Published on *Alternet* (http://www.alternet.org)

Home > When Strong Encryption Isn't Enough to Protect Our Privacy

When Strong Encryption Isn't Enough to Protect Our Privacy

By Bill Blunden [1] / AlterNet [2]
February 26, 2015

“None of the claims of what comsec works is to be taken saltless: Tor, OTR, ZTRP are lures.” —*Cryptome* [3], Dec. 30, 2014

In the aftermath of Edward Snowden's disclosures, the American public has been deluged with talking points that advocate strong encryption as a universal solution for protecting our privacy. Unfortunately the perception of strong encryption as a panacea is flawed. In this report I’ll explain why strong encryption isn’t enough and then present some operational guidelines which can be used to enhance your online privacy. Nothing worthwhile is easy. Especially sidestepping the Internet’s global Eye of Providence.

Anyone who reads through privacy recommendations published by the Intercept [4] or the Freedom of the Press Foundation [5] will encounter the same basic lecture. In a nutshell they advise users to rely on open source encryption software, run it from a CD-bootable copy of the TAILS operating system, and route their Internet traffic through the TOR anonymity network.

This canned formula now has a degree of official support from, of all places, the White House. A few days ago during an interview with Re/Code, President Obama assured [6] listeners that “there’s no scenario in which we don’t want really strong encryption.” It’s interesting to note how this is in stark contrast to public admonishments [7] by FBI director James Comey this past October for key escrow encryption, which is anything but strong.

So it would appear that POTUS is now toeing a line advocated by none other than whistler-blower Snowden who asserted [8] that “properly implemented strong crypto systems are one of the few things that you can rely on.”

Only there’s a problem with this narrative and its promise of salvation: When your threat profile entails a funded outfit like the NSA, cyber security is largely a placebo.

Down To the Metal

A report [9] released by Moscow-based anti-virus vendor Kaspersky Lab proves that, despite the self-congratulatory public relations messaging of Google or Apple, strong encryption might not be the trendy cure-all it's cracked up to be. The NSA has poured vast resources into hacking hardware platforms across the board, creating firmware modifications [10] that allow [11] U.S. spies to "capture a machine's encryption password, store it in 'an invisible area inside the computer's hard drive' and unscramble a machine's contents."

On a side note, Kaspersky Lab is one of two companies authorized [12] by Russian security service to provide anti-virus technology to the Russian government. The company's founder, Eugene Kaspersky, a former [13] Soviet intelligence officer himself, has links to the Russian Federal Security Service, or FSB. So it makes sense that the one company with the audacity and skill to publicly showcase a global espionage program by the NSA would also be a company aligned with a countervailing power center outside of the United States.

Anyway, when it comes to bare-metal skullduggery there are plenty [14] of proof-of-concept [15] examples available in the public domain. But these experiments are nothing compared to the slick production-level malware deployed by NSA spies. When the Pentagon aims for information dominance [16] it doesn't screw around. Hence blind trust in encryption software is exposed as a sort of magical thinking.

Some people would argue that the NSA's hardware hacks aren't a big deal because they're used selectively for targeted intrusions. One problem with this stance is that spy gear has a habit of filtering down into the underworld because spies and crooks are kindred spirits who often work together. Another problem is that the NSA is actively working to industrialize [17] attacks so that they can be pulled off on a mass scale against large swathes [18] of users. The recent discovery of pre-installed malware [19] on Lenovo PCs should offer an unsettling hint [20] of where spies and their front companies are taking things.

Face it, an intelligence agency that makes off [21] with the encryption keys from a large multinational company that manufactures billions of SIM cards each year is an agency that's doing much more than just small-scale targeted hardware attacks. They want to "collect it all."

OPSEC Is Law

> "Iraqi Assault to Retake Mosul from Islamic State Is Planned for Spring" —
> *New York Times*headline, Feb. 20, 2015

Given the sorry state of software engineering and the sheer scope of clandestine subversion programs, if spies want to root your machine they'll probably find a way. The Internet is akin to a vast swamp in the Deep South. Users wade through a hostile murky environment surrounded by alligators prowling silently just below the surface.

And don't think that tools like Tor [22] will protect you. The FBI has demonstrated repeatedly that it can unmask [23] Tor users with exploits. The FBI's collection of cyber scalps includes [24] a high-ranking cyber security director who probably thought his game was tight. The litany of Tor's failures have led security researchers to conclude [25] that, "Tor makes you stick out as much as a transgender Mongolian in the desert."

