## **Schneier on Security**

A blog covering security and security technology.

<u>« The Effect of Money on Trust | Main</u>

## September 5, 2013

## The NSA Is Breaking Most Encryption on the Internet

The new Snowden revelations are explosive. Basically, the NSA is able to decrypt most of the Internet. They're doing it primarily by cheating, not by mathematics.

It's joint reporting between the Guardian, the New York Times, and ProPublica.

I have been working with Glenn Greenwald on the Snowden documents, and I have seen a lot of them. These are my two essays on today's revelations.

Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted.

Tags: cryptography, encryption, intelligence, internet, NSA, privacy, Schneier news, secrecy, surveillance Posted on September 5, 2013 at 2:46 PM • 147 Comments

To receive these entries once a month by e-mail, sign up for the Crypto-Gram Newsletter.



## Comments

## Alex • September 5, 2013 2:59 PM

My biggest fear and complaint is that NO ONE in the US government seems to have any concern nor intention of stopping or severely limiting this.

No doubt that today's revelations violate HIPPA and probably many other laws, yet there's no one looking to hold anyone accountable.

All of this just further confirms my decisions to stay with as much open-source software for our office, maintain everything in-house, and work with internet providers and carriers who are a bit on the hippie/libertarian side of things. Does this make me immune? No, but it certainly makes it us a much more difficult target when not using the standard stuff.

Also, has anyone looked into the CIA's quasi-private organization, In-Q-Tel? They work with a company called CallMiner which handles hundreds of thousands of phone calls a day. Probably something going on there too.

#### james • September 5, 2013 3:03 PM

Cheating indeed. Backdoors. Stallman will have such a smug face today.

# Doug Coulter • September 5, 2013 3:07 PM

Great essays, Bruce. Hope enough people listen.

# Daniel • September 5, 2013 3:07 PM

Now it becomes clearer why Obama has gained such a sudden interest in Syria. Anything to control the narrative and deflect attention from the vital issues.

Give the man credit. No, he wasn't going to make a stink about a "hacker" but he's going to do everything in his power to makes sure that what the hacker reveals is promptly buried.

So basically, the U.S. decided it didn't need no stinkin' trust in its corporations, governments, systems, and standards.

They really should have consulted with our host before destroying all the credibility of all U.S.-related entities.

## Hanno • September 5, 2013 3:15 PM

On the crypto bits in your guardian piece, I found especially interesting that you suggest classic discrete log crypto over ecc.

I want to ask if you could elaborate more on that. Because other respectable cryptographers recommend the opposite: <a href="http://blog.cryptographyengineering.com/2013/08/...">http://blog.cryptographyengineering.com/2013/08/...</a>

Also, how does RSA play in this? With RSA vs. DSA vs. ECDSA, I'd still say RSA with long keys is the safest bet. How do you consider ecc with non-nsa-influenced curves? What about Curve25519? (I don't think DJB is secretly an NSA-spy)

What I found especially troubling to hear about DSA is that it's unsafe as soon as you have a single signature made with a broken RNG. Though I don't know what other dlp/ecdlp-based algos suffer from that.

# Pete • September 5, 2013 3:17 PM

Loved your call to action in The Guardian today. Thank you! http://www.theguardian.com/commentisfree/2013/...

## Jack • September 5, 2013 3:23 PM

Bruce,

You are writing about openness in your essays. You are writing about monitoring government and NSA activities. You are asking for people to tell their stories to you.

Why then do you and others take such care to not really be open and share all of the Snowden documents?

## Richard • September 5, 2013 3:29 PM

Hey Bruce,

Please expand on the undocumented command line option in Password safe.

Security by obscurity doesn't work.

#### Felix • September 5, 2013 3:30 PM

From the Guardian report:

"It shows the agency worked covertly to get its own version of a draft security standard issued by the US National Institute of Standards and Technology approved for worldwide use in 2006."

Which standard is that?

#### charlie • September 5, 2013 3:36 PM

We need a truth and reconciliation commission.

Any guilty of these loses their security clearance. Forever.

#### Tom • September 5, 2013 3:38 PM

Please, whenever you have time/opportunity, tell us more about the 'why' of these comments:

"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."

Thank you...a luta continua!! May the Force be with you!!

You know, we mathematicians go to ALL THIS WORK coming with all these FANTASTIC structures that are all theoretically UNBREAKABLE.

And what happens? YOU HUMANS SCREW IT ALL UP! STOP MAKING BABY MATH JESUS CRY!

## Mike • September 5, 2013 3:40 PM

Someone owning the internet is inevitable. People should be happy that its the good guys and not the Russians or the Chinese. Does everyone here really want Iran, China, Russia, Syria, etc to be able to do their business without the intelligence community being able to keep tabs on it?

This sort of pwnage is why people should be proud to be American and they should be irate that Snowdon is giving a huge leg up to our geopolitical adversaries. Hey, if you want to stop using American products go right ahead. All technology should be considered to have little goodies from its host government hiding inside of it. Anarchists who think that we can enter some sort of stateless utopia through radical transparency are delusional.

# William A. Hamilton • September 5, 2013 3:41 PM

I just read today's Snowden-based articles in the New York Times and the Guardian on NSA actions to SIGINT-enable target communications. What the NSA and the CIA did with copies of the PROMIS database software, beginning in 1981, provided a robust learning experience for NSA for what it appears to have been been doing more recently, according to the latest NSA documents furnished by Edward Snowden.

A CIA contractor, GE Aerospace, allegedly operated a PROMIS packaging facility in Herndon, Virginia, beginning in the early 1980s, to install unauthorized, copyright-infringing copies of INSLAW, Inc.'s PROMIS database software on computers into which the government had covertly inserted a replacement integrated circuit, before shipping the turnkey systems to buyers overseas.

An NSA integrated circuit manufacturing facility in the Silicon Valley allegedly produced the "Petrie Chip" which the CIA contractor covertly inserted into the computers equipped with the PROMIS software.

These turnkey systems were allegedly sold to foreign intelligence and law enforcement agencies and banks through cutout companies.

The Petrie Chip allegedly replaced an identical-looking integrated circuit and consumed an identical amount of power, making it virtually impossible to discover its presence in the computer.

The Petrie Chip allegedly automatically copied data tracked in the PROMIS system and periodically transmited the data to a local NSA listening device, defeating any Tempest Shield-type protections.

The CIA allegedly continued to use this contractor-operated PROMIS packaging facility after GE Aerospace was acquired by Martin Marietta and Martin Marietta morphed into Lockheed Martin.

