Alberti, a 15th century Italian, Renaissance polymath and humanist who is also credited as the godfather of western cryptography. His cipher is similar to the Vigenère cipher, where every letter of the alphabet gets a unique number (e.g. 1-26). The message is then encrypted by writing down the message along with the password repeatedly written beneath it.

In the Vigenère cipher the corresponding numbers of the letters of message and key are summed up (with numbers exceeding the alphabet being dragged around the back) making the message so unreadable that it couldn't be deciphered for centuries (nowadays, with the help of computers, this obviously isn't true anymore).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 15.3: Cryptography

Image: VigenÃre cipher taken from Wikimedia Commons (3.10.12)

During World War 2 there was a surge in cryptography, which led to the development of new algorithms such as the one-time pad (OTP). The OTP algorithm combines plaintext with a random key that is as long as the plaintext so that each character is only used once. To use it you need two copies of the pad, which are kept by each user and exchanged via a secure channel. Once the message is encoded with the pad, the pad is destroyed and the encoded message is sent. On the recipient's side, the encoded message has a duplicate copy of the pad from which the plaintext message is generated. A good way to look at OTP is to think of it as a 100% noise source, which is used to mask the message. Since both parties of the communication have copies of the noise source they are the only people who can filter it out.

OTP lies behind modern day stream ciphers, which are explained below. Claude Shannon, (a key player in modern cryptography and information theory), in his seminal 1949 paper "Communication Theory of Secrecy Systems" demonstrated that theoretically all unbreakable ciphers should include the OTP encryption, which if used correctly are impossible to crack.

15.1.4 Modern ciphers

Post the World Wars the field of cryptography became less of a public service and fell more within the domain of governance. Major advances in the field began to reemerge in the mid-1970s with the advent of personalised computers and the introduction of the Data Encryption Standard (DES, developed at IBM in 1977 and later adopted by the U.S government). Since 2001 we now use the AES, Advanced Encryption Standard), which is based on symmetric cryptography forms.

Contemporary cryptography can be generally divided into what is called symmetric, asymmetric and quantum cryptography.

Symmetric cryptography, or secret key, cryptography refers to ciphers where the same key is used to both encrypt and decrypt the text or information involved. In this class of ciphers the key is shared and kept secret within a restricted group and therefore it is not possible to view the encrypted information without having the key. A simple analogy to secret key cryptography is having access to a community garden, which has one key to open gate, which is shared by the community. You cannot open the gate, unless you have the key. Obviously the issue here with the garden key and with symmetric cryptography is if the key falls into the wrong hands, then an intruder or attacker can get in and the security of the garden, or the data or information is compromised. Consequently one of the main issues with this form of cryptography is the issue of key management. As a result this method is best employed within single-user contexts or small group environments.

Despite this limitation symmetric key methods are considerably faster than asymmetric methods and so are the preferred mechanism for encrypting large chunks of text.

Symmetric ciphers are usually implemented using **block ciphers** or **stream ciphers**.

Block ciphers work by looking at the input data in 8 or 16 or 32 byte blocks at a time and spreading the input and key within those blocks. Different modes of operation are performed on the data in order to transform and spread the data between blocks. Such

ciphers use a secret key to convert a fixed block of plain text into cipher text. The same key is then used to decrypt the cipher text.

In comparison stream ciphers (also known as state cipher) work on each plaintext digit by creating a corresponding keystream which forms the ciphertext. The keystream refers to a stream of random characters (bits, bytes, numbers or letters) on which various additive or subtractive functions are performed and combined to a character in the plaintext message, which then produces the ciphertext. Although this method is very secure, it is not always practical, since the key of the same length as the message needs to be transmitted in some secure way so that receiver can decypher the message. Another limitation is that the key can only be used once and then its discarded. Although this can mean almost watertight security, it does limit the use of the cipher.

Asymmetric ciphers work much more complex mathematical problems with back doors, enabling faster solutions on smaller, highly important pieces of data. They also work on fixed data sizes, typically 1024-2048 bits and and 384 bits. What makes them special is that they help solve some of the issues with key distribution by allocating one public and one private pair per person, so that everyone just needs to know everyone else's public portion. Asymmetric ciphers are also used for digital signatures. Where as symmetric ciphers are generally used for message authenticity. Symmetric ciphers cannot non-repudiation signatures (i.e., signatures that you cannot later deny that you did not sign). Digital signatures are very important in modern day cryptography. They are similar to wax seals in that they verify who the message is from and like seals are unique to that person. Digital signatures are one of the methods used within public key systems, which have transformed the field of cryptography are central to modern day Internet security and online transactions.

15.1.5 Quantum Cryptography

Quantum cryptography is the term used to describe the type of cryptography that is now necessary to deal with the speed at which we now process information and the related security measures that are necessary. Essentially it deals with how we use quantum communication to securely exchange a key and its associated distribution. As the machines we use become faster the possible combinations of public-key encryption and digital signatures becomes easier to break and quantum cryptography deals with the types of algorithms that are necessary to keep pace with more advanced networks.

