CRYPTOME

The FBI Can Bypass Encryption

Cyber Security Is a Magic Act

By **Bill Blunden**, October 31, 2014

Encryption has gained the attention of actors on both sides of the mass surveillance debate. For example in a speech at the Brookings Institution FBI Director James Comey complained that strong encryption was causing U.S. security services to "go dark." Comey described encrypted data as follows:

> *"It's the equivalent of a closet that can't be opened, a safe deposit box that can't be opened, a safe that can't ever be cracked."*

Got that? Comey essentially says that encryption is a sure bet. Likewise during an interview with James Bamford whistleblower Ed Snowden confidently announced that:

> *"We have the means and we have the technology to end mass surveillance without any legislative action at all, without any policy changes... By basically adopting changes like making encryption a universal standard—where all communications are encrypted by default—we can end mass surveillance not just in the United States but around the world."*

If you glanced over the above excerpts and took them at face value you'd probably come away thinking that all you needed to protect your civil liberties is the latest encryption widget. Right? Wow, let me get my check book out! Paging Mr. Omidyar…

Not so fast bucko. There's an important caveat, some fine print that Ed himself spelled out when he initially contacted film director Laura Poitras. In particular Snowden qualified that:

> *"If the device you store the private key and enter your passphrase on has been hacked, it is trivial to decrypt our communications."*

This corollary underscores the reality that, despite the high profile sales pitch that's being repeated endlessly, strong encryption alone isn't enough. Hi-tech subversion is a trump card as the Heartbleed bug graphically illustrated. In light of the NSA's mass subversion programs it would be naïve to think that there aren't other critical bugs like Heartbleed, subtle *intentional* flaws, out in the wild being leveraged by spies.

The FBI's Tell

James Comey's performance at Brookings was an impressive public relations stunt. Yet recent history is chock full of instances where the FBI employed malware like Magic Lantern and CIPAV to foil encryption and identify people using encryption-based anonymity software like Tor. If it's expedient the FBI will go so far as to impersonate a media outlet to fool suspects into infecting their own machines. It would seem that crooks aren't the only attackers who wield social engineering techniques.

In fact the FBI has gotten so adept at hacking computers, utilizing what are referred to internally as *Network Investigative Techniques*, that the FBI wants to change the law to reflect this. The *Guardian* reports on how the FBI is asking the U.S. Advisory Committee on Rules and Criminal Procedure to move the legal goal posts, so to speak:

> *"The amendment [proposed by the FBI] inserts a clause that would allow a judge to issue warrants to gain 'remote access' to computers 'located within or outside that district' (emphasis added) in cases in which the 'district where the media or information is located has been concealed through technological means'. The expanded powers to stray across district boundaries would apply to any criminal investigation, not just to terrorist cases as at present."*

In other words the FBI wants to be able to hack into a computer when its exact location is shrouded by anonymity software. Once they compromise the targeted machine it's pretty straightforward to install a software implant (i.e. malware) and exfiltrate whatever user data they want, including encryption passwords.

If encryption is really the impediment that director Comey makes it out to be then why is the FBI so keen to amend the rules in a manner which implies that they can sidestep it? In the parlance of poker this is a "tell."

Denouement

As a developer who has built malicious software designed to undermine security tools I can attest that there is a whole burgeoning industry which prays on naïve illusions of security. Companies like Hacking Team have found a lucrative niche offering products to the highest bidder that compromise security and… a drumroll please… defeat encryption.

There's a moral to this story. Cryptome's own curmudgeon, John Young, prudently observes:

> *"Protections of promises of encryption, proxy use, Tor-like anonymity and 'military-grade' comsec technology are magic acts -- ELINT, SIGINT and COMINT always prevail over comsec. The most widely trusted and promoted systems are the most likely to be penetrated, exploited, spied upon, successfully attacked, covertly compromised with faults hidden by promoters, operators, competitors, compromisers and attackers all of whom warn against the others while mutually benefiting from continuous alarms about security and privacy."*

When someone promises you turnkey anonymity and failsafe protection from spies, make like that guy on *The Walking Dead* and reach for your crossbow. Mass surveillance is a vivid expression of raw power and control. Hence what ails society is fundamentally a political problem, with economic and technical facets, such that safeguarding civil liberties on the Internet will take a lot more than just the right app.

Bill Blunden is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.