The CIA's Division D, comprising both CIA clandestine services officers and NSA engineers, allegedly managed this PROMIS/Petrie Chip operation until the creation of the successor Special Collection Service, which thereafter assumed the responsibility.

The government euphemistically referred to NSA's Petrie Chip as its "special data retrieval capability" for PROMIS systems designed to steal intelligence secrets.

NSA sold PROMIS through cutouts to banking sector entities to enable real-time electronic surveillance of wire transfers of money and letters of credit, and to foreign law enforcement and intelligence agencies to facilitate computer thefts of their intelligence secrets. In addition, the CIA deployed unauthorized, copyright-infringing copies of PROMIS to virtually every component of the U.S. intelligence community as the standard database software for the gathering and dissemination of U.S. intelligence information.

Neither NSA nor any of the other agencies of the U.S. intelligence community has ever paid copyright-infringement compensation to INSLAW despite two federal court rulings about the government's theft of PROMIS "through trickery, fraud, and deceit," and two Congressional investigations.

William A. Hamilton President INSLAW, Inc.

#### Felix • September 5, 2013 3:42 PM

In "How to remain secure against NSA surveillance" you suggest a number of methods you have taken to protect your machine used for reviewing classified documents.

How about removing the wifi card and physically disabling the microphone and webcam?

As well as putting a screen filter on to reduce the angle of view, I suppose.

## **G** • <u>September 5, 2013 3:44 PM</u>

#### The first question to ask: is the IETF compromised?

## http://irtf.org/cfrg

#### QnJ1Y2U • September 5, 2013 3:47 PM

From one of the Guardian articles linked above:

Since I started working with the Snowden documents, I bought a new computer that has never been connected to the internet.

Coming next: NSA compromises all brand new computers. (What's scary is that this no longer sounds crazy).

#### S • September 5, 2013 3:48 PM

There's a "Snoden" typo in your summary.

#### Martin • September 5, 2013 3:52 PM

This only works IF you can guarantee that 100% of the government employees and individuals entrusted with these tasks are 100% trustworthy, 100% infallible and 100% non-subvertable.

Certainly the common assumption in the US is there is always someone you know who seems to know someone who knows someone with enough clearance in a government agency that can get you the "inside" skinny on any individual. No matter how careful an agency can be there will always be another individual, at some time in the future who enables inappropriate access to the stuff we are asked to "trust" the government to protect.

Pretty sure you could substitute any other country's government and state the same. So until then we should NEVER allow them the keys to our digital house especially when it's our tax dollars paying for them to copy the keys!!

## Felix • September 5, 2013 3:54 PM

@Mike,

unfortunately the US can no longer be classed as 'the good guys' even by normal non-conspiracy theorists.

You can argue that you are not as bad as the others governments, but what with the government torture programs, total surveillance, the utter dismissal of constitutional rights in the name of national security, and a political system totally owned by the 1% and the military industrial complex, your days of being the good guys are well and truly over.

#### Thomas • September 5, 2013 3:58 PM

"People should be happy that its the good guys and not the Russians or the Chinese."

Good guys? NSA? Serious perspective error or what? Patriotic blindness?

As far as we know, US has started more wars in last 30 years than Russians or Chinese put together and you call them "good guys"?

We call them war-mongering idiots, definitely not "good guys".

Definitely not any better than Chinese or Russians, but much worse: Obama is already starting a war just to hide this NSA-scandal and UK is following.

Nice job.

Also NSA is directly attacking your own constitution, i.e. are criminals at very high level and you are missing that too: How a professional criminal can be a "good guy"?

You have wrong role models, pal.

"This sort of pwnage is why people should be proud to be American"

Just like the Nazis were proud for their efficiency in handling the "jew issue". We do know that many were. Just like you are now.

@Mike. I think you are trolling but I'll take your comment seriously.

A key problem with the "someone has to own the internet" logic is that no one can. You say the good guys own it and Snowden is a traitor but what about all the Chinese and Russian spies in the NSA? There is a long list of traitors in the security business. The problem is that when the NSA installs a backdoor for itself it installs one for everyone else too who can get access to that backdoor. So the idea that the NSA is "on my side" is bogus. They are only one my side so long as they can keep a secret and there is plenty of evidence they can't do that. Once that secret is out I now have a backdoor in my computer than anyone can get to, friend and foe, and the NSA isn't going to to squat for me.

So the idea that the NSA represents the "good guys" is very short sighted. The NSA is the good guys right up until the NSA's own ineptitude betrays me to the Russians and Chinese.

Nobody Special • September 5, 2013 4:01 PM

@Thomas - I think that was irony (it's always so difficult to tell with Americans)

Andy • September 5, 2013 4:04 PM

The second essay makes me fear Bruce might have an accident soon.

Lots of people assumed the NSA has a lollypop.

Snowden went half a globe away to be protected when he came forward and proved the NSA actually had a lollypop much larger than assumed. Now openly calling for engineers and coders to start taking that sucker away from the NSA...

I admire your courage.

#### Jan • September 5, 2013 4:07 PM

I would be really interested to know if RSA or DSA are preferable where there is a choice. RSA is most likely a more interesting target, on the other hand, DSA fails horribly if you ever use a key on a system with a broken PRNG. Since PRNGs are obviously a prime target for subverison, my gut feeling would be not to touch DSA with a 10-foot pole.

Also, please spill the beans. Yes, it will suck for the US, but the US isn't the only country in the world, and is it really a good thing to protect their interests and thus help them violate the rights of everyone else, including their own citizens?

#### Bruce Schneier • September 5, 2013 4:07 PM

"On the crypto bits in your guardian piece, I found especially interesting that you suggest classic discrete log crypto over ecc. I want to ask if you could elaborate more on that."

I no longer trust the constants. I believe the NSA has manipulated them through their relationships with industry.

## Bruce Schneier • September 5, 2013 4:09 PM

"Why then do you and others take such care to not really be open and share all of the Snowden documents?"

I believe the Guardian and Greenwald have both written about this.

It's not my show; I am not in charge of what gets released.

#### Bruce Schneier • September 5, 2013 4:10 PM

"Please expand on the undocumented command line option in Password safe. Security by obscurity doesn't work."

I added it in an early version.

There's no obscurity. It's Blowfish -- you can verify the implementation with any other implementation.

