Editor: Charles Petrie • petrie@stanford.edu

How Badly Do You Want Privacy?

Charles Petrie • *University of St. Gallen, Switzerland*

Volker Roth • *Freie Universität Berlin, Germany*

So you want to be a whistle blower. Just gen up a strong PGP key, hide your IP address with Tails and the Tor browser (running off your USB stick), and use a secure email such as Hushmail (www.hushmail.com) or Hide My Ass (www.hidemyass.com). Make sure you're using HTTPS. Done, yes? So, why did Edward Snowden have to flee?

Not only did he know that they would find him sooner or later, but that it would be sooner with the available technology.

Too Many Vulnerabilities

There are lots of holes in technology-dependent solutions. Even an anonymizing network such as Tor is theoretically vulnerable to passive analysis. With far-reaching network access and enough computing power, the routing can be determined. The security agencies claim they can't. Go ahead and trust this if you wish. But let's look at the other vulnerabilities.

First, there are government hack attacks. A previous "Peering" column[1] mentioned the AdLeaks technology that would defeat passive detection by an agency such as the US National Security Agency (NSA). But any computer (that you know of) is subject to attack. If they can get into the machine at either end of a communication, your communications are compromised. And usually you don't really know how secure the machine on the other end is. Even if the server is really secure, they can attack the client. One feature of AdLeaks is that they won't know which client to attack. But this is still a vulnerability.

The major western security agencies claim that they haven't been able to break the main Tor protocol, but they've been successful in attacking the users' computers and even Tor servers.[2] (By the way, they make such attacks on the Tor system even though it's partially funded by the US government.)

Within the US, the FBI has been successful in installing malware on some servers to learn the real IP address of users, most notably in breaking Silk Road and shutting down hundreds of Tor network nodes, but also in some other cases. They've declined to be more specific in how they accomplished this hacking.

Second, the government's job is made easier by the fact that software is eternally imperfect and there are always exploits. Anyone depending upon HTTPS was probably disappointed by the Heartbleed bug. Anyone thinking this won't ever happen again is simply ignoring the history of HTTPS bugs.

We can hear you now saying that's what someone gets for depending upon non-professional and Open Source software, though much of the Internet infrastructure does rely on such software. But major commercial operating systems are also continuously beset by security bugs (remember "goto fail"?), so much so that the only defense is to quickly fix them before they can be exploited. Peter Loscocco and his colleagues wrote an excellent paper on this topic,[3] which also demonstrates that, unsurprisingly, the NSA is on top of this. Though this paper is old, it has proven to be correct.

Other Encryption Issues

Aside from these issues, you can always rely upon the encryption delivered by the major providers, right? Unfortunately, apart from direct attacks and bugs, even if everything else was perfect, you would still be at the mercy of the NSA, because these companies cooperate in opening up their encryption.[4]

We mentioned Hushmail and Hide My Ass near the beginning of this article. They're not secure against the government compelling them to turn over their keys or their users' email. Lavabit and Silent Circle shut down their email

Published by the IEEE Computer Society
1089-7801/15/$31.00 © 2015 IEEE

services because of this possibility. Skype is also unsafe.

It's not so much that the NSA and these providers are conspiring to control everything. Google, Microsoft, and Apple are certainly large corporations and there are large corporations who share interests with the NSA, but not necessarily these providers. But, as US companies, they have no choice. They're required by law to open up their encryption to the NSA.

They could get around this by not having access to your messages, but then that would make the service inconvenient and they want your data anyway. Their business model makes you insecure.

So, if you want to spend your money with these companies based upon promises of security, it's a free market, but you don't always get what you pay for. (And please don't think you aren't paying because the service or product is free.)