15.1.6 Challenges & Implications

At the heart of cryptography lies the challenge of how we use and communicate information. The above methods describe how we encrypt written communication but obviously as shown in the Navajo example other forms of communication (speech, sound, image etc) can also be encrypted using different methods.

The main goal and skill of encryption is to apply the right methods to support trustworthy communication. This is achieved by understanding the tradeoffs, strengths and weaknesses of different cipher methods and how they relate to the level of security and

privacy required. Getting this right depends on the task and context.

Importantly when we speak about communication, we are speaking about trust. Traditionally cryptography dealt with the hypothetical scenarios, where the challenge was to address how ‘Bob’ could speak to ‘Alice’ in a private and secure manner.

Our lives are now heavily mediated via computers and the Internet. So the boundaries between Bob, Alice + the ‘other’ (Eve, Oscar, Big Brother, your boss, ex-boyfriend or the government) are a lot more blurred. Given the quantum leaps in computer processing, in order for ‘us’, Bob’s and Alice’s to have trust in the system, we need to know who we are talking too, we need to know who is listening and importantly who has the potential to eavesdrop. What becomes important is how we navigate this complexity and feel in control and secure, so that you can engage and communicate in a trustful manner, which respects our individual freedoms and privacy.

15.2 Glossary

Much of this content is based on <http://en.cship.org/wiki/Special:Allpages>

15.2.1 aggregator

An aggregator is a service that gathers syndicated information from one or many sites and makes it available at a different address. Sometimes called an RSS aggregator, a feed aggregator, a feed reader, or a news reader. (Not to be confused with a Usenet News reader.)

15.2.2 anonymity

(Not be confused with privacy, pseudonymity, security, or confidentiality.)

Anonymity on the Internet is the ability to use services without leaving clues to one’s identity or being spied upon. The level of protection depends on the anonymity techniques used and the extent of monitoring. The strongest techniques in use to protect anonymity involve creating a chain of communication using a random process to select some of the links, in which each link has access to only partial information about the process. The first knows the user’s Internet address (IP) but not the content, destination, or purpose of the communication, because the message contents and destination information are encrypted. The last knows the identity of the site being contacted, but not the source of the session. One or more steps in between prevents the first and last links from sharing their partial knowledge in order to connect the user and the target site.

15.2.3 anonymous remailer

An anonymous remailer is a service that accepts e-mail messages containing instructions for delivery, and sends them out without revealing their sources. Since the remailer has access to the user’s address, the content of the message, and the destination of the

message, remailers should be used as part of a chain of multiple remailers so that no one remailer knows all this information.

15.2.4 ASP (application service provider)

An ASP is an organization that offers software services over the Internet, allowing the software to be upgraded and maintained centrally.

15.2.5 backbone

A backbone is one of the high-bandwidth communications links that tie together networks in different countries and organizations around the world to form the Internet.

15.2.6 badware

See malware.

15.2.7 bandwidth

The bandwidth of a connection is the maximum rate of data transfer on that connection, limited by its capacity and the capabilities of the computers at both ends of the connection.

15.2.8 bash (Bourne-again shell)

The bash shell is a command-line interface for Linux/Unix operating systems, based on the Bourne shell.

15.2.9 BitTorrent

BitTorrent is a peer-to-peer file-sharing protocol invented by Bram Cohen in 2001. It allows individuals to cheaply and effectively distribute large files, such as CD images, video, or music files.

15.2.10 blacklist

A blacklist is a list of forbidden things. In Internet censorship, lists of forbidden Web sites or the IP addresses of computers may be used as blacklists; censorware may allow access to all sites except for those specifically listed on its blacklist. An alternative to a blacklist is a whitelist, or a list of permitted things. A whitelist system blocks access to all sites except for those specifically listed on the whitelist. This is a less common approach to Internet censorship. It is possible to combine both approaches, using string matching or other conditional techniques on URLs that do not match either list.

15.2.11 bluebar

The blue URL bar (called the Bluebar in Psiphon lingo) is the form at the top of your Psiphon node browser window, which allows you to access blocked site by typing its URL inside.

See also Psiphon node

15.2.12 block

To block is to prevent access to an Internet resource, using any number of methods.

15.2.13 bookmark

A bookmark is a placeholder within software that contains a reference to an external resource. In a browser, a bookmark is a reference to a Web page – by choosing the bookmark you can quickly load the Web site without needing to type in the full URL.

15.2.14 bridge

See Tor bridge.

15.2.15 brute-force attack

A brute force attack consists of trying every possible code, combination, or password until you find the right one. These are some of the most trivial hacking attacks.

15.2.16 cache

A cache is a part of an information-processing system used to store recently used or frequently used data to speed up repeated access to it. A Web cache holds copies of Web page files.

15.2.17 censor

To censor is to prevent publication or retrieval of information, or take action, legal or otherwise, against publishers and readers.