"From the Guardian report: 'It shows the agency worked covertly to get its own version of a draft security standard issued by the US National Institute of Standards and Technology approved for worldwide use in 2006.' Which standard is that?"

I don't know. DUAL\_EC\_DRBG, perhaps?

https://www.schneier.com/essay-198.html

# Bruce Schneier • September 5, 2013 4:18 PM

"I would be really interested to know if RSA or DSA are preferable where there is a choice. RSA is most likely a more interesting target, on the other hand, DSA fails horribly if you ever use a key on a system with a broken PRNG. Since PRNGs are obviously a prime target for subverison, my gut feeling would be not to touch DSA with a 10-foot pole."

In general, I don't think there is a difference. Cryptanalytic advances against one transfer to the other.

## How Far • September 5, 2013 4:22 PM

Could the NSA be intercepting downloads of open-source encryption software and silently replacing these with their own versions? Is there any way to detect such interference had the NSA enough control over communications channels to automatically replace binaries and published hash lists?

## Mike • September 5, 2013 4:23 PM

Excellent article Bruce. Was wondering about Linux tough. Some people reporting that the NSA added its own set of security features to Linux SE in 2003. Many top Linux users say it has been reviewed many times with no findings of system compromise; but with recent events, some saying it needs another look. Keep up the good work sir!

## jay c • September 5, 2013 4:29 PM

"My biggest fear and complaint is that NO ONE in the US government seems to have any concern nor intention of stopping or severely limiting this."

Mostly true, but not entirely. Ted Cruz and Rand Paul appear to want to stop it.

## USB? Really? • September 5, 2013 4:30 PM

From your article:

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.

You should know as well as anybody else -- USB 0days are a dime a dozen; USB drivers and their userland stacks are all terrible, filesystem drivers are worse, and so on. It doesn't take that much development effort to own your internet facing computer, load particular code onto your USB stick, and then when you plug it into your airgapped machine, own that, and so forth.

Please use caution. I think you're better off just using a serial cable and moving data fairly slowly in a very primitive way.

#### SteveB • <u>September 5, 2013 4:33 PM</u>

Just thinking about NSA inserting backdoors...

What's the likelihood that an open-source security product (perhaps something like SELinux, which NSA contributed much of the code for...) contains vulnerabilities that are subtle enough to withstand non-expert scrutiny?

## Bruce Schneier • September 5, 2013 4:35 PM

"Could the NSA be intercepting downloads of open-source encryption software and silently replacing these with their own versions?"

Yes, I believe so.

# Bruce Schneier • September 5, 2013 4:37 PM

"What's the likelihood that an open-source security product (perhaps something like SELinux, which NSA contributed much of the code for...) contains vulnerabilities that are subtle enough to withstand non-expert scrutiny?"

Less likely than a closed source product.

All we're doing here is playing the odds.

## Brad Hicks (@jbradhicks) • September 5, 2013 4:38 PM

I worked in computer security for 14 years, Mr. Schneier, and I want you to know something, even if it only matters to me that you know it:

You are the man I wish I had become, the man who has found a way to make it his job to be right about security. My fondest wish is that I could have found a way to get your job; my deepest hope is that, if I had gotten it, I could have done it as well as you have.

You are a hero.

## Tin foil hat • September 5, 2013 4:40 PM

I am now even more convinced than before that we should start using one-time pads when it is feasible. And more important messages should be encrypted with the OTP encryption done outside PC -- manually or using some simple microcontroller based solution. You shouldn't use the PC keyboard for input or use PC to display those messages, because it is far too easy to install remotely a backdoor to PC which is connected to Internet.

And if you are very afraid of possible biased random numbers when creating the OTP, you can always cascade encrypt that data with some more common methods.

If you aren't able to use OTP, maybe we should start using cascade encryption with unrelated keys and encryption algorithms and demanding signing with more than one method and key. Traditionally this has been objected, but I think that the NSA leaks give a good reason to change that tradition.

#### Bruce Schneier • September 5, 2013 4:43 PM

"I am now even more convinced than before that we should start using one-time pads when it is feasible."

No.

Don't break what isn't broken.

#### Mike • September 5, 2013 4:47 PM

@Thomas Oh that Obama, be careful cause I bet he's itching to take your gun away.

The fact that the tin foil hat crowd seems to be the only one up in arms here makes me fetter better about the public's ability to perceive risk.

The Big Bad Government already pays for your healthcare, processes all of your private tax information and can do all sorts of other nasty things but guess what 99.999...% of the time it does its fucking job.

China and Russia make no bones about emptying your bank account and stealing your intellectual property. Come on, take a lesson from Bruce and see who is actually going to screw you over rather than believe some fantasy story that validates your world view.

In one of the Guardian articles you said: "Since I started working with Snowden's documents, I have been using GPG, Silent Circle, Tails, OTR, TrueCrypt, BleachBit, and a few other things I'm not going to write about."

Why are you not going to write about those "other few things"? Can you write about the here please?

Thanks.

#### anonymouser • September 5, 2013 4:50 PM

ahh... but what exactly is not broken? how far can we trust the maths? I never believed in the magic numbers of ecc, I still don't understand how come the exponent 3(three) is acceptable for RSA... there are many things which seem amiss.

## bf skinner • September 5, 2013 4:51 PM

@Jack "Why then do you and others take such care to not really be open and share all of the Snowden documents?"

In addition to what Bruce writes above - Snowden and Greenwald have said repeatedly they are making narrow disclosures so as to not possibly jeopardize anyone.

In addition...did you notice anything particular about the Bradley dump on Wikileaks? The way there was SO much that public analysis choked and it went away as an issue. The story went away.

I'm not saying the public needs to be spoon fed but the stories are just that stories and the larger public needs things to be explained, correlated and put into context so that the larger public can understand 'what the big freaking deal is'

# Concerned about ECDSA • September 5, 2013 4:52 PM

You encourage us to prefer older discrete log systems over elliptic curve systems. I know about the dual ec prng vulnerability. But what about P-521 and that family of NIST curves? Are these magic numbers a legitimate cause of concern?

#### Bruce Schneier • September 5, 2013 4:58 PM

"Why are you not going to write about those 'other few things'? Can you write about the here please?

I want to keep some secrets in my back pocket.

#### Jeff • September 5, 2013 4:58 PM

#### @Bruce

Great essays and I really respect your stand on this.

Are you still working for BT and do you have anything to say about their involvement in these abuses?