You could make yourself a complicated ring seal and buy good-quality sealing wax to convey your typewritten letters. But of course a good 3D scanner/printer would make short work of replicating the seal on your intercepted letters.[5]

Back to the non-professionals. There's another choice this year: ProtonMail.[6,7] It's a browser-based mail service that keeps users' data and mail encrypted at all times, inaccessible even to them. Secret user data needed in the browser is downloaded and decrypted locally with a password that's never sent to them. Their software implements end-to-end encryption. This is probably the best you can get for secure browser-based mail. Of course, their security rests on the enforcement of the Same Origin policy in browsers, user-chosen passwords, and our good old friends, Transport Layer Security and Secure Sockets Layer (TLS/SSL), along with a long list of X.509 trust anchors. Well, if you're still unsure what that means then you may wish to read further.[10] Being Swiss-based, they argue, means they can't be compelled by other governments, such as the US government, to help compromising users' keys or mail. We would like to believe that, but in the murky and shadowy world of intelligence service cooperation, this reassurance might not be worth as much as you would hope.

Another recommendation is to use a combination of open source software for your communication needs, such as chat clients with Off The Record (OTR) support, Tor, TrueCrypt, CSpace, and/or ZRTP.[8] (Finding and implementing is left as an exercise for the reader.)

But try to use a secure operating system. Oh, wait ...[3,8]

There is hope. Even if technology isn't perfect, you can use technology to make it difficult for the government to invade your privacy. You just have to use it. But remember to defend your rights to use it. Your best bet is really to use your democracy to make government hacking and wholesale intercepts of citizen messages strictly illegal and hold the intelligence agencies accountable for breaking the law.

References

1. C. Petrie, "The Age of DIY," *IEEE Internet Computing*, vol. 17, no. 6, 2013, pp. 93–94.
2. J. Ball, B. Schneier, and G. Greenwald, "NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users," *The Guardian*, 4 Oct. 2013; www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.
3. P. Loscocco et al., "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments," *Proc. 21st National Information Systems Security Conf.*, 1998, pp. 303–314; www.nsa.gov/research/_files/publications/inevitability.pdf.
4. G. Greenwald et al., "Microsoft Handed the NSA Access to Encrypted Messages," 11 July 2013; www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.
5. J. Hicks, "Postal Service Almost Never Denies Mail-Surveillance Requests," *The Washington Post*, 20 Nov. 2014; www.washingtonpost.com/blogs/federal-eye/wp/2014/11/20/postal-service-almost-never-denies-mail-surveillance-requests/.
6. T.B. Lee, "NSA-Proof Encryption Exists. Why Doesn't Anyone Use It?" *The Washington Post*, 14 June 2013; www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/.
7. H. Slade, "The Only Email System The NSA Can't Access," *Forbes*, 19 May 2014; www.forbes.com/sites/hollieslade/2014/05/19/the-only-email-system-the-nsa-cant-access/.
8. J. Appelbaum et al., "Prying Eyes: Inside the NSA's War on Internet Security," *Der Spiegel*, 28 Dec. 2014; www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.
9. Q. Norton, "Everything Is Broken," *The Message*, 20 May 2014; https://medium.com/message/everything-is-broken-81e5f33a24e1.
10. A. Arnbak et al., "Security Collapse in the HTTPS Market," *Comm ACM*, vol. 57, no. 10 2014, pp. 47–55; http://doi.acm.org/10.1145/2660574.

Charles Petrie teaches and coaches the topic of innovation in design thinking at the University of St. Gallen, Switzerland (http://dthsg.com/dt-at-hsg/). He retired as a senior research scientist from the Stanford University Computer Science Department. His research topics are concurrent engineering, enterprise management, and collective work. Petrie has a PhD in computer science from the University of Texas at Austin. He was a founding member of the technical staff at the MCC AI Lab, the founding editor in chief of *IEEE Internet Computing,* and the founding chair of the Semantic Web Services Challenge. He also manages the Black

Rock City Municipal Airport 88NV. Contact him at petrie@cdr.standford.edu.

Volker Roth is a professor in the Institute of Computer Science at Freie Universität Berlin. His primary research is in the area of information systems security, with a particular interest in secure identity and psychological acceptability of security mechanisms. Roth has a Dr.-Ing. in computer science from Technische Universität Darmstadt. Contact him at volker.roth@fu-berlin.de.