

A Few Thoughts on Cryptographic Engineering

Some random thoughts about crypto. Notes from a course I teach. Pictures of my dachshunds.



Tuesday, September 10, 2013

A note on the NSA, the future, and fixing mistakes

Readers of this blog will know this has been an [interesting couple of days for me](#). I have very mixed feelings about all this. On the one hand, it's brought this blog a handful of new readers who might not have discovered it otherwise. On the other hand, it's made me a part of the story in a way that I don't deserve to be.



After speaking with my colleagues and -- most importantly -- with my wife, I thought I might use the last few seconds of my (inadvertent) 'fame' to make some of highly non-technical points regarding the recent NSA revelations, and mainly: my decision to [blog about them](#).

I believe that my first point should be self-evident: The NSA has made a terrible set of mistakes. These range from policy decisions to technical direction, all the way to matter of their own internal security. I believe there may have been a time when these mistakes could have been mitigated or avoided, but that time has passed. Personally I believe it passed even before Edward Snowden sent his first email to the press. But the disclosures of classified documents have set those decisions in stone.

With the mistakes made, we're now faced with the job of cleaning up the mess. To that end there are two sets of questions: *public policy questions* -- who should the NSA be spying on, and how far should they be allowed to go in pursuit of that goal? And a second set of more *technical questions*: how do we repair the technical blowback from these decisions?

There are many bright people -- quite a few of whom are [in Congress](#) -- tending to the first debate. While I have my opinions about this debate, they're (mostly) not the subject of this blog. Even if they were, I'm probably the wrong person to discuss them.

So my concern is the technical question. And I stress that while I label this '*technical*', it isn't just a question of equations and logic gates. The tech sector is one of the fastest growing and most innovative areas of the US economy. I believe the NSA's actions have caused long-term damage to our credibility, in a manner that (ironically) threatens our own national security as well as our economic viability.

The question to me -- as an American and as someone who cares about the integrity of speech -- is *how we restore faith in our technology*. I don't have the answers to this question right now. Unfortunately this is a long-term problem that will consume the output of researchers and technologists much more talented than I am. I only hope to be involved in the process.

So while I know there are people at NSA who must be cursing Edward Snowden's name (and possibly even my own!) I hope that they understand the game we're playing now. Their interests as well as mine now depend on fixing the damage. Downplaying the extent of the damage, or trying to restrict access to (formerly) classified documents does nobody any good.

It's time to start fixing things.

Posted by [Matthew Green](#) at 5:35 AM

+7 [Recommend this on Google](#)

27 comments:

[Anonymous](#) [September 10, 2013 at 6:06 AM](#)

About Me



Matthew Green

I'm a cryptographer and research professor at Johns Hopkins University. I've designed and analyzed cryptographic systems used in wireless networks, payment systems and digital content protection platforms. In my research I look at the various ways cryptography can be used to promote user privacy.

[My website](#)
[Guide to this blog](#)
[My twitter feed](#)
[Useful crypto resources](#)
[RSS](#)
[Bitcoin tipjar](#)
[View my complete profile](#)

Popular Posts



On the NSA

Let me tell you the story of my tiny brush with the biggest crypto story of the year. A few weeks ago I received a call from a reporter a...

Dear Apple: Please set iMessage free

Normally I avoid complaining about Apple because (a) there are plenty of other people carrying that flag, and (b) I honestly like Apple ...



Here come the encryption apps!

It seems like these days I can't eat breakfast without reading about some new encryption app that will (supposedly) revolutionize our c...



Zerocoin: making Bitcoin anonymous

This is what it's like to die of stupid. Wow, what the heck is going on with Bitcoin? When I started this post, the value of a si...



Attack of the week: RC4 is kind of broken in TLS

Update: I've added a link to a page at Royal Holloway describing the new attack. Listen, if you're using RC4 as your primary c...



The USA has to fix a lot now otherwise US companies will get bankrupt because nobody trust products "Made in USA" anymore.
I sold my latest Android smartphone and will never again use this OS or any other closed source OS made in the US.

SELinux is thankfully not included in Debian based distributions. I don't trust the USA. Don't play poker with them as they will always try to cheat.

Good luck over there in the US.
Greetings from South Africa.

[Reply](#)



Anonymous [September 10, 2013 at 6:42 AM](#)

Same here in Europe, trust is at bottom level because the US government is treating non-Americans as 2nd class humans. The USA are not the only country which has a constitution to protect citizens. Lots of people are protected by a constitution like that. Furthermore there is the Universal declaration of Human Rights and the European Convention of Human Rights that protects the privacy of all humans, protects humans from surveillance like that, and which ensures a fair trial. The USA is terribly wrong to not feel the need to respect such laws.