15.2.18 censorware

Censorware is software used to filter or block access to the Internet. This term is most often used to refer to Internet filtering or blocking software installed on the client machine (the PC which is used to access the Internet). Most such client-side censorware is used for parental control purposes.

Sometimes the term censorware is also used to refer to software used for the same purpose installed on a network server or router.

15.2.19 CGI (Common Gateway Interface)

CGI is a common standard used to let programs on a Web server run as Web applications. Many Web-based proxies use CGI and thus are also called “CGI proxies”. (One popular CGI proxy application written by James Marshall using the Perl programming language is called CGIProxy.)

15.2.20 chat

Chat, also called instant messaging, is a common method of communication among two or more people in which each line typed by a participant in a session is echoed to all of the others. There are numerous chat protocols, including those created by specific companies (AOL, Yahoo!, Microsoft, Google, and others) and publicly defined protocols. Some chat client software uses only one of these protocols, while others use a range of popular protocols.

15.2.21 cipher

In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption

15.2.22 circumvention

Circumvention is publishing or accessing content in spite of attempts at censorship.

15.2.23 Common Gateway Interface

See CGI.

15.2.24 command-line interface

A method of controlling the execution of software using commands entered on a keyboard, such as a Unix shell or the Windows command line.

15.2.25 cookie

A cookie is a text string sent by a Web server to the user’s browser to store on the user’s computer, containing information needed to maintain continuity in sessions across multiple Web pages, or across multiple sessions. Some Web sites cannot be used without accepting and storing a cookie. Some people consider this an invasion of privacy or a security risk.

15.2.26 country code top-level domain (ccTLD)

Each country has a two-letter country code, and a TLD (top-level domain) based on it, such as .ca for Canada; this domain is called a country code top-level domain. Each

such ccTLD has a DNS server that lists all second-level domains within the TLD. The Internet root servers point to all TLDs, and cache frequently-used information on lower-level domains.

15.2.27 cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

15.2.28 DARPA (Defense Advanced Projects Research Agency)

DARPA is the successor to ARPA, which funded the Internet and its predecessor, the ARPAnet.

15.2.29 decryption

Decryption is recovering plain text or other messages from encrypted data with the use of a key.

See also encryption.

15.2.30 disk encryption

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage.

15.2.31 domain

A domain can be a Top-Level Domain (TLD) or secondary domain on the Internet.

See also Top-Level Domain, country code Top-Level Domain and secondary domain.

15.2.32 DNS (Domain Name System)

The Domain Name System (DNS) converts domain names, made up of easy-to-remember combinations of letters, to IP addresses, which are hard-to-remember strings of numbers. Every computer on the Internet has a unique address (a little bit like an area code+telephone number).

15.2.33 DNS leak

A DNS leak occurs when a computer configured to use a proxy for its Internet connection nonetheless makes DNS queries without using the proxy, thus exposing the user's attempts to connect with blocked sites. Some Web browsers have configuration options to force the use of the proxy.

15.2.34 DNS server

A DNS server, or name server, is a server that provides the look-up function of the Domain Name System. It does this either by accessing an existing cached record of the IP address of a specific domain, or by sending a request for information to another name server.

15.2.35 DNS tunnel

A DNS tunnel is a way to tunnel almost everything over DNS/Nameservers.

Because you "abuse" the DNS system for an unintended purpose, it only allows a very slow connection of about 3 kb/s which is even less than the speed of an analog modem. That is not enough for YouTube or file sharing, but should be sufficient for instant messengers like ICQ or MSN Messenger and also for plain text e-mail.

On the connection you want to use a DNS tunnel, you only need port 53 to be open; therefore it even works on many commercial Wi-Fi providers without the need to pay.

The main problem is that there are no public modified nameservers that you can use. You have to set up your own. You need a server with a permanent connection to the Internet running Linux. There you can install the free software OzymanDNS and in combination with SSH and a proxy like Squid you can use the tunnel. More Information on this on <http://www.dnstunnel.de>.

15.2.36 Eavesdropping

Eavesdropping is listening to voice traffic or reading or filtering data traffic on a telephone line or digital data connection, usually to detect or prevent illegal or unwanted activities or to control or monitor what people are talking about.

15.2.37 e-mail

E-mail, short for electronic mail, is a method to send and receive messages over the Internet. It is possible to use a Web mail service or to send e-mails with the SMTP protocol and receive them with the POP3 protocol by using an e-mail client such as Outlook Express or Thunderbird. It is comparatively rare for a government to block e-mail, but e-mail surveillance is common. If e-mail is not encrypted, it could be read easily by a network operator or government.

15.2.38 embedded script

An embedded script is a piece of software code.

15.2.39 encryption

Encryption is any method for recoding and scrambling data or transforming it mathematically to make it unreadable to a third party who doesn't know the secret key to decrypt it. It is possible to encrypt data on your local hard drive using software like TrueCrypt (<http://www.truecrypt.org>) or to encrypt Internet traffic with TLS/SSL or SSH.