Hence when going toe-to-toe with spies from the NSA's Office of Tailored Access Operations [26] or, heaven forbid, its more daunting CIA brethren [27] in the Special Collection Service [28], *operational security* (OPSEC) becomes essential. This isn't cynical "privacy nihilism" but rather clear-headed contingency planning. Once the NSA owns a computer the only things that stands between the user and spies is OPSEC. It takes groundwork, patience and (most of all) discipline. Even the professionals get this wrong. And when they do the results can be disastrous.

For a graphic illustration of this contemplate the case of Ross Ulbricht, the creator of Silk Road. The celebrated Tor anonymity network did very little [29] to stop the feds from getting a bead on him. To make matters worse you'd think Ulbricht would know better [30] to work with his back to the room so the feds could sneak up on him before he could log off, leaving his encrypted laptop in a decidedly vulnerable state.

It didn't help that the Silk Road's servers were configured to auto-login certain client machines and that Ulbricht's laptop just happened to be connected to the Silk Road servers as a full administrator. Ditto that for Bitcoin wallets on the aforementioned laptop which allowed law enforcement agents to trace [31] over $13 million in Bitcoins to Ulbricht.

When professionals get operational security right they sometimes look a bit silly. Close circuit TVs are cheap and ubiquitous. Let's just say that Snowden wasn't being paranoid when he covered himself with a red blanket (the so-called [32] "magic mantle of power") while entering his laptop password. For the sake of maintaining cover, simply obscuring your keyboard may be a wiser option in public as it's less conspicuous. The last thing you want to do in a crowd is draw attention to yourself.

Anti-Forensics in Theory and Practice

> "The only protection against communication systems is to avoid their use." —*Cryptome* [33], Communications Privacy Folly, June 13, 2012

A researcher like the Grugq [34] will inform listeners, when he's not out scoring [35] zero-day exploits, that anti-forensics [36] is all about reducing both the *quantity* and *quality* of information that adversaries acquire. In other words, if spies succeed in breaching your computer then give them as little useful information as possible. One way to achieve this is through *compartmentalization*, a technique honed to a fine edge by intelligence outfits like the KGB.

In the years following World War II the Soviet nuclear program was targeted heavily by U.S. spies. To counter this effort, the Soviets employed sophisticated, multi-level, denial and deception strategies. According to Mikhail Gladyshev [37], who was in charge of the plutonium enrichment station at the Mayak complex in the city of Ozersk, compartmentalization of information was pervasive:

> "[W]e put the [plutonium] paste in a box and transferred it to the consumer plant. How much plutonium was in that box we didn't know and it was not recommended for us to know. Even later, when I was the plant's chief engineer, the plans for plutonium production were known only to the facility's director, and all documents were prepared in single copies"

Given the reality of mass interception let's look at mobile phones as a case study. They're essentially portable Telescreens [21], glorified tracking [38] beacons that double as walkie-talkies. In private, when NSA spies feel comfortable enough to speak candidly with each other, iPhone users are referred to [39] as zombies who literally pay for their own surveillance. This is not an exaggeration and it speaks yards about how intelligence officers view society. You've been warned.

The best option is to follow the example of WikiLeaks activist Sarah Harrison [40] and simply not carry a cellphone. Jihadists in the Middle East have learned this lesson the hard way and use hand couriers [41] for sensitive messages. Other organization like Los Zetas in Mexico have built private radio networks [42] to avoid official communication channels. Lebanon's Hezbollah went so far as to set up its own covert fiber optic [43] data network in an effort to elude conventional eavesdropping.

Listen to John Young of the web site Cryptome. The only sure-fire way to protect yourself against monitoring on a given communication system is not to use it.

If having a cellphone is an absolute necessity there are shielding cases [44] available. Though removing the battery works just fine in a pinch as does sticking a cellphone in a sealed metal container like a refrigerator. Another thing to remember is that "dumb phones" lacking in bells and whistles tend to accumulate far less information [45] than more elaborate smartphones.

Compromised mobile devices should be smashed and dumped in a remote location. Make sure the SIM card is completely destroyed. Recall how methodically the GCHQ officials disposed [46] of hardware belonging to the Guardian newspaper. This is another area where $10 dumb phones have an advantage.

Once a cell phone is out in the open with its battery in place, consider the following recommendations. First, it's extremely unwise for someone to power on a "secure" cell phone where they normally live and work. This includes recharging the phone! While traveling to a remote site to communicate be aware that automated license plate readers, traffic cameras, facial recognition software and built-in vehicle GPS units are becoming more commonplace.

Avoid patterns (geographic, chronological, etc.). Arbitrarily relocate to new spots during the course of a phone call. Stay in motion. Phone calls should be as short as possible so that the amount of data collected by surveillance equipment [47] during the call's duration is minimized. This will make it more difficult for spies to make accurate predictions.

