

How to remain secure against NSA surveillance

The NSA has huge capabilities – and if it wants in to your computer, it's in. With that in mind, here are five ways to stay safe



Bruce Schneier theguardian.com, Thursday 5 September 2013 15.06 EDT



'Trust the math. Encryption is your friend. That's how you can remain secure even in the face of the NSA.' Photograph: Beck Diefenbach/Reuters

Now that we have enough details about how the <u>NSA</u> eavesdrops on the <u>internet</u>, including <u>today's disclosures</u> of the <u>NSA</u>'s deliberate weakening of cryptographic systems, we can finally start to figure out how to protect ourselves.

For the past two weeks, I have been working with the Guardian on <u>NSA</u> stories, and have read hundreds of top-secret NSA documents provided by whistleblower Edward Snowden. I wasn't part of today's story – it was in process well before I showed up – but everything I read confirms what the Guardian is reporting.

At this point, I feel I can provide some advice for keeping secure against such an adversary.

The primary way the NSA eavesdrops on internet communications is in the network. That's where their capabilities best scale. They have invested in enormous programs to automatically collect and analyze network traffic. Anything that requires them to attack individual endpoint computers is significantly more costly and risky for them, and they will do those things carefully and sparingly.

Leveraging its secret agreements with telecommunications companies – all the US and UK ones, and many other "partners" around the world – the NSA gets access to the communications trunks that move internet traffic. In cases where it doesn't have that sort of friendly access, it does its best to surreptitiously monitor communications channels: tapping undersea cables, intercepting satellite communications, and so on.

That's an enormous amount of data, and the NSA has equivalently <u>enormous capabilities</u> to quickly sift through it all, looking for interesting traffic. "Interesting" can be defined in many ways: by the source, the destination, the content, the individuals involved, and so on. This data is funneled into the vast NSA system for future analysis.

The NSA collects much more <u>metadata</u> about internet traffic: who is talking to whom, when, how much, and by what mode of communication. <u>Metadata</u> is a lot easier to store and analyze than content. It can be extremely personal to

the individual, and is enormously valuable intelligence.

The Systems Intelligence Directorate is in charge of data collection, and the resources it devotes to this is staggering. I read status report after status report about these programs, discussing capabilities, operational details, planned upgrades, and so on. Each individual problem – recovering electronic signals from fiber, keeping up with the terabyte streams as they go by, filtering out the interesting stuff – has its own group dedicated to solving it. Its reach is global.

The NSA also <u>attacks network devices directly</u>: routers, switches, firewalls, etc. Most of these devices have <u>surveillance</u> capabilities <u>already built in</u>; the trick is to surreptitiously turn them on. This is an especially fruitful avenue of attack; routers are updated less frequently, tend not to have security software installed on them, and are generally ignored as a vulnerability.

The NSA also devotes considerable resources to attacking endpoint computers. This kind of thing is done by its TAO – <u>Tailored Access Operations</u> – group. TAO has a menu of exploits it can serve up against your computer – whether you're running Windows, Mac OS, Linux, iOS, or something else – and a variety of tricks to get them on to your computer. Your anti-virus software won't detect them, and you'd have trouble finding them even if you knew where to look. These are hacker tools designed by hackers with an essentially unlimited budget. What I took away from reading the Snowden documents was that if the NSA wants in to your computer, it's in. Period.

The NSA deals with any encrypted data it encounters more by subverting the underlying cryptography than by leveraging any secret mathematical breakthroughs. First, there's a lot of bad cryptography out there. If it finds an internet connection protected by MS-CHAP, for example, that's easy to break and recover the key. It exploits poorly chosen user passwords, using the same dictionary attacks hackers use in the unclassified world.

As was <u>revealed today</u>, the NSA also works with security product vendors to ensure that commercial encryption products are broken in secret ways that only it knows about. We know this has happened historically: <u>CryptoAG</u> and <u>Lotus Notes</u> are the most public examples, and there is evidence of a back door in <u>Windows</u>. A few people have told me some recent stories about their experiences, and I plan to write about them soon. Basically, the NSA asks companies to subtly change their products in undetectable ways: making the random number generator less random, leaking the key somehow, adding a common exponent to a public-key exchange protocol, and so on. If the back door is discovered, it's explained away as a mistake. And as we now know, the NSA has enjoyed enormous success from this program.

TAO also hacks into computers to recover long-term keys. So if you're running a VPN that uses a complex shared secret to protect your data and the NSA decides it cares, it might try to steal that secret. This kind of thing is only done against high-value targets.