See also decryption.

15.2.40 exit node

An exit node is a Tor node that forwards data outside the Tor network.

See also middleman node.

15.2.41 file sharing

File sharing refers to any computer system where multiple people can use the same information, but often refers to making music, films or other materials available to others free of charge over the Internet.

15.2.42 file spreading engine

A file spreading engine is a Web site a publisher can use to get around censorship. A user only has to upload a file to publish once and the file spreading engine uploads that file to some set of sharehosting services (like Rapidshare or Megaupload).

15.2.43 filter

To filter is to search in various ways for specific data patterns to block or permit communications.

15.2.44 Firefox

Firefox is the most popular free and open source Web browser, developed by the Mozilla Foundation.

15.2.45 forum

On a Web site, a forum is a place for discussion, where users can post messages and comment on previously posted messages. It is distinguished from a mailing list or a Usenet newsgroup by the persistence of the pages containing the message threads. Newsgroup and mailing list archives, in contrast, typically display messages one per page, with navigation pages listing only the headers of the messages in a thread.

15.2.46 frame

A frame is a portion of a Web page with its own separate URL. For example, frames are frequently used to place a static menu next to a scrolling text window.

15.2.47 FTP (File Transfer Protocol)

The FTP protocol is used for file transfers. Many people use it mostly for downloads; it can also be used to upload Web pages and scripts to some Web servers. It normally uses ports 20 and 21, which are sometimes blocked. Some FTP servers listen to an uncommon port, which can evade port-based blocking.

A popular free and open source FTP client for Windows and Mac OS is FileZilla. There are also some Web-based FTP clients that you can use with a normal Web browser like Firefox.

15.2.48 full disk encryption

see disk encryption.

15.2.49 gateway

A gateway is a node connecting two networks on the Internet. An important example is a national gateway that requires all incoming or outgoing traffic to go through it.

15.2.50 GNU Privacy Guard

GNU Privacy Guard (GnuPG or GPG) is a GPL Licensed alternative to the PGP suite of cryptographic software. GnuPG is compliant with RFC 4880, which is the current IETF standards track specification of OpenPGP.

see also Pretty Good Privacy (PGP).

15.2.51 GPG

see GNU Privacy Guard.

15.2.52 honeypot

A honeypot is a site that pretends to offer a service in order to entice potential users to use it, and to capture information about them or their activities.

15.2.53 hop

A hop is a link in a chain of packet transfers from one computer to another, or any computer along the route. The number of hops between computers can give a rough measure of the delay (latency) in communications between them. Each individual hop is also an entity that has the ability to eavesdrop on, block, or tamper with communications.

15.2.54 HTTP (Hypertext Transfer Protocol)

HTTP is the fundamental protocol of the World Wide Web, providing methods for requesting and serving Web pages, querying and generating answers to queries, and accessing a wide range of services.

15.2.55 HTTPS (Secure HTTP)

Secure HTTP is a protocol for secure communication using encrypted HTTP messages. Messages between client and server are encrypted in both directions, using keys generated when the connection is requested and exchanged securely. Source and destination IP addresses are in the headers of every packet, so HTTPS cannot hide the fact of the communication, just the contents of the data transmitted and received.

15.2.56 IANA (Internet Assigned Numbers Authority)

IANA is the organization responsible for technical work in managing the infrastructure of the Internet, including assigning blocks of IP addresses for top-level domains and licensing domain registrars for ccTLDs and for the generic TLDs, running the root name servers of the Internet, and other duties.

15.2.57 ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN is a corporation created by the US Department of Commerce to manage the highest levels of the Internet. Its technical work is performed by IANA.

15.2.58 Instant Messaging (IM)

Instant messaging is either certain proprietary forms of chat using proprietary protocols, or chat in general. Common instant messaging clients include MSN Messenger, ICQ, AIM or Yahoo! Messenger.

15.2.59 Intermediary

See man in the middle.

15.2.60 Internet

The Internet is a network of networks interconnected using TCP/IP and other communication protocols.

15.2.61 IP (Internet Protocol) Address

An IP address is a number identifying a particular computer on the Internet. In the previous version 4 of the Internet Protocol an IP address consisted of four bytes (32 bits), often represented as four integers in the range 0-255 separated by dots, such as

74.54.30.85. In IPv6, which the Net is currently switching to, an IP address is four times longer, and consists of 16 bytes (128 bits). It can be written as 8 groups of 4 hex digits separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

15.2.62 IRC (Internet relay chat)

IRC is a more than 20-year-old Internet protocol used for real-time text conversations (chat or instant messaging). There exist several IRC networks – the largest have more than 50 000 users.

15.2.63 ISP (Internet Service Provider)

An ISP (Internet service provider) is a business or organization that provides access to the Internet for its customers.

15.2.64 JavaScript

JavaScript is a scripting language, commonly used in Web pages to provide interactive functions.

