Asia Times Online
www.atimes.com

The NSA war on Internet integrity

By Peter Lee

The US government has taken a pretty decent open network idea - the Internet - and turned it into a security nightmare.

In one of life's many ironies, the US was forced to degrade the security functions and overall integrity of the Internet because the US Constitution, law, and public and techie opposition combined to impede legal US government surveillance access to communications over the Internet.

Instead of accepting these limits, the US government sought to evade them - by weakening the encryption and security regimes that are at the heart of secure Internet communications for businesses and innocent civilians, as well as for the usual

The US government has taken a pretty decent open network idea - the Internet - and turned it into a security nightmare.

In one of life's many ironies, the US was forced to degrade the security functions and overall integrity of the Internet because the US Constitution, law, and public and techie opposition combined to impede legal US government surveillance access to communications over the Internet.

Instead of accepting these limits, the US government sought to evade them - by weakening the encryption and security regimes that are at the heart of secure Internet communications for businesses and innocent civilians, as well as for the usual suspects invoked to justify subversion of Internet privacy: terrorists, criminals, and pedophiles.

The role of US IT corporations in crippling the security and privacy functions of the Internet is an awkward and relatively unexplored question.

So far, the most overt naming and shaming has taken place concerning cooperation of the IT bigs in the National Security Agency's PRISM program - which involved controlled, legally colored access to unencrypted materials on corporate servers. Under PRISM, the NSA apparently installed equipment at corporate sites to process government requests for unencrypted user data if it involved people that the NSA was "51%" sure weren't US persons.

Included in the Snowden documents was a slide showing the accession of the US IT heavyweights to the PRISM regime, starting with Microsoft in 2007 and including Yahoo!, Google, Facebook, Youtube, Skype, AOL, and Apple. PRISM looked something like exploitation of the CALEA (Communications Assistance for Law Enforcement Act) mandated backdoors in US telecommunications equipment, albeit with the disturbing realization that these backdoors could be exploited by anonymous NSA analysts without a FISA court order for a week and, when the free week was up, upon resort to the notoriously rubber-stamp FISA court (without the need to show probable cause as is the case when applying to get a warrant to spy on a US citizen).

The Washington Post's Bernard Gellman spoke of NSA efforts to suppress the names of the nine companies named on the PRISM slide:

Speaking at a Cato Institute conference on Wednesday, Gellman said The Washington Post has a practice of talking to the government before running stories that may impact national security. According to Gelman, there were "certain things" in the PRISM slides that they agreed raised legitimate security concerns. But, he said:

The thing that the government most wanted us to remove was the names of the nine companies. The argument, roughly speaking, was that we will lose cooperation from companies if you expose them in this way. And my reply was "that's why we are including them." Not in order to cause a certain result, or to get you to lose your cooperation but if the harm that you are describing consists of reputational or business damage to a company because the public doesn't like what it's doing or you're doing, that's the accountability we are supposed to be promoting.

Gellman believes that it's because the names were released that many of those technology companies started to be vocal advocates of greater transparency about the program. While they "previously had very little incentive to fight for disclosure because it wasn't their information that was being collected and there was no market pressure," he said, these companies "are now, because they are suffering business damage and reputational harm, pushing very hard in public debate and in lawsuits to disclose more about how the collection program works," which current FISA Court orders prohibit them from telling the public about. [1]

The NSA Nine, perhaps alerted to the upcoming PR firestorm, went public with defenses that sought to give a picture of limited, by-the-book, almost grudging cooperation. There was a lot of generous reporting about the struggles of Google, Facebook, Yahoo! et al to buck their NSA gag orders so they could reveal to an eager world how hard they have struggled to protect user privacy. Also, the PRISM revelations were explained and excused in the public media since they involved responses to FISA court warrants with specific, identified targets and, for that matter, were targeting "non-US persons", ie non-US citizens residing outside the United States.

What IT professionals found more disturbing than government backdoors into corporate servers, however, was Snowden's revelations of the NSA's war on encryption.

As I describe in an article in the upcoming print edition of Counterpunch, the NSA has aggressively acquired capabilities and resources in pursuit of its goal to crack encrypted e-mail, virtual private networks (VPNs), and mobile device communications.

Possible corporate collusion in the apparent NSA campaign to undermine the integrity of encryption and, for that matter, degrade the systemic security functionality of the Internet has received relatively little attention.

It can be speculated that some US IT corporations may have cooperated with the NSA in weakening security standards, installing backdoors, and botching implementation, perhaps with the idea that these were vulnerabilities that probably only the NSA could exploit.

Some of the most egregious NSA shenanigans have been in the arcane area of fiddling with the random number generators that lie at the heart of encryption. If the randomness is compromised incrementally, cracking becomes easier. And the more networked computers an attacker has, and the more messages are stored for analysis, the more important the reduced randomness of the encryption becomes.

It can be seen how US corporations might go along with the US government's machinations in this area; after all, the possibility of a non-NSA actor acquiring all those capabilities to exploit random number generator flaws seems vanishingly small.