Another aim should be to maintain a closed communication network at all costs. Secure cell phones should not be used casually to call friends or relatives. Dial only other cell phones intended specifically for sensitive communication. Also remember that calling a landline may end up exposing the person who answers.

Carrying additional mobile devices (e.g. surface tablet, second cell phone) creates the risk that the peripheral hardware may undermine anonymity through correlation. Finally, pay for items using cash when operational. Credit card transactions are like a big red flag.

If spies somehow captures a secure cell phone and are able to siphon data off of it, one potential countermeasure is to flood the device with false information. Skillful application of this technique can lead spies on a goose chase. When Edward Snowden was fleeing Hong Kong he intentionally bought a plane ticket to India with his own credit card in an effort to throw pursuers off his track.

Final Words

Ultimately there's no ironclad formula for protecting your identity. No guarantees. Privacy isn't something I can give you, it's something you must attain on your own through hard work. In summary, expect security tools to fail, compartmentalize to contain damage and apply the Grugq's core tenets of anti-forensics. Don't put blind faith in technology. Focus your resources on maintaining rigorous procedures. When things get dicey it'll be your training and preparation that keep you secure.

Bill Blunden is the author of several books, including "The Rootkit Arsenal" and "Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex." He is the lead investigator at Below Gotham Labs.

Share on Facebook Share
Share on Twitter Tweet
Report typos and corrections to 'corrections@alternet.org'. [48]
[49]

Source URL: http://www.alternet.org/news-amp-politics/when-strong-encryption-isnt-enough-protect-our-privacy

Links:
[1] http://www.alternet.org/authors/bill-blunden
[2] http://alternet.org

[3] https://twitter.com/Cryptomeorg/status/550010942072049666
[4] https://firstlook.org/theintercept/2014/10/28/smuggling-snowden-secrets/
[5] https://freedom.press/encryption-works
[6] https://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/
[7] http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
[8] http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
[9] https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf
[10] http://arstechnica.com/information-technology/2015/02/how-hackers-could-attack-hard-drives-to-create-a-pervasive-backdoor/
[11] http://www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html
[12] http://www.wired.com/2012/07/kaspersky-indy/
[13] http://www.wired.com/2012/07/ff_kaspersky/
[14] http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/
[15] https://www.blackhat.com/presentations/bh-usa-09/TERESHKIN/BHUSA09-Tereshkin-Ring3Rootkit-SLIDES.pdf
[16] http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html
[17] http://www.wired.com/2013/05/pentagon-cyberwar-angry-birds/all/
[18] https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/
[19] http://bits.blogs.nytimes.com/2015/02/22/lenovo-and-superfish-penetrate-the-heart-of-a-computers-security/
[20] http://arstechnica.com/security/2015/02/ssl-busting-code-that-threatened-lenovo-users-found-in-a-dozen-more-apps/
[21] https://firstlook.org/theintercept/2015/02/19/great-sim-heist/
[22] http://www.belowgotham.com/Darknet-Sweep.pdf
[23] http://www.wired.com/2014/12/fbi-metasploit-tor/
[24] http://www.wired.com/2014/08/federal-cybersecurity-director-guilty-child-porn-charges/
[25] https://grugq.github.io/presentations/COMSEC%20beyond%20encryption.pdf
[26] http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html
[27] http://cryptome.info/0001/cia-nsa-scs.htm
[28] http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html
[29] http://www.wired.com/2014/09/fbi-silk-road-hacking-question/
[30] http://www.itworld.com/article/2881775/four-technologies-that-betrayed-silk-roads-anonymity.html
[31] http://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/
[32] http://www.theguardian.com/film/2014/oct/16/citizen-four-review-edward-snowden-documentary
[33] http://cryptome.org/2012/06/comms-folly.htm

[34] http://www.blogsofwar.com/2013/11/11/interview-hacker-opsec-with-the-grugq

[35] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

[36] http://www.belowgotham.com/RootkitArsenalTOC.htm

[37] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no2/article01.html

[38] http://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/

[39] https://privacysos.org/node/1177

[40] http://www.vogue.com/11122973/sarah-harrison-edward-snowden-wikileaks-nsa/

[41] http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html

[42] http://www.vice.com/read/the-los-zetas-drug-cartel-have-their-own-radio-network

[43] http://www.theguardian.com/world/2010/dec/05/lebanon-warned-allies-hezbollah-telecoms

[44] http://silent-pocket.com/

[45] http://www.networkworld.com/article/2855134/microsoft-subnet/the-latest-mobile-trend-flip-phones.html

[46] http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london

[47] http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533

[48] mailto:corrections@alternet.org?Subject=Typo on When Strong Encryption Isn&#039;t Enough to Protect Our Privacy

[49] http://www.alternet.org/

[50] http://www.alternet.org/%2Bnew_src%2B