15.2.65 KeePass, KeePassX

KeePass and KeePassX are types of Password Manager.

15.2.66 keychain software

see Password Manager.

15.2.67 keyword filter

A keyword filter scans all Internet traffic going through a server for forbidden words or terms to block.

15.2.68 latency

Latency is a measure of time delay experienced in a system, here in a computer network. It is measured by the time between the start of packet transmission to the start of packet reception, between one network end (e.g. you) to the other end (e.g. the Web server). One very powerful way of Web filtering is maintaining a very high latency, which makes lots of circumvention tools very difficult to use.

15.2.69 log file

A log file is a file that records a sequence of messages from a software process, which can be an application or a component of the operating system. For example, Web servers or proxies may keep log files containing records about which IP addresses used these services when and what pages were accessed.

15.2.70 low-bandwidth filter

A low-bandwidth filter is a Web service that removes extraneous elements such as advertising and images from a Web page and otherwise compresses it, making page download much quicker.

15.2.71 malware

Malware is a general term for malicious software, including viruses, that may be installed or executed without your knowledge. Malware may take control of your computer for purposes such as sending spam. (Malware is also sometimes called badware.)

15.2.72 man in the middle

A man in the middle or man-in-the-middle is a person or computer capturing traffic on a communication channel, especially to selectively change or block content in a way that undermines cryptographic security. Generally the man-in-the-middle attack involves impersonating a Web site, service, or individual in order to record or alter communications. Governments can run man-in-the-middle attacks at country gateways where all traffic entering or leaving the country must pass.

15.2.73 middleman node

A middleman node is a Tor node that is not an exit node. Running a middleman node can be safer than running an exit node because a middleman node will not show up in third parties' log files. (A middleman node is sometimes called a non-exit node.)

15.2.74 monitor

To monitor is to check a data stream continuously for unwanted activity.

15.2.75 network address translation (NAT)

NAT is a router function for hiding an address space by remapping. All traffic going out from the router then uses the router's IP address, and the router knows how to route incoming traffic to the requestor. NAT is frequently implemented by firewalls. Because incoming connections are normally forbidden by NAT, NAT makes it difficult to offer a service to the general public, such as a Web site or public proxy. On a network where NAT is in use, offering such a service requires some kind of firewall configuration or NAT traversal method.

15.2.76 network operator

A network operator is a person or organization who runs or controls a network and thus is in a position to monitor, block, or alter communications passing through that network.

15.2.77 node

A node is an active device on a network. A router is an example of a node. In the Psiphon and Tor networks, a server is referred to as a node.

15.2.78 non-exit node

See middleman node.

15.2.79 obfuscation

Obfuscation means obscuring text using easily-understood and easily-reversed transformation techniques that will withstand casual inspection but not cryptanalysis, or making minor changes in text strings to prevent simple matches. Web proxies often use obfuscation to hide certain names and addresses from simple text filters that might be fooled by the obfuscation. As another example, any domain name can optionally contain a final dot, as in “somewhere.com.”, but some filters might search only for “somewhere.com” (without the final dot).

15.2.80 open node

An open node is a specific Psiphon node which can be used without logging in. It automatically loads a particular homepage, and presents itself in a particular language, but can then be used to browse elsewhere.

See also Psiphon node.

15.2.81 OTR/Off-the-Record messaging

Off-the-Record Messaging, commonly referred to as OTR, is a cryptographic protocol that provides strong encryption for instant messaging conversations.

15.2.82 packet

A packet is a data structure defined by a communication protocol to contain specific information in specific forms, together with arbitrary data to be communicated from one point to another. Messages are broken into pieces that will fit in a packet for transmission, and reassembled at the other end of the link.

15.2.83 password manager

A password manager is software that helps a user organize passwords and PIN codes. The software typically has a local database or a file that holds the encrypted password data for secure logon onto computers, networks, web sites and application data files. KeePass <http://keepass.info/> is an example of a password manager.

15.2.84 pastebin

A web service where any kind of text can be dumped and read without registration. All text will be visible publicly.

15.2.85 peer-to-peer

A peer-to-peer (or P2P) network is a computer network between equal peers. Unlike client-server networks there is no central server and so the traffic is distributed only among the clients. This technology is mostly applied to file sharing programs like BitTorrent, eMule and Gnutella. But also the very old Usenet technology or the VoIP program Skype can be categorized as peer-to-peer systems.

See also file sharing.

15.2.86 perfect forward secrecy

In an authenticated key-agreement protocol that uses public key cryptography, perfect forward secrecy (or PFS) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.

15.2.87 Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications.

PGP and similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

15.2.88 PHP

PHP is a scripting language designed to create dynamic Web sites and web applications. It is installed on a Web server. For example, the popular Web proxy PHPProxy uses this technology.

15.2.89 plain text

Plain text is unformatted text consisting of a sequence of character codes, as in ASCII plain text or Unicode plain text.