At least up until now, there seems to be a code of techie omerta (and maybe the well-founded fear of a lawsuit) that precludes calling out IT bigs for climbing into bed with the NSA on the encryption issue.

In the issue of undermining cryptography, it would seem that a finger could be pointed at RSA Corp. RSA was founded by the three academics, Ron Ravist, Avi Shamir, and Leonard Adleman, who created the RSA algorithm at the heart of many encryption schemes (currently ensconced at MIT, Weizmann Institute, and USC, respectively, the three are apparently not involved in the running of the eponymous corporation).

RSA made it into the news by being forced to withdraw one of its products after September 2013 Snowden reporting let it be known that a random number generating scheme, DUAL EC EBRG, had been compromised during the standards-writing process by the NSA.

What made the RSA climbdown particularly damning was that 1) ever since 2007, DUAL EC EBRG had been recognized by the crypto community as flawed; 2) although its inclusion in encryption products sold to the US government as an option is mandated, no self-respecting crypto-expert ever deployed it as the default random number generator; 3) except RSA, which was was chock-a-block with top flight cryptographers who presumably knew better.

A recent edition of National Public Radio's Science Friday program featured Philip Zimmerman, the father of PGP public key encryption (which provoked the all-out NSA war on encrypted communications), Stanford crypto authority Martin Hellman, and Matthew Green, the Johns Hopkins professor who was in the news after his university pressed him to delete a blog post about the crypto wars.

Host Ira Flatow asked Philip Zimmerman why RSA would have done such a thing. There was a long, awkward silence and some awkward laughter before Zimmerman slid into the passive voice/third person zone:

ZIMMERMAN: And yet RSA did a security - did use it as their default random number generator. And they do have competent cryptographers working there. So.

FLATOW: How do you explain that?

ZIMMERMAN: Well, I'm not going to - I think I'd rather not be the one to say.

(LAUGHTER)

FLATOW: But if someone else were to say it, what would they say?

ZIMMERMAN: Well, someone else might say that maybe they were incentivized. [2]

RSA is also responsible for another eminently crackable encryption standard, RC4.

The flagship RSA algorithm also has an unfortunate feature in its implementation in the Secure Socket Layer encryption at the heart of e-commerce and mobile device connections (to ensure privacy when connecting via a public WiFi hotspot). The encryption key used on the server side (ie the servers at Amazon, Visa, your bank, etc.) doesn't change.

Which means if someone stores the encrypted communications (presumably a capability that only the NSA has, thanks to its privileged position on the Internet backbones) and acquires the server side key (something that the NSA is apparently extremely aggressive about), the traffic can eventually be decoded and read.

Nevertheless, nobody has expressed an interest in getting in RSA's face for its possible role in implementing the NSA's weak encryption strategy or, for that matter, exploring Google's, Cisco's, Microsoft's, or Facebook's possible roles in enabling the NSA's acquisition of encryption keys.

This is despite - or because of - the fact that these are publicly traded corporations with vulnerable market capitalizations and accountable to their boards and stockholders and therefore compelled to engage with the media - unlike the NSA.

The collusion between industry and government which, I suspect, may lie at the heart of the NSA revelations, can only be defended if the NSA can claim to control the "resources and methods" and thereby provide legal and moral cover to the IT corporations that justify their cooperation with the thought that only the NSA can crack these systems with these tools, so it's OK.

Well, it's probably not OK.

Edward Snowden walked out the door with the keys to the kingdom. He's not revealing all the keys. But somebody else might.

Much of what's come out has been exposure of massive hacks that rely on the NSA's unique, privileged access to the Internet backbone and corporate servers, the ability to massively archive communications, and to harness unparalleled brain power and computing power for systemic surveillance, analysis, and decryption.

The NSA has more money than god, so it can pursue these capabilities, up to and including quantum computing, which will win the NSA a Nobel Prize as well as the ability to crack any encryption in the world if it can figure out how to really do it. But the real day to day action may lie in evading encryption security through a multitude of smaller exploits lovingly collected, catalogued, and exploited by the NSA.

There are a lot of security flaws on the Internet. Presumably, the NSA created some, mandated its corporate partners to install some more, and picked up information on genuine flaws from black and white hat hackers and their own employees. I imagine there's a lot of penny ante hacks the NSA knows and does, smaller-scale, copyable tricks that Edward Snowden and his media partners have carefully and responsibly chosen not to reveal. Things that the NSA chooses not to alert the IT companies about, at least not right away, because they are convenient, but which the "bad guys" could exploit if they found out.

Maybe things like the Microsoft zero-day (built-in) software vulnerability which the PRC allegedly exploited for its "Aurora" hack of Gmail and other high-tech companies in 2010. Bruce Schneier speculated at the time this could have been the exploitation of the backdoor Google had thoughtfully installed for the US government - and Aurora apparently turned out to be exactly that, according to the Washington Post in May 2013:

Former government officials with knowledge of the breach said attackers successfully accessed a database that flagged Gmail accounts marked for court-ordered wiretaps. Such information would have given attackers insight into active investigations being conducted by the FBI and other law enforcement agencies that involved undercover Chinese operatives. [3]

The concurrent exposure of the e-mail accounts of Chinese dissidents, which were described as "a separate branch" of the 2010 Aurora attack on Google - and which allowed Google to clothe itself in anti-authoritarian righteousness while sliding past the issue of government backdoors into its services - raised the interesting possibility that the US government itself was monitoring the e-mail accounts of Chinese dissidents, and that's how they turned up in the database.