#### Bruce Schneier • September 5, 2013 4:59 PM

"You encourage us to prefer older discrete log systems over elliptic curve systems. I know about the dual ec prng vulnerability. But what about P-521 and that family of NIST curves? Are these magic numbers a legitimate cause of concern?"

I personally am concerned about any constant whose origins I don't personally trust.

## Bruce Schneier • September 5, 2013 5:00 PM

"Are you still working for BT and do you have anything to say about their involvement in these abuses?"

Yes. And because of the first answer, no.

It's okay; lots of other people are talking about BT's involvement. I don't have anything to add.

## Bruce Schneier • September 5, 2013 5:03 PM

"ahh... but what exactly is not broken? how far can we trust the maths?"

I don't know. This is what I think:

https://www.schneier.com/essay-446.html

Peter • September 5, 2013 5:04 PM

I would've disabled HTTPS on schneier.com for the day after posting this. >)

#### Stephen • September 5, 2013 5:05 PM

There was once an age where we feared the Soviets and the Orwellian police state they represented.

50 years later, we became it.

Nietzsche would be proud.

## anonymouser • September 5, 2013 5:09 PM

thanks for the reply. since we're on the topic of trust, do you trust PBDKF2?

#### Sandy Harris • September 5, 2013 5:10 PM

Over a decade ago I worked on a project whose main goal was preventing massive surveillance: <a href="http://www.freeswan.org/freeswan\_trees/...">http://www.freeswan.org/freeswan\_trees/...</a>

A more detailed rationale is here: http://www.freeswan.org/freeswan\_trees/...

& a description of technology we developed is here: <u>http://en.citizendium.org/wiki/...</u>

Our project failed; we never got wide enough adoption to have it take off. Should it, or at least the basic notion, be resurrected?

#### Argon • September 5, 2013 5:24 PM

There is a mention in NYT article about backdoors in hardware - do you know if they are firmware/microcode key backdoors, or are they actually backdoors embedded in the silicon?

## gonzo • September 5, 2013 5:28 PM

Hi Bruce,

I see you're still comfortable working with Truecrypt. Is it too much to ask if you're using the pre-compiled executable available for download, or only if your comfort level attaches only to a version you've compiled yourself?

## Mike Doherty • September 5, 2013 5:36 PM

You recommended to "Prefer symmetric cryptography over public-key cryptography." Can you elaborate on why?

#### Jose • September 5, 2013 5:37 PM

Winrar and 7zip are already compromised, the owners dont give the hashing of originals installers... OTP encryption is flashing, back to the stone age again hell....

There are, as there always have been, three points of attack:

Key Management Implementation Sources of Random

The algorithms we have, overall, are good. Those three areas however though pay huge rewards. I was a student at a NSA Center of Excellence and had (one of) the "best education money can't buy"

My personal favorite to attack during the time I was involved and studying: sources of random. Let's just say there is a surprising amount of implementations that can be defeated with large enough database lookup tables.

I sleep better now that I am no longer involved though. I saw what my work turned into and decided I wanted no part of it, left before I got in too deep to get out.

#### Ninho • September 5, 2013 5:45 PM

Mr Schneier, congrats and respect !

Guys, remember the 'NSAKEY' apparent in, was it, windows 95 binaries ? At the time many people assumed it had nothing to do with the NSA, the funny naming being rather some sort of an unimaginative programmer's idea of a joke.

In retrospect, knowing what we learnt today, that may have been the actual key to an NSA sanctionned backdoor.

Unless it were just a decoy used to hide the /real. NSA backdoor from view :=)

#### cody • September 5, 2013 5:48 PM

"On the crypto bits in your guardian piece, I found especially interesting that you suggest classic discrete log crypto over ecc." ... I no longer trust the constants. I believe the NSA has manipulated them through their relationships with industry.

In essay-198 you wrote "It's possible to implement Dual\_EC\_DRBG in such a way as to protect it against this backdoor, by generating new constants with another secure random-number generator and then publishing the seed. This method is even in the NIST document, in Appendix A."

If we're using constants that can be verified with such a technique, is there still a reason to avoid ECDSA?

I'm also wondering whether curve25519 is safe, given that the Tor project is planning to use it.

#### name.withheld.for.obvious.reasons • September 5, 2013 5:49 PM

@ GhostIn(Your)Machine

I would add a time base/reference.

## Steve • September 5, 2013 5:57 PM

@b f skinner: "In addition to what Bruce writes above - Snowden and Greenwald have said repeatedly they are making narrow disclosures so as to not possibly jeopardize anyone."

Or the forthcoming book deal.

Greenwald is a self-aggrandizing little toad who mishandled his source.

Just sayin'.

# Clive Robinson • September 5, 2013 5:57 PM

@ Bruce,

I want to keep some secrets in my back pocket

Welcome to my world ;-)

What realy suprises me is peoples apparent shock to this news, all of it has been discussed befor on this blog by the likes of Nick P, RobertT, one or two others and myself for some years now.

For quite a while I've said the NSA's priority list was,

- 1, Known plaintext in common file formats (MS office etc)
- 2, Getting weaknesses into protocols.
- 3, Getting weaknesses into standards.

I've pointed out "end runs" around security via device shims etc publicaly since the late 1990's

I've also developed "backdoors" in crypto software and provided some details to this blog.

I even give details about research by Adam Young and Moti Yung about Cryptovirology and kleptography and given details of how to use it to make PK certs that reveal one of the PQ primes.

I've also pointed out the advantages of "oportunistic harvesting" -v- targeted attacks in the way such agencies work due to it being a lot more efficient.

I've also repeatedly pointed out the dangers of random number generators with to little entropy in software apps and embeded systems (such as routers and switches).

I've also repeatedly warned of "magic pixie dust" issues with hardware RNGs in the likes of Intel's chips.

I've also warned of other attacks such as "protocol fallback" which we know have and probably still are used by the likes of the NSA and GCHQ (oddly not mentioned in the articles).

So most regular readers should be totaly unsuprised by these revelations.

But as they say "You can lead a horse to water...".

#### cody • September 5, 2013 5:58 PM

DSA fails horribly if you ever use a key on a system with a broken PRNG

It's evidently possible to avoid that (see the linked OpenSSL patch too).

#### Bryan • September 5, 2013 6:06 PM

It seems to me that, by the NSA shoe-horning in back doors to all communications hardware, that it has provided its adversaries with the same capabilities.

Israel, China, Russia all have competent mathematicians that know how to cryptanalyze components and PRNGs. For the hardware pieces that look identical and use the same power, they can be reverse-engineered and/or sliced apart and microscopically analyzed.