Europeans will be avoiding hardware products from the USA because the industry creates (willingly or not) vulnerable hardware. We will be avoiding Operating systems like Microsoft Windows, Apple iOS and Google Android. We will be avoiding Software and Internet services from the USA.

I guess the only solution for the IT industry is open hardware, open software, open standards for communication and encryption. Thanks to the NSA we have to restart basically from point zero.

To be clear: the damage was done by the actions taken by the NSA, not by Edward Snowden who only revealed the wrong doings to the public.

[Reply](#)

[Replies](#)



marchwinds [September 10, 2013 at 1:57 PM](#)

Sadly, European governments are most likely doing the same thing as the NSA - it's just the scale that may be smaller. The same with Canada, and certainly Russia and China would have huge spy apparatuses. The difference is that America's program has been revealed to the world - now we need Snowdens from other spy agencies in other countries to step forward and tell the rest of the story.



Dan [September 10, 2013 at 3:39 PM](#)

At the level of spying that the NSA is doing, scale does matter. My third world government can't even afford all the fancy wiretapping stuff your local police have, and don't have enough technical people to use it effectively. So I have more to fear a far-off spy agency that reads all foreign communications than my own government.

[Reply](#)



Anonymous [September 10, 2013 at 7:50 AM](#)

I'm curious why the previous 2 comments talk about Android as a closed OS... I agree with their feelings though - I too am more skeptical of US technology now.

[Reply](#)

Anonymous [September 10, 2013 at 8:39 AM](#)



Can Apple read your iMessages?

(source: Gizmodo) About a year ago I wrote a short post urging Apple to

publish the technical details of iMessage encryption. I...



Attack of the week: Cross-VM side-channel attacks

It's been a busy week for crypto flaws. So busy in fact, that I'm totally overwhelmed and paralyzed trying to write about them. I...

Surviving a bad RNG

A couple of weeks ago I wrote a long post about random number generation , which I find to be one of the most fascinating subjects in crypto...

Let's talk about ZRTP

Source: Zooko . I just checked the date on my last post and it seems that I haven't blogged in nearly a month. Believe me, this is...

Is the cryptopocalypse nigh?

I've been traveling a bit over the past couple of weeks, so I haven't had much of a chance to keep up on blogging. One consequence i...

My Blog List

Bristol Cryptography Blog
Practical secure logging ... (Esorics day one)
1 day ago

ellipticnews
Geocrypt 2013, Tahiti
1 day ago

Schneier on Security
Government Secrecy and the Generation Gap
1 day ago

Shtetl-Optimized
NSA: Possibly breaking US laws, but still bound by laws of computational complexity
2 days ago

The MPC Lounge
Workshop on Applied Multi-Party Computation (February 20-21, 2014, MSR Redmond)
1 month ago

root labs rdist
Keeping skills current in a changing world
4 months ago

Cryptanalysis



It saddens me a lot what the internet has become. Once a wonderful opportunity to communicate and create new businesses, connecting people. Now its a surveillance trap, bloggers get harassed for expressing their ideas and feelings and LAWYERS are hunting you.

Goodness

[Reply](#)



Anonymous [September 10, 2013 at 9:02 AM](#)

>>I guess the only solution for the IT industry is open hardware, open software, open standards for communication and encryption. Thanks to the NSA we have to restart basically from point zero. >>

True, Richard Stallman must be laughing at the fools and crooks who opposed him. The only solution is keeping everything, hardware software and every standards open.

Building trust will take a lot of time.

[Reply](#)



Anonymous [September 10, 2013 at 9:59 AM](#)

There are symptoms, and there are diseases. <http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying>

[Reply](#)



Anonymous [September 10, 2013 at 10:53 AM](#)

You are correct, you have gained a number of new readers because of current events and many thanks for your blog. To play wack-a-mole at both of your points at once, both the public policy and technical questions should be brought out entirely into the open for national discussion. In other words, I do not share your faith in the US Congress. There is an ongoing breakdown in trust between the US Federal Government and the American people. In the short term the NSA has done great damage to both the US Government and the American people. In the long term, what the NSA has done is a good thing. This will necessitate us(world community) to start over. All standards, software, and hardware should be open source. There can be no bugs with millions of eyeballs.

To the point: Constitutional republic forms of government and governmental secrecy cannot co-exist. This is almost axiomatic.