How do you communicate securely against such an adversary? Snowden <u>said it</u> in an online Q&A soon after he made his first document public: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

<u>I believe this is true</u>, despite today's revelations and tantalizing hints of "groundbreaking cryptanalytic capabilities" made by James Clapper, the director of national intelligence in another top-secret document. Those capabilities involve deliberately weakening the cryptography.

Snowden's follow-on sentence is equally important: "Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."

Endpoint means the software you're using, the computer you're using it on, and the local network you're using it in. If the NSA can modify the encryption algorithm or drop a Trojan on your computer, all the cryptography in the world doesn't matter at all. If you want to remain secure against the NSA, you need to do your best to ensure that the encryption can operate unimpeded.

With all this in mind, I have five pieces of advice:

- 1) **Hide in the network**. Implement hidden services. Use Tor to anonymize yourself. Yes, the NSA targets Tor users, but it's work for them. The less obvious you are, the safer you are.
- 2) **Encrypt your communications**. Use TLS. Use IPsec. Again, while it's true that the NSA <u>targets encrypted connections</u> and it may have explicit exploits against these protocols you're much better protected than if you communicate in the clear.

- 3) Assume that while your computer can be compromised, it would take work and risk on the part of the NSA so it probably isn't. If you have something really important, use an air gap. Since I started working with the Snowden documents, I bought a new computer that has *never* been connected to the internet. If I want to transfer a file, I encrypt the file on the secure computer and walk it over to my internet computer, using a USB stick. To decrypt something, I reverse the process. This might not be bulletproof, but it's pretty good.
- 4) **Be suspicious of commercial encryption software**, **especially from large vendors**. My guess is that most encryption products from large US companies have NSA-friendly back doors, and many foreign ones probably do as well. It's prudent to assume that foreign products also have foreign-installed backdoors. Closed-source software is easier for the NSA to backdoor than open-source software. Systems relying on master secrets are vulnerable to the NSA, through either <u>legal</u> or more clandestine means.
- 5) Try to use public-domain encryption that has to be compatible with other implementations. For example, it's harder for the NSA to backdoor TLS than BitLocker, because any vendor's TLS has to be compatible with every other vendor's TLS, while BitLocker only has to be compatible with itself, giving the NSA a lot more freedom to make changes. And because BitLocker is proprietary, it's far less likely those changes will be discovered. Prefer symmetric cryptography over public-key cryptography. Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can.

Since I started working with Snowden's documents, I have been using <u>GPG</u>, <u>Silent Circle</u>, <u>Tails</u>, <u>OTR</u>, <u>TrueCrypt</u>, <u>BleachBit</u>, and a few other things I'm not going to write about. There's an undocumented encryption feature in my <u>Password Safe</u> program from the command line); I've been using that as well.

I understand that most of this is impossible for the typical internet user. Even I don't use all these tools for most everything I am working on. And I'm still primarily on Windows, unfortunately. Linux would be safer.

The NSA has turned the fabric of the internet into a vast surveillance platform, but they are not magical. They're limited by the same economic realities as the rest of us, and our best defense is to make surveillance of us as expensive as possible.

Trust the math. Encryption is your friend. Use it well, and do your best to ensure that nothing can compromise it. That's how you can remain secure even in the face of the NSA.



Get the Guardian's daily US email

Our editors' picks for the day's top news and commentary delivered to your inbox each morning.

Sign up for the daily email

More from the Guardian



Nirvana's importance hasn't kill it off diminished 31 Aug 2013



Twenty years after In Utero, True Blood: why it's time to 05 Sep 2013



10 commandments for new teachers 03 Sep 2013



What's this?

West and Russia clash over UK evidence of sarin gas attack in Syria 05 Sep 2013

More from around the web



Wars Between Nations are Being Fought on Computer Screens

(The TIBCO Blog)



to Life Back on The Daily Show? (The Daily Show with Jon Stewart)



How's Jon Stewart Adjusting 10 Famous People You Didn't Know Were Black (How Stuff Works)



Should offshore manufacturing be counted as U.S. production? (PTC)

Ads by Google

Barracuda Firewall

Next Gen Features w/L7 and Cloud Malware Filtering.

www.Barracuda.com

Protection Education

B.S./M.S. in Protection Management Taught by Former CIA, FBI and DoD

www.Henley-Putnam.edu

Live Bandwidth Monitoring

Spot the sudden spike in Internet Bandwidth usage graph in real-time

www.manageengine.com/FWAnalyzer

© 2013 Guardian News and Media Limited or its affiliated companies. All rights reserved.

;				