It's not that the USG/NSA can decrypt all; if the NSA can, then all of these govts can.

Does the USG/NSA not care that they've provided these capabilities to potential adversaries? Is it really thought that the recently publicized USG cyberwarfare initiative can protect us?

Pogo was right: "We have met the enemy and he is us."

#### George • September 5, 2013 6:11 PM

" I feel I can provide some advice for keeping secure against such an adversary."

That's the most telling (and horrifying) sentence in the Guardian article. Something is seriously wrong if we have to regard an agency of our own government-- an agency that supposedly exists to protect our Homeland from dangerous enemy threats-- as an "adversary."

#### Tin foil hat • September 5, 2013 6:22 PM

"No. Don't break what isn't broken."

Why put all the eggs in the same basket and make the secrets vulnerable if NSA manages to find a method to break the symmetric encryption (or public key encryption) you are using? Using OTP with other encryption methods probably won't make the security any worse, especially when there is reason to suspect that some of those other encryption methods might be broken. Wouldn't it be preferable that there would be still some security left even if some encryption method is later found to be weak?

@Steve "just saying"

What that someone's going to write a book? Well that IS how we pass information from one of us to the next right? A formal, researched presentation of masses of data IN CONTEXT It's not like tweets and blogs provide much in the way of knowledge let alone wisdom.

Have you read the Pentagon Papers? No? Few have. The only people who read it were MacNamara, probably, (may he burn) and Ellsberg and his insider circle of DoD analysts.

Why did it become such a hugh issue? Because Nixon, (who never read it ) and Kissinger, (who never read it) moved heaven, earth, prior restraint, and attempted murder tried to keep anyone from reading it. All they and everyone else ultimately learned was that it was proof the war was unwinnable and had been for years. But had they ignored it...would've dropped off the radar soon enough.

## Another commenter • September 5, 2013 6:35 PM

Bruce, Given your opinion on what happened to ecc constants, could it be that the "new capabilities" against Google which apparently came on stream in 2012 were as a result of their adoption of ECDHE - which may well have been Google's attempt (via forward secrecy) to thwart the NSA?

## Lorenzo • September 5, 2013 6:48 PM

I'm interested to speculate on what forces can actually **balance** the NSA's power over the entire Internet. I am talking about actual economics, not just people's boycotting facebook for a month or two. What if US-based corporations were to show a dent in their profit due to a dip in public trust? Imagine if Google saw their users decline - would they be powerful enough to **lobby** Congress to curb the NSA? What if Facebook, Google, Yahoo joined forces for that?

It's all a game of balancing forces; in the current cloud-frenzy situation, it was inevitable for the NSA to be on top of it and take advantage of the situation. I wonder what's next - todays' story is probably a few years old. I am worried about mobile telephony (who cares about breaking 4g when you can pwn Android AND iOS?), the fabled Internet of things, RFIDs, etc.

Furthermore, today's documents show how there's no silver bullet to breaking security, especially on large deployment: it's a combination of slow-moving tactics (e.g. infiltrating telecoms), political pressure (on standard bodies), commercial pressure (cash to tech giants), lawful pressure (security letters), luck (the 0day), and who knows what else. As such, there's no silver bullet to counter-fight this: we (as tech-savy people with freedom in mind) must be ready to counteract the political pressure, the economical pressures, the technological advantages, etc.

Lastly, I bet some sort of *quantum computing* has been deployed successfully in 2010; and that actually gave access to the loads of encrypted data that have been collected over the years. We shall see in 15-20 years how things actually went, but I have a strong feeling about this.

ps: where do I sign in on your call for geeks to bring back the Internet to what it works best, e.g. a free and openly interconnected system? I'm interested :)

## anon • September 5, 2013 6:51 PM

@Bruce: I think one of the more surprising revelations in one of your articles today is that you still use Windows for most things. Seriously?!? How and why?

## Solstate • September 5, 2013 6:59 PM

What the NSA and the US Government don't seem to get is that whatever hacking information they assemble WILL eventually leak out to the wider hacker community and the script kiddies. The NSA is using US taxpayer funds to permanently reduce the effectiveness of the Internet.

Some of these vulnerabilities will be discovered sooner or later anyway, but it is quite possible that many of them, especially the ones engineered by NSA coercing business into adding backdoors, would not have been made possible without the immense wealth of the US taxpayer to fund it.

## Tango • September 5, 2013 7:06 PM

TrueCrypt is an NSA program. You offer a free program that works on almost all personal computers. Millions download and use it. When your agents or assets get caught with TC on their laptop, it doesn't mean they are working intelligence. Everyone uses TC. But is it secure, or is there an NSA backdoor in the program?

I've been wanting to write this for a few weeks now, and feel it ever so much more today:

I'm deeply grateful for the strong public light you have shed on threats to privacy and liberty -- those inseparable companions! -- ever since I started following your blog not long after the 2001 terrorist attacks, but most acutely since the "Snowden affair" broke.

I observe that your perspective on true security is not that of those "doctrinaire libertarians" who deny the legitimacy of almost all government power. Rather, the valuable and necessary exercise of that power *must be rigorously monitored and constrained*.

My distress about the cancerous growth of the "national security state" has grown near to agony in recent months: not only the naked contempt for the United States Constitution displayed from the Oval Office down to the lowest functionaries in such agencies as NSA, but also the slavish acquiesence of the dozens of elected lickspittles on Capitol Hill (and others in high echelons of government) who not only knew about and enabled this criminality, but still continue to defend their cowardice without hint of shame or remorse.

By birth, I received the unmerited honor of descent from men who faced grave danger to life and limb ... ineffable horror ... and in one case the spilling of his last drops of lifeblood ... on battlefields where the fundamental values underlying the American idea were at issue.

Today, my grief and discouragement about my once courageous country are greater even than during the tragedy of US military involvement in Viet Nam.

"Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety." These United States now permit our liberty to bleed out, casting off dignity and honor in the face of the terrorist bogeyman. Having done so, we shall neither deserve liberty and safety, nor can we expect them.

Bruce, your work in resisting the flood tide of cowardly surrender to fear is of immeasurable value, especially now that the public voices of resistance are so few. Your patient, persistent, ever calm and reasoned arguments counter to the mainstream have been a great comfort to me in a time of near despair -- extending to your generous expenditure of time responding to this comment thread.

As you carry on, please know that have the gratitude and best wishes of many!