[Reply](#)



karl malbrain [September 10, 2013 at 12:17 PM](#)

I had never bothered to think about TLS MITM vulnerability in specific or even SSL much in general. My experience in cryptography has been mostly in implementing the SRP protocol for system access control and AES session key generation.

The NSA apparently has capability to attach MITM taps into TLS network connections almost anywhere by having both the private keys to the servers it wants to compromise and programmatic access to the routers to spoof their traffic sources.

I don't think there is going to be a general solution to the TLS MITM weakness. The NSA claims to exploit this weakness in cross-border international traffick which seems to me to be legal and lawful. The ability for a lesser adversary to compromise a single router and a single server with an MITM attack of their own is troubling enough to keep me thinking.

[Reply](#)



marchwinds [September 10, 2013 at 1:03 PM](#)

Indeed, I think these revelations have damaged the States' reputation as a provider of IT and as an IT innovator. I have to say I am disgusted by the NSA's actions, and have absolutely no trust anymore in any of the technologies I use to communicate online. The whole thing makes me think of that expression: "you're not paranoid; people really ARE out

SSL/TLS broken again – A weakness in the RC4 stream cipher
5 months ago

Chargen
Flint 1.1.0 Available
3 years ago

Subscribe

- Posts
- Comments

Followers

Join this site with Google Friend Connect

Members (98)



Already a member? [Sign in](#)

Blog Archive

- ▼ 2013 (17)
 - ▼ September (2)
 - [A note on the NSA, the future, and fixing mistakes...](#)
 - [On the NSA](#)
 - ▶ August (1)
 - ▶ July (1)
 - ▶ June (2)
 - ▶ May (2)
 - ▶ April (2)
 - ▶ March (2)
 - ▶ February (3)
 - ▶ January (2)
- ▶ 2012 (48)
- ▶ 2011 (39)

to get you." In light of the stories that have emerged in response to Snowden's disclosures, I have closed down my iCloud account and switched from Gmail to Hushmail. I also closed down my Facebook account and then created a new one that is entirely public and contains almost no personal info. As a Canadian, I am particularly perturbed by the fact that anyone outside US borders doesn't count - we can't compel the NSA to stop spying on us, the Rest of the World. Having said that, I am sure my own government is as bad as the NSA, so it might not matter!

[Reply](#)



Karl Malbrain September 10, 2013 at 3:23 PM

One solution to the TLS MITM vulnerability relies on the security of the client's private key. The client's public key is uploaded to the server during a registration process. TLS has a flavor of this called strong authentication, which uses certificates.

Users must create their own strong private key, and this can become a vulnerability with a weak generator that doesn't uniformly distribute keys across the universe of users.

[Reply](#)

[Replies](#)



Anonymous September 10, 2013 at 9:27 PM

If I'm not mistaken, this is the idea of using signed (by the service provider) public keys (your public key) for authentication? - the resulting certificate being generated during the first transaction/registration. This would then allow the provider to authenticate you and also let you challenge/authenticate the service provider themselves, then being able create a secure connection. (I may be mistaken on a few pts, looked at a corresponding credit card implementation some years back).

I remember thinking that this would be a solid idea for certain transactions such as with credit cards (you can append the certificate with the dollar amount, and sign it to build a certificate chain as it passes through different banks/financial institutions).

However, for daily online communications wouldn't this still rely on that initial transaction being secure? ie. you'd still have to acquire the service provider's key uncompromising which isn't feasible without a secondary way of authenticating any key you receive over the wire, at least for normal usage.

[Reply](#)



Dan September 10, 2013 at 3:35 PM

I have already emailed the D.N.I. expressing my loss of confidence in US cloud providers and will be migrating to a European or Asian service. We're just a small company, but given enough outraged small foreign companies moving away from US companies, it will negatively impact your economy.

I am not an engineer so I don't know how you can "fix" the technical problems. But it would have to be significant to earn back my confidence.

[Reply](#)



Anonymous September 10, 2013 at 3:53 PM

There is a need to educate those who seem disinterested and/or uninterested in the problems surrounding mass, suspicionless surveillance, in addition to the need to start fixing these problems.

As a European and software developer I am disheartened by a magnificent ignorance: I interact with plenty of people wanting to discuss confidential matters over gmail or skype and people who are quite willing to collect personal details from their customers (scanned passport images for example) and store them in US based cloud services.

Mr Snowden's concern that nothing would change seems particularly astute and it's right and proper that we're having the conversations prompted by such blog posts as Mr Green's.

So thank you.

[Reply](#)



karl malbrain September 10, 2013 at 4:25 PM

I agree that we need to address the political problem of the U.S. government that has acquired over the years unrestricted access to all of the hardware that makes up the internet. They have nearly unrestricted ability to generate MITM attachments to all TLS connections.