15.2.90 plaintext

Plaintext is unencrypted text, or decrypted text.

See also encryption, TLS/SSL, SSH.

15.2.91 privacy

Protection of personal privacy means preventing disclosure of personal information without the permission of the person concerned. In the context of circumvention, it means preventing observers from finding out that a person has sought or received information that has been blocked or is illegal in the country where that person is at the time.

15.2.92 private key

see public key encryption/public-key cryptography.

15.2.93 POP3

Post Office Protocol version 3 is used to receive mail from a server, by default on port 110 with an e-mail program such as Outlook Express or Thunderbird.

15.2.94 port

A hardware port on a computer is a physical connector for a specific purpose, using a particular hardware protocol. Examples are a VGA display port or a USB connector.

Software ports also connect computers and other devices over networks using various protocols, but they exist in software only as numbers. Ports are somewhat like numbered doors into different rooms, each for a special service on a server or PC. They are identified by numbers from 0 to 65535.

15.2.95 protocol

A formal definition of a method of communication, and the form of data to be transmitted to accomplish it. Also, the purpose of such a method of communication. For example, Internet Protocol (IP) for transmitting data packets on the Internet, or Hypertext Transfer Protocol for interactions on the World Wide Web.

15.2.96 proxy server

A proxy server is a server, a computer system or an application program which acts as a gateway between a client and a Web server. A client connects to the proxy server to request a Web page from a different server. Then the proxy server accesses the resource by connecting to the specified server, and returns the information to the requesting site. Proxy servers can serve many different purposes, including restricting Web access or helping users route around obstacles.

15.2.97 Psiphon node

A Psiphon node is a secured web proxy designed to evade Internet censorship. It is developed by Psiphon inc. Psiphon nodes can be open or private.

15.2.98 private node

A private node is a Psiphon node working with authentication, which means that you have to register before you can use it. Once registered, you will be able to send invitations to your friends and relatives to use this specific node.

See also Psiphon node.

15.2.99 public key

see public key encryption/public-key cryptography.

15.2.100 public key encryption/public-key cryptography

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions. One of these keys is published or public, while the other is kept private.

Public-key cryptography uses asymmetric key algorithms (such as RSA), and can also be referred to by the more generic term “asymmetric key cryptography.”

15.2.101 publicly routable IP address

Publicly routable IP addresses (sometimes called public IP addresses) are those reachable in the normal way on the Internet, through a chain of routers. Some IP addresses are private, such as the 192.168.x.x block, and many are unassigned.

15.2.102 regular expression

A regular expression (also called a regexp or RE) is a text pattern that specifies a set of text strings in a particular regular expression implementation such as the UNIX grep utility. A text string “matches” a regular expression if the string conforms to the pattern, as defined by the regular expression syntax. In each RE syntax, some characters have special meanings, to allow one pattern to match multiple other strings. For example, the regular expression `lo+se` matches `lose`, `loose`, and `looose`.

15.2.103 remailer

An anonymous remailer is a service which allows users to send e-mails anonymously. The remailer receives messages via e-mail and forwards them to their intended recipient after removing information that would identify the original sender. Some also provide an anonymous return address that can be used to reply to the original sender without disclosing her identity. Well-known Remailer services include Cypherpunk, Mixmaster and Nym.

15.2.104 router

A router is a computer that determines the route for forwarding packets. It uses address information in the packet header and cached information on the server to match address numbers with hardware connections.

15.2.105 root name server

A root name server or root server is any of thirteen server clusters run by IANA to direct traffic to all of the TLDs, as the core of the DNS system.

15.2.106 RSS (Real Simple Syndication)

RSS is a method and protocol for allowing Internet users to subscribe to content from a Web page, and receive updates as soon as they are posted.

15.2.107 scheme

On the Web, a scheme is a mapping from a name to a protocol. Thus the HTTP scheme maps URLs that begin with HTTP: to the Hypertext Transfer Protocol. The protocol determines the interpretation of the rest of the URL, so that `http://www.example.com/dir/content.html` identifies a Web site and a specific file in a specific directory, and `mailto:user@somewhere.com` is an e-mail address of a specific person or group at a specific domain.

15.2.108 shell

A UNIX shell is the traditional command line user interface for the UNIX/Linux operating systems. The most common shells are sh and bash.

15.2.109 SOCKS

A SOCKS proxy is a special kind of proxy server. In the ISO/OSI model it operates between the application layer and the transport layer. The standard port for SOCKS proxies is 1080, but they can also run on different ports. Many programs support a connection through a SOCKS proxy. If not you can install a SOCKS client like FreeCap, ProxyCap or SocksCap which can force programs to run through the Socks proxy using dynamic port forwarding. It is also possible to use SSH tools such as OpenSSH as a SOCKS proxy server.

15.2.110 screenlogger

A screenlogger is software able to record everything your computer displays on the screen. The main feature of a screenlogger is to capture the screen and log it into files to view at any time in the future. Screen loggers can be used as powerful monitoring tool. You should be aware of any screen logger running on any computer you are using, anytime.