## nano • September 5, 2013 7:25 PM

anon • September 5, 2013 6:51 PM

@Bruce: I think one of the more surprising revelations in one of your articles today is that you still use Windows for most things.
Seriously?!?
How and why?

I would think they are all compromised. Name one that you think is not.

#### Bruce Schneier • September 5, 2013 7:26 PM

"thanks for the reply. since we're on the topic of trust, do you trust PBDKF2?"

I don't know it.

## Bruce Schneier • September 5, 2013 7:28 PM

"There is a mention in NYT article about backdoors in hardware - do you know if they are firmware/microcode key backdoors, or are they actually backdoors embedded in the silicon?"

I don't know.

I assume the NSA aims for robustness, and does everything it can.

# James • September 5, 2013 7:29 PM

@Tango

Department of Justice FAQ on Encryption Policy April 24, 1998

Still accessible here:

http://web.archive.org/web/20091120073126/http://...

## Excerpt:

"5. Why does law enforcement oppose the use of encryption? Don't you realize that it will make your job easier by stopping crime?

We do not oppose the use of encryption -- just the opposite, because strong encryption can be an extraordinary tool to prevent crime. We believe that the use of strong cryptography is critical to the development of the "Global Information Infrastructure," or the GII. We agree that communications and data must be protected -- both in transit and in storage -- if the GII is to be used for personal communications, financial transactions, medical care, the development of new intellectual property, and other applications.

The widespread use of unrecoverable encryption by criminals, however, poses a serious risk to public safety. Encryption may be used by terrorist groups, drug cartels, foreign intelligence agents, and other criminals to secure their data and communications, thus nullifying the effectiveness of search warrants and wiretap orders.

# The Department's goal -- and the Administration's policy -- is to promote the development and use of strong encryption that enhances the privacy of communications and stored data while also preserving law enforcement's current ability to gain access to evidence as part of a legally authorized search or surveillance.

At bottom, it is important to recognize that society has an important choice to make. On the one hand, it can promote the use of unrecoverable encryption, and give a powerful tool to the most dangerous elements of our global society. On the other hand, it can promote the use of recoverable encryption and other techniques, achieve all of the benefits, and help protect society from these criminals. Faced with this choice, there is only one responsible solution."

(Other parts of this extensive document are also very interesting, especially in light of the new debate about encryption and snooping).

## old nsa from crypto • September 5, 2013 7:30 PM

http://web.archive.org/web/http://...

## Nick P • September 5, 2013 7:30 PM

### My reactions to guardian article

"The NSA spends \$250m a year on a program which, among other goals, works with technology companies to "covertly influence" their product designs."

This was to be assumed ever since Crypto AG, Lotus and the fact that subversion is the best method (more on that later). This kind of thing is why lve griped about the fact that there are only six fabs for top mobile chip sets. Just six organizations to subvert with a portion of a \$250m/yr budget. I wish my job was that easy. ;)

"A GCHQ team has been working to develop ways into encrypted traffic on the "big four" service providers, named as Hotmail, Google, Yahoo and Facebook."

At first I was surprised because I thought those were already compromised. The key point might be \*GCHQ\*, rather than NSA, is still trying to crack them. Or something else.

"Among other things, the program is designed to "insert vulnerabilities into commercial encryption systems". These would be known to the NSA, but to no one else, including ordinary customers, who are tellingly referred to in the document as "adversaries"."

If they don't know everything, you're an "adversary." Ha!

Many times on this blog in the past I pushed for designs at EAL5-7 level with review by mutually distrusting parties for subversion resistance. The reason is that subverting the producer of software means you can't trust them, and therefore the software. It's the most powerful attack as it can bootstrap others.

Even OSS isn't totally safe as games have been hidden in the likes of OpenOffice without people's knowledge and NSA's M.O. is ideal: insert subtle vulnerabilities that look like bugs. FOSS programmers are often volunteers without all the domain expertise we would like who at least put the time and effort into giving us the features. This can be true for security features too. Whose going to ban or accuse a hardworking FOSS developer because they picked a bad exponent? I mean, "seriously, who even knows about all that stuff?" ;)

"The document reveals that the agency has capabilities against widely used online protocols, such as HTTPS, voice-over-IP and Secure Sockets Layer (SSL), used to protect online shopping and banking."

Their implementations have had plenty of issues and the protocols often allow weak choices during negotiation phase. Both could be what the quote refers to. Of course, going back to subversion, they could get companies to build vulnerable knockoffs of SSL or insert taps on the side with the server or SSL offload engines. Or just offer businesses cheap SSL engines that also leak the keys. An old idea I came up with that lead me to stop using them.

" Documents show that Edgehill's initial aim was to decode the encrypted traffic certified by three major (unnamed) internet companies and 30 types of Virtual Private Network (VPN) – used by businesses to provide secure remote access to their systems. By 2015, GCHQ hoped to have

cracked the codes used by 15 major internet companies, and 300 VPNs."

This is entirely unsurprising. Others and I into high robustness security have consistently pointed out that most VPN's and OS's max out at Common Criteria EAL4, with many below that. I'm less concerned about the certification than the development process that implies: EAL4 certifiably produces shit. It (mostly) corresponds to C2 in Orange Book days and even then you had to go up two levels before a system was self-protecting enough. Those levels correspond to EAL5-7 with some extra, critical features. There \*are\* VPN's and network protections developed like that but hardly anyone uses them and a few are hard to obtain.

"This GCHQ team was, according to an internal document, "responsible for identifying, recruiting and running covert agents in the global telecommunications industry.""

THERE IT IS! I've been waiting for confirmation. The subversion threat in its most powerful form: active, malicious insiders who the customers trust. Even if the company is pro customer, this type of compromise can be disasterous. For this, I've included a list at the end of this post showing all the ways it can mess you up.

## My reactions to Bruce's essay

"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."

Bamford's Puzzle Palace said the same kind of thing in another time. The resources into these efforts were specialized, massive, and cutting edge. I'm sure the specifics you read on their 21st century version were pretty amazing. Of course, commercial organizations such as Facebook do the same thing so govt no longer has a monopoly on tech for massive data movement and analyses. There's potential for cooperation and competition. And probably other implications we've yet to think of.

"The NSA also attacks network devices directly: routers, switches, firewalls, etc. Most of these devices have surveillance capabilities already built in; 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."