Perhaps a world-wide database hosted by each and every country that cares to participate of users' client certificates is needed. These database copies could be audited against one another to demonstrate consistency, and would obviate the need to register with servers one-by-one.

[Reply](#)

[Replies](#)



Anonymous September 10, 2013 at 8:52 PM

I'm not clear on what you're suggesting.

If we take trust in your own gov't as a given, there'd still be no way to avoid, "obviate", registering with gov't servers one by one. No gov't would trust the other, unless you're suggesting we maintain one list that each gov't individually audits for their citizens - a massive task only feasible for very large countries.

Either way, we're no better off.

[Reply](#)



Anonymous September 10, 2013 at 5:32 PM

They can begin "fixing" the situation by:

#1 impeaching Obama (Nixon quit over much less). Impeaching of Obama would send a very strong message to all future presidents that trying to recreate the surveillance state will be unacceptable. If Obama gets away with it, you can bet that maybe not the next one, but the next one after him will try again.

#2 firing Clapper, Alexander, and others involved at the top (Holder?), and possibly even putting them in prison over lying to Congress (we can't just have rogue agencies doing anything they want like that)

#3 overhauling the entire Intelligence Committee, perhaps with the exception of Wyden and Udall, who have been trying to warn us about all of this (but didn't use their immunity to actually tell us the truth).

#4 Reducing the NSA by say, I don't know - 90 percent? (clearly they have too much money to crack everyone's computers, tap all the cables, and launch hundreds of offensive actions, against who knows who). They should say thanks for not being shut down for good. Spy agencies like NSA, especially rogue ones, have no place in transparent and democratic societies.

#5 Repealing the Surveillance State (http://holt.house.gov/index.php?option=com_content&task=view&id=1200&Itemid=18). Clearly all of these laws have been passed with no real debate. Get rid of them, and start the debate from scratch.

#6 Forget about NIST. Form a new international body for security standards. Have no trust in anyone working with the government, or who worked in the recent past for the government

#7 Fight to get everyone on open source firmware. We can never trust hardware vendors

again until their firmware is open source, and we can audit it. This goes not just for American companies, but companies like Huawei and others who try to do business in US or EU, and so on. Open source firmware is going to be vital in the future, to establish trust

Let's call all of those the "starting steps" that are needed to recreate a trusting environment again in technology. Anything less will be a mockery, and will mean nothing has been solved, just swept under the rug, waiting to be exposed a few years later.

[Reply](#)



Brian [September 10, 2013 at 5:51 PM](#)

I think there's also an interesting opportunity for the US government and US companies here. While the stories (and their associated reactions) are obviously US focused, it seems reasonable to assume that there will be an increased overall interest in security issues. And because of the US-centric nature of the current discussion, the US government and US companies are in a unique position (and uniquely motivated) to focus on improving confidence and security in terms of technical, legal and policy solutions.

While non-US companies are likely to get some mileage out of "we're outside US jurisdiction", the smart person asks what's going on in the jurisdiction they ARE subject to. If you're moving your data away from US services to somewhere else because you're afraid of the NSA, I would imagine most people would want some sort of assurance that they're also protected from the local equivalent. And that's a lot harder assurance to provide.

[Reply](#)



Anonymous [September 10, 2013 at 8:16 PM](#)

I would like to be able to purchase a cheap laptop just for surfing the net via my Ethernet cable. It would use Tor automatically. It would only read content on the internet but there would be no capacity to download files or malicious software. It would have speakers but no mic or cam. It would have zero wireless function. The operating system would be set in stone and could not be updated/alterd in any way.

Is it possible to create such a device which has some basic functionality but is impossible to hack since no changes can be made to the device?

[Reply](#)

[Replies](#)



Anonymous [September 10, 2013 at 8:42 PM](#)

There are ways, however, by making it impossible to be altered/updated this also reasons that the moment an exploitable bug is discovered you're done. You have to throw it out and buy a new device that is updated. It's pretty clear that such an implementation quickly becomes a pain.



Anonymous [September 10, 2013 at 8:50 PM](#)

It could have a cheap removable cassette hard drive. I purchase the updated disc from the trusted hardware company and plug it in??????



Anonymous [September 10, 2013 at 10:00 PM](#)

We're not talking a small number of times, see: http://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26

Not to mention, these days gov'ts and others no doubt stockpile zero days just like any conventional weapon.