One can also speculate that the de facto ban on the use of the PRC-based Huawei and ZTE equipment on the American telecommunications backbone was implemented because the US government was loath to give China any privileged insight into exactly how the covert legal and extra-legal surveillance sausage is created, and denying potential Chinese access to US government watch-lists.

It appears that the NSA has an enormous and potentially unhealthy interest in acquiring and exploiting vulgar computer and Internet vulnerabilities in order to gain access to information it can't get through legal compulsion, court-mandated access, or use of its own big science decryption capabilities.

In describing the NSA's Foxacid program (in which the target computer is duped into communicating with an NSA tool for inserting spyware) Bruce Schneier described how NSA grunts can call up exploits to penetrate a target system as if they're ordering options off a Chinese take-out menu:

Here are the FOXACID basics: By the time the NSA tricks a target into visiting one of those servers, it already knows exactly who that target is, who wants him eavesdropped on, and the expected value of the data it hopes to receive. Based on that information, the server can automatically decide what exploit to serve the target, taking into account the risks associated with attacking the target, as well as the benefits of a successful attack. According to a top-secret operational procedures manual provided by Edward Snowden, an exploit named Validator might be the default, but the NSA has a variety of options. The documentation mentions United Rake, Peddle Cheap, Packet Wrench, and Beach Head - all delivered from a FOXACID subsystem called Ferret Cannon. Oh how I love some of these code names. (On the other hand, EGOTISTICALGIRAFFE has to be the dumbest code name ever.)

Snowden explained this to Guardian reporter Glenn Greenwald in Hong Kong. If the target is a high-value one, FOXACID might run a rare zero-day exploit that it developed or purchased. If the target is technically sophisticated, FOXACID might decide that there's too much chance for discovery, and keeping the zero-day exploit a secret is more important. If the target is a low-value one, FOXACID might run an exploit that's less valuable. If the target is low-value and technically sophisticated, FOXACID might even run an already-known vulnerability.

We know that the NSA receives advance warning from Microsoft of vulnerabilities that will soon be patched; there's not much of a loss if an exploit based on that vulnerability is discovered. FOXACID has tiers of exploits it can run, and uses a complicated trade-off system to determine which one to run against any particular target.

This cost-benefit analysis doesn't end at successful exploitation. According to Snowden, the TAO - that's Tailored Access Operations - operators running the FOXACID system have a detailed flowchart, with tons of rules about when to stop. If something doesn't work, stop. If they detect a PSP, a personal security product, stop. If anything goes weird, stop. This is how the NSA avoids detection, and also how it takes mid-level computer operators and turn them into what they call "cyberwarriors." It's not that they're skilled hackers, it's that the procedures do the work for them. [4]

We can assume Edward Snowden knows about the NSA's portfolio of computer, server, and router vulnerabilities ... and so does the next Edward Snowden, who might find it a lot more pleasant and profitable to sell the keys to the kingdom to Chinese intelligence or the Russian mafia, instead of ruining his life to inform the public and win Glenn Greenwald a (well-deserved) Pulitzer.

Andy Greenberg, a Forbes columnist, provided what he alleged were black-market prices for zero-day exploits, ie inherent vulnerabilities in software systems:

A six-figure price for a single hacking technique may sound extravagant, but it's hardly unique. Based on speaking with sources in this secretive but legal trade, I've assembled a rough price list for zero-day exploits below. [5]

That implies there's a lot of money sitting on the table for the next disgruntled/libertarian and/or greedy system admin to scoop up on his way out of the NSA door.

To market their products, US IT companies rely on the now discredited assumption that they provide the best security that they can to their customers within the limits of the law. The actual situation appears to be that much of the US industry provides the minimum level of security that the NSA permits it to implement.

The most logical conclusion would be to sweep aside the current, compromised regime of the NSA's enablers and replace it with a new, open source system from scratch. But that would involve replacing hundreds of millions of dollars worth of equipment and - perhaps more importantly - stripping away hundreds of billions of dollars of market capitalization of US IT corporations complicit in the current system. That's where the implication of the Edward Snowden revelations seems to lead. But, as yet, it seems nobody wants to go there.

Notes:
[1] Post reporter: Here's why we refused the NSA's demand to censor the names of PRISM companies, Washington Post, October 9, 2013.
/ [2] Click here.
[3] Google Aurora Hack Was Chinese Counterespionage Operation, Information Week Security, May 21, 2013.
[4] Schneier on Security, October 9, 2013.
[5] Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits, Forbes Magazine, March 23, 2012.

Peter Lee writes on East and South Asian affairs and their intersection with US foreign policy.