15.2.111 script

A script is a program, usually written in an interpreted, non-compiled language such as JavaScript, Java, or a command interpreter language such as bash. Many Web pages include scripts to manage user interaction with a Web page, so that the server does not have to send a new page for each change.

15.2.112 smartphone

A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary feature phone, such as Web access, ability to run elaborated operating systems and run built-in applications.

15.2.113 spam

Spam is messages that overwhelm a communications channel used by people, most notably commercial advertising sent to large numbers of individuals or discussion groups. Most spam advertises products or services that are illegal in one or more ways, almost always including fraud. Content filtering of e-mail to block spam, with the permission of the recipient, is almost universally approved of.

15.2.114 SSH (Secure Shell)

SSH or Secure Shell is a network protocol that allows encrypted communication between computers. It was invented as a successor of the unencrypted Telnet protocol and is also used to access a shell on a remote server.

The standard SSH port is 22. It can be used to bypass Internet censorship with port forwarding or it can be used to tunnel other programs like VNC.

15.2.115 SSL (Secure Sockets Layer)

SSL (or Secure Sockets Layer), is one of several cryptographic standards used to make Internet transactions secure. It is was used as the basis for the creation of the related Transport Layer Security (TLS). You can easily see if you are using SSL by looking at the URL in your Browser (like Firefox or Internet Explorer): If it starts with https instead of http, your connection is encrypted.

15.2.116 steganography

Steganography, from the Greek for hidden writing, refers to a variety of methods of sending hidden messages where not only the content of the message is hidden but the very fact that something covert is being sent is also concealed. Usually this is done by concealing something within something else, like a picture or a text about something innocent or completely unrelated. Unlike cryptography, where it is clear that a secret message is being transmitted, steganography does not attract attention to the fact that someone is trying to conceal or encrypt a message.

15.2.117 subdomain

A subdomain is part of a larger domain. If for example “wikipedia.org” is the domain for the Wikipedia, “en.wikipedia.org” is the subdomain for the English version of the Wikipedia.

15.2.118 threat analysis

A security threat analysis is properly a detailed, formal study of all known ways of attacking the security of servers or protocols, or of methods for using them for a particular purpose such as circumvention. Threats can be technical, such as code-breaking or exploiting software bugs, or social, such as stealing passwords or bribing someone who has special knowledge. Few companies or individuals have the knowledge and skill to do a comprehensive threat analysis, but everybody involved in circumvention has to make some estimate of the issues.

15.2.119 Top-Level Domain (TLD)

In Internet names, the TLD is the last component of the domain name. There are several generic TLDs, most notably .com, .org, .edu, .net, .gov, .mil, .int, and one two-letter country code (ccTLD) for each country in the system, such as .ca for Canada. The European Union also has the two-letter code .eu.

15.2.120 TLS (Transport Layer Security)

TLS or Transport Layer Security is a cryptographic standard based on SSL, used to make Internet transactions secure.

15.2.121 TCP/IP (Transmission Control Protocol over Internet Protocol)

TCP and IP are the fundamental protocols of the Internet, handling packet transmission and routing. There are a few alternative protocols that are used at this level of Internet structure, such as UDP.

15.2.122 Tor bridge

A bridge is a middleman Tor node that is not listed in the main public Tor directory, and so is possibly useful in countries where the public relays are blocked. Unlike the case of exit nodes, IP addresses of bridge nodes never appear in server log files and never pass through monitoring nodes in a way that can be connected with circumvention.

15.2.123 traffic analysis

Traffic analysis is statistical analysis of encrypted communications. In some circumstances traffic analysis can reveal information about the people communicating and the information being communicated.

15.2.124 tunnel

A tunnel is an alternate route from one computer to another, usually including a protocol that specifies encryption of messages.

15.2.125 UDP (User Datagram Packet)

UDP is an alternate protocol used with IP. Most Internet services can be accessed using either TCP or UDP, but there are some that are defined to use only one of these alternatives. UDP is especially useful for real-time multimedia applications like Internet phone calls (VoIP).

15.2.126 URL (Uniform Resource Locator)

The URL (Uniform Resource Locator) is the address of a Web site. For example, the URL for the World News section of the NY Times is <http://www.nytimes.com/pages/world/index.html>. Many censoring systems can block a single URL. Sometimes an easy way to bypass the block is to obscure the URL. It is for example possible to add a dot after the site name, so the URL <http://en.cship.org/wiki/URL> becomes <http://en.cship.org./wiki/URL>. If you are lucky with this little trick you can access blocked Web sites.

15.2.127 Usenet

Usenet is a more than 20-year-old discussion forum system accessed using the NNTP protocol. The messages are not stored on one server but on many servers which distribute their content constantly. Because of that it is impossible to censor Usenet as a whole, however access to Usenet can and is often blocked, and any particular server is likely to carry only a subset of locally-acceptable Usenet newsgroups. Google archives the entire available history of Usenet messages for searching.