To return to your idea give an applied example: a lot of people (this blog incl., if I recall) suggest banking on a live cd which isn't a bad idea if you're using a Windows box (not getting into if Windows is less secure by design argument, just most commonly used) that is likely infected with ROUTINE keyloggers/spyware /whathaveyou. This will for the most part prevent logging of your banking

credentials because the majority of such programs a)won't spread to CDs, b)won't run on linux distros even if they do, c)won't remain beneath the OS, or d)even if you acquire CDs independently, very few target linux.

Live CDs, however, are not as useful if someone is actively snooping on your network (I'm looking at you SMBs) because, depending on when you get/make them & how often the devs update the .iso, the distro or software (webbrowser, etc) isn't updated and may be vulnerable to the pt. where it makes you no safer.

All this is besides the pt. really; no system is going to be completely immune to exploitation and all the additional trouble you'd be putting yourself through in your example wouldn't make you any safe.



Pattern_Juggled September 10, 2013 at 10:19 PM

We're in process of delivering such a device based on "smartphone" hardware with <http://cleanphone.is> - doing so is the least-bad way to protect against endpoint vulns.

Yes, this means the hardware itself becomes "obsolete" when new OS builds or versions are necessary. In practice, that means the hardware comes back to our company, we hard wipe all memory storage, and we reinstall the new rev - making it a completely "new" phone rather than any kind of conventional upgrade.

Nowadays hardware is cheap - very much so. It's not the bottleneck. That's not an excuse to throw hardware away carelessly, as there's still a sizeable environmental footprint created by the entire supply chain. But it does mean that the model of "sell folks hardware and then they upgrade that prized possession with software over time" really isn't applicable any longer. Now, it's "sell them the expertise in configuring software that's stable and secure - on whatever hardware is handy to do the job for the time being."

If one seeks to deliver actual end to end security confidence to nontechnical customers, the above is at present the only way to do so. Leaving a bunch of applications - not to mention the OS - with dangling hooks to accept updates, and expecting nontechnical customers to wade through which updates are genuine and so forth, is simply not feasible if one seeks an end configuration that's even vaguely TAO-hardened.

It's interesting, because we've been working on the "Cleanphone project" for nearly three years. Until several months ago, bringing up "endpoint hardening" was enough to make anyone's eyes glaze over - nobody wanted to hear that paranoid blather. Heck, back in 2008 via a predecessor company we tried building & delivering "security hardened" laptops via this model (operating as Baneki Privacy Technology, now evolved to Baneki Privacy Labs at <http://baneki.nu>). We sold only a handful - nobody wanted to have limits on what Windows gadgets they could grab from "free" download sites, basically. What people wanted was some program that made them "secure" (which of course was dependent on secure endpoints, which of course were and are quite scarce).

Hence was born the "consumer VPN industry" as our work evolved, in turn, into Cryptocloud VPN... which itself has been shut down to make way for the cryptostorm darknet.

And now, more than five years later and thanks to Snowden's courage and the NSA' perfidy, folks are much more aware of endpoint security - and asking security technologists to provide systems which can at least partially meet that challenge.

It's a new world, post-Snowden.



Anonymous September 11, 2013 at 1:23 AM

I really wish you the best of luck with your projects Pattern_Juggled! I'm just an average Jo, as you can gather from my post requesting a secure laptop but if I'm prepared to pay a few hundred dollars for hardware like that I'm sure millions of other will be coming online soon as the reality of the post-Snowden world sets it.

I will send another 'internet dummy' post soon about a suggestion I have for Big Father Dot Com security service website. I's love to hear what you have to say.

[Reply](#)



Anonymous September 11, 2013 at 1:47 AM

I'm an 'internet dummy' so please excuse me if this suggestion is not technically feasible. It occurs to me that us little endpoint users battling the NSA, China, Russia, Identity thieves etc. is like ants fighting elephants.

Could we all band together and send funds to Big Father dot Com providers. As an internet user I would send all my searches, via strong encryption, to a company whose sole purpose is to keep me and my searches and activity anonymous. They decode the encrypted request visit the website and send me back the info in encrypted form. If I have my secure laptop (see above)then 'she'll be right mate'?????

This same Big Father company could also let me know about various attacks with a detailed report which I may be able to use in court if necessary.

This would make a mess of Google Analytics as most IPs will be coming from Big Fathers (elephants) rather than private sites (ants).

If it is the sole purpose of Big Father websites to protect privacy then they will go bankrupt overnight if discovered to be infiltrated by the NSA or other groups.

[Reply](#)



berkus September 11, 2013 at 2:04 AM

We definitely start by reading some Cory Doctorow prose.

Let's say, "Human Readable" fits well here.

[Reply](#)

Comment as:

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)