I've often told people to use hardened, minimized versions of OpenBSD for routers or security appliances. This strategy's worth just went up 1,000%. The other was MILS type kernels with plenty partitioning and info flow control on system components. Those companies are tight with government, though, so might be backdoored by now. There's still at least open source microkernel type platforms to build on such as OKL4, Tud:OS, Turaya, NOVA, Minix and Genode. And CHACS at Navy has a paper on how to break a basic network stack into pieces a sep kernel can manage. Do the same for the other functions, etc.

"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. "

Subversions that look like accidents. It's been the gold standard of compromises for years. Keeps proving itself out. Deniability works for them just as well as for crooks.

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

The encryption part ideally should be a black box the average developer can initialize and run traffic through. The box should work with pipeline type designs. There's a few OSS crypto libraries that do this already and which have had a decent amount of scrutiny over time. I'd advise people wanting more standardized approach to start with those libraries.

For more safety, it's best if the specific algorithms, IV's, or other security-critical parameters are both randomized and transmitted secretely like the key. The simple version is to program all these things to send 512bits of material. You can squeeze all kinds of keys, IV's, salts, algorithm choices, etc. into 512 bits. Combine that with fixed message size and fixed transmission rates for a tunnel that will look the same for many types of traffic. And put 50-80% of the effort into handling error conditions safely during initiation, processing, or cleanup. And \*only\* allow safe arguments or configurations: don't even code them if they're not safe.

(Certain people I've told about removing all weak options and unneeded code claimed to have edited proprietary binaries in the part that handles weaker options to just freeze the app and signal a problem.)

#### Points on Bruce's Advice

" 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."

This is a nice idea for a few reasons although I'd add I2P and Freenet to the mix. They could use the extra scrutiny. More people on these networks is like a denser, busier crowd. Easy to get lost in. However, using Tor will be impractical for many as it's slow, exit nodes can be blocked, or it creates extra scrutiny on the individual.

So, an alternative here is for us to disguise traffic as ordinary traffic. Let's use HTTPS as an example. When they go to attack it, it doesn't work. They come to realize that it might not even be a web browser communicating with a web server. It may be a peer to peer app that speaks a limited amount of HTTP. And the crypto wasn't really AES with SHA2. And the weak failure modes or algorithms in SSL cause an instant connection failure with optional IP block. And some implementations were done in C++, some in Java via GCJ, some in Python, and... one Genera LISP machine (?) with apparent security modifications.

NSA director internal memo: "Deceptive protocols with diverse/deceptive implementations and non-standard usage... who ARE these people?

Even the Chinese don't give us this much trouble! "

"Encrypt your communications. Use TLS. Use IPsec. Again, while it's true that the NSA targets encrypted connections – and it may have explicit exploits against these protocols – you're much better protected than if you communicate in the clear."

Good advice. Add in my simple, strong algorithms/protocols with safe defaults and obscure defaults you get plenty headaches for them.

" 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."

I've also said that before. It makes sense. The more work and risk an op takes, the more they must justify [to their bosses] doing it. That makes it non-default for them.

"Be suspicious of commercial encryption software, especially from large vendors."

New assumption: this product is safe against everyone but the NSA.

"Try to use public-domain encryption that has to be compatible with other implementations. "

Good too. Allows diversity, peer review and subversion resistance.

Appendix to this below. Now, I can read the comments to this article and maybe respond to them. I can also link to old posts of mine breaking down subversion resistant software engineering and all the levels of attacks they have, if anyone wants.

## A Subverted Organization, Role-by-Role, Attack-by-Attack

1. The person handling the supply chain can buy compromised parts from NSA.

2. The systems architect can weaken total system security with a bad design choice or with an obscure interaction between components.

3. The software engineer coding a security feature can sabotage it.

4. The auditors/testers looking for problems can ignore specific vulnerabilities.

5. The service reps that help the customer choose the product that provides the necessary level of protection can mislead them into buying a weaker product.

6. The project managers can declare certain hard to exploit vulnerabilities as "theoretical" or "not cost effective to fix," then tell the NSA about them. One could argue that this is exactly what all NSA assessments with source code do. ;)

7. The people that write policies on detecting problems or compliance issues can leave out something.

8. System administrators can use logical or physical access to pull details on systems or backdoor them.

9. Maintenance personnel can do any of the above if they have access to the computers or customer data.

10. The company's head lawyer can create fake NSL's sent to his or her department to request information or force backdoor implementation.

11. A member of IT staff might accidentally give a partner organization with intranet access too much privilege. And they do the attack.

12. People maintaining the firewall or access controls might slip up.

The common denominator: all of these involve insiders and each was "probably an accident.... well that's all that's provable." That's the dark beauty of well-executed subversion. ;)

## Bruce Schneier • September 5, 2013 7:30 PM

"I see you're still comfortable working with Truecrypt. Is it too much to ask if you're using the pre-compiled executable available for download, or only if your comfort level attaches only to a version you've compiled yourself?"

I don't compile.

Basically, I'm just playing the odds here. I think TrueCrypt is less likely to be backdoored than either PGP Disk (what I was previously using) or BitLocker.

## Bruce Schneier • September 5, 2013 7:32 PM

"You recommended to 'Prefer symmetric cryptography over public-key cryptography.' Can you elaborate on why?"

## Bruce Schneier • September 5, 2013 7:34 PM

"Using OTP with other encryption methods probably won't make the security any worse, especially when there is reason to suspect that some of those other encryption methods might be broken."

One-time pads are worse than symmetric algorithms. Don't let the theoretical security fool you.

https://www.schneier.com/crypto-gram-0210.html#7

## hoodathunkit • September 5, 2013 7:34 PM

Bruce wrote:

"Could the NSA be intercepting downloads of open-source encryption software and silently replacing these with their own versions?"

## Yes, I believe so.

Of course they could . . . and have. They did it with PGP back in '91-'93 (MSDOS 5&6). The PGP software was usually safe, but entirely command line and a lot of people used a shell to drive it. *Somebody* had dozens of shells written that deliberately left 'bits' on the hard drive, pretended to use PGP but encoded using ROT13, thrashed hard drives (you could do it back then), and assorted mayhem.

#### Bruce Schneier • September 5, 2013 7:37 PM

"I think one of the more surprising revelations in one of your articles today is that you still use Windows for most things. Seriously?!? How and why?"

Yeah, well.

## Gweihir • September 5, 2013 7:45 PM

Thank you for working on this with the Guardian and others! Having a true and recognized crypto expert that also has sound judgment on the non-technical issues in there is incredible valuable.