15.2.128 VoIP (Voice over Internet Protocol)

VoIP refers to any of several protocols for real-time two-way voice communication on the Internet, which is usually much less expensive than calling over telephone company voice networks. It is not subject to the kinds of wiretapping practiced on telephone networks, but can be monitored using digital technology. Many companies produce software and equipment to eavesdrop on VoIP calls; securely encrypted VoIP technologies have only recently begun to emerge.

15.2.129 VPN (virtual private network)

A VPN (virtual private network) is a private communication network used by many companies and organizations to connect securely over a public network. Usually on the Internet it is encrypted and so nobody except the endpoints of the communication can look at the data traffic. There are various standards like IPSec, SSL, TLS. The use of a

VPN provider is a very fast, secure and convenient method to bypass Internet censorship with little risks but it generally costs money every month. Further, note that the VPN standard PPTP is no longer considered secure, and should be avoided.

15.2.130 whitelist

A whitelist is a list of sites specifically authorized for a particular form of communication. Filtering traffic can be done either by a whitelist (block everything but the sites on the list), a blacklist (allow everything but the sites on the list), a combination of the two, or by other policies based on specific rules and conditions.

15.2.131 World Wide Web (WWW)

The World Wide Web is the network of hyperlinked domains and content pages accessible using the Hypertext Transfer Protocol and its numerous extensions. The World Wide Web is the most famous part of the Internet.

15.2.132 Webmail

Webmail is e-mail service through a Web site. The service sends and receives mail messages for users in the usual way, but provides a Web interface for reading and managing messages, as an alternative to running a mail client such as Outlook Express or Thunderbird on the user's computer. For example a popular and free webmail service is <https://mail.google.com/>

15.2.133 Web proxy

A Web proxy is a script running on a Web server which acts as a proxy/gateway. Users can access such a Web proxy with their normal Web browser (like Firefox) and enter any URL in the form located on that Web site. Then the Web proxy program on the server receives that Web content and displays it to the user. This way the ISP only sees a connection to the server with the Web proxy since there is no direct connection.

15.2.134 WHOIS

WHOIS (who is) is the aptly named Internet function that allows one to query remote WHOIS databases for domain registration information. By performing a simple WHOIS search you can discover when and by whom a domain was registered, contact information, and more.

A WHOIS search can also reveal the name or network mapped to a numerical IP address

15.3 The necessity of Open Source

The last 20 years have seen network technology reaching ever more deeply into our lives, informing how we communicate and act within the world. With this come inherent risks: the less we understand the network environment we depend upon, the more vulnerable we are to exploitation.

This ignorance is something traditionally enjoyed by criminals. In recent years however some corporations and governments have exploited civilian ignorance in a quest for increased control. This flagrant and often covert denial of dignity breaches many basic rights, the right to privacy, in particular.

Closed source software has been a great boon to such exploitation – primarily due to the fact there is no code available for open, decentralised security auditing by the community. Under the auspices of hiding trade secrets, closed-source software developers have proven to be unwilling to explain to users how their programs work. This might not always be an issue were it not for the high stakes: identity theft, the distribution of deeply personal opinion and sentiment, a persons diverse interests and even his/her home increasingly come into close contact with software in a world-wide network context. As such, many people find themselves using software for personal purposes with full trust that it are secure. The Windows operating system itself is the most obvious real-world example. Apple's OS X follows close behind, with large portions of the operating system's inner-workings barred from public inspection.

In Cryptography there is a strong principle, established in the 19th century by *Auguste Kerckhoff* (and hence named after him) which demands that

“[the encryption method] must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience”.

While this principle has been taken further by most scientific and (of course) open source communities – publishing their methods and inner-workings upfront, so potential weaknesses can be pointed out and fixed before further distribution – most distributors of proprietary software rely on obfuscation to hide the weaknesses of their software. As such they often prove to address newly discovered vulnerabilities in a non-transparent way – leaving many trusting users at risk of exploitation.

Of course it must be said that Open Source Software is as secure as you make it (and there is a lot of OSS written by beginners). However there are many good examples of well written, well managed software which have such a large (and concerned) user base that even the tiniest of mistakes are quickly found and dealt with. This is especially the case with software depended upon in a network context.

To use closed source software in a network context is not only to be a minority, it is to be overlooked by a vast community of concerned researchers and specialists that have your privacy and safety in mind.

N.B. There is also a more cynical view of Open Source Software, which points out that since nobody is paid full time to constantly review and regression test the latest tinkering by unskilled or deliberately malicious programmers, it can also suffer from major security

15 Appendices

weaknesses which go undetected for long periods of time in complicated software, leaving it vulnerable to hackers, criminals and intelligence agencies etc. e.g. the (now fixed) Debian Linux predictable random number generator problem which led to the creation of lots of weak cryptographic keys.