#### GhostIn(Your)Machine • September 5, 2013 7:51 PM

@name.withheld.for.obvious.reasons: I got "involved" in late 2003 or so, was just a student with an interest in security who had broken a few school systems and found some (looking back on them) pretty crappy holes. Still, there was a program at my school, and it got attention from them. In said program, I must say I had some of the best teachers I ever have met, and I wish I could still be studying under them. Many of them have forgotten more about computer security than most practitioners will ever know, and have their names in the thank-you sections of many of the basic texts in the field.

I had a talent for finding bad assumptions made in network devices, and that is what my research was based around, but classes covered everything from the Shannon papers and mathematical modeling to quantum crypto theory, forensics, and counter-forensics. I was always clearly taught that the US agencies, particularly the NSA, are dual-mission, charged with both protecting US government and commercial computer systems as well as ensuring the capability to penetrate other systems on demand.

Around 2008 I started to see a very disturbing trend: The focus shifted from offensive and defensive mix to almost pure offense, both in teaching and in the direction that projects were heading (and what my fellow students were being prepared for). It went as far as sitting at dinner with professors from the program one night and them actually trying to convince their pupils that some classes of security vulnerabilities in systems we were discovering should NOT be disclosed to the vendors or open source communities, because it would make it likely that not only would those issues be fixed, but also similar vulnerabilities in other system might be fixed.

That thought disgusted me, and when I asked the head of the program about it, it was made clear that was the direction that leadership from the very top had decided to go, and there was little to no hope of changing it. More than any other event, that was the one that drove me out.

I joined to learn to break systems, but I also discovered it was possible to construct systems that could not be broken, and could be proven to be secure. During my time there I worked on many exotic systems I never had encountered before, including a TCSEC A1 rated system. There was one project with complete formal modeling, I wasn't directly involved, but got to watch and see the results of fellow students, go through and be taught everything step-by-step. The other students built a provable secure server for a modern protocol, and had it validated! (I was doing a

different project, more offensive than defensive in another lab, so sadly I was not hands-on for that)

Seeing it done, knowing it could be done, and knowing enough to understand how, from the ground up a provable secure system with modern networking and protocol support was built, I determined that what I wanted to do was provide that. Later seeing the decision to stop all development on it, and even discussions about government silencing public research in the field to prevent that information getting out, as it would pose a threat to the "primary mission"... I left, thinking "to hell with them all".

Now I work for a private company, not US based, in the computer security field. We make software that touches many of these areas, and I am pleased to say the quality of the software has improved since I joined, a lot. Still, I must admit it is a long way from what I hold in my mind as "secure" after seeing it done right.

Maybe some day it will be done right, but for now I am having to settle for trying to prioritize what vulnerabilities and potential vulnerabilities must be fixed first. I have recently come to the realization that my employer will never release software I would consider absolutely secure, and for all they say about providing security against national-level threat actors, the way they work, they will never compete at that level, and I am pretty sure they do not want to.

Right now I am debating how to proceed; what I want to do I have become convinced will never occur at my current employer, but I can't think of anywhere outside a government it is practiced, and I don't have the means to start my own company yet. How I will proceed, I do not know, I just know what I feel must be done.

# Nick P • September 5, 2013 8:02 PM

## @ William A Hamilton

+1 for mentioning PROMIS. I should have had that one in my list of precedents. It was one of my early inspirations for worrying about subversions and software companies being front organizations.

## @ How Far

"Could the NSA be intercepting downloads of open-source encryption software and silently replacing these with their own versions? Is there any way to detect such interference had the NSA enough control over communications channels to automatically replace binaries and published hash lists?"

Yes. That's called a Man in the Middle attack and swapping out executables in transit was even used by clever black hats closer to 2000. File integrity checks are the main proposed method of validating the download. However, if the source is compromised, they might put compromised hashes on the site. So, using trustworthy sources and validating them is the most important defense. One can also use separate PC's for acquiring the file and checking/using it.

## @ Mike Doherty

"You recommended to "Prefer symmetric cryptography over public-key cryptography." Can you elaborate on why?"

I totally missed that line when I read the article. I've been pushing people to do that on his blog for a long time. The reason is that symmetric algorithms are both safer from their codebreakers, interchangeable due to large number of good ones available, easy to implement on many chips, accelerated on some chips, faster in about every case, use less bandwidth for integrity protection than public key, and can be used for many extra things such as authorization (e.g kerberos) or proof of work schemes. You can do a high assurance implementation of a few primitives for many CPU types and FPGA's, then leverage them in countless designs for both standalone and distributed, servers and desktops, general purpose and embedded.

Symmetric crypto kicks public keys ass except for it's signature (no pun intended) use case: trading a secret without pre-sharing a secret. Even so, it's use can be limited to that part and symmetric used for everything else.

## @ Tin Foil Hat

"Why put all the eggs in the same basket and make the secrets vulnerable if NSA manages to find a method to break the symmetric encryption (or public key encryption) you are using?"

That's why I've always pushed for us having a bunch of different primitives that are each heavily cryptanalyzed. The classic example is in block ciphers where we have Blowfish, IDEA, Triple DES, and all the AES candidates. That's not one basket: that's about nine algorithms. Then quite a few different ways of implementing and using them. Or was I using one of the ESTREAM stream ciphers? The data always looks the same scambled...;)

## @ Tango

"TrueCrypt is an NSA program. You offer a free program that works on almost all personal computers. Millions download and use it. When your agents or assets get caught with TC on their laptop, it doesn't mean they are working intelligence. Everyone uses TC. But is it secure, or is there an NSA backdoor in the program?"

Honestly, if it was, I'd call it one of the best investments of tax dollars into INFOSEC the government ever did. I'd even praise them for it. OF COURSE, there could be a subtle flaw NSA can see but nobody else can. That's true even if Truecrypt is built by trustworthy people, yeah? However, the NSA would have also protected our data at rest from every OTHER attacker including the FBI and it seems DOD investigating their

opponents. It would be a win for us (mostly) and an epic fail for the majority of government eavesdroppers.

## M. • September 5, 2013 8:06 PM

You mention you still primarily use Windows. But why? Do you have things you need to do that you feel you would be unable to do in Linux? Do you plan to fully switch to Linux?

It seems contradictory to assume Windows is compromised and guess that another system is likely to be more secure but still not switch.

Another question: do you see any reason to assume that OpenBSD (or some other security-oriented OS) is any safer than Linux?

## Werner Almesberger • September 5, 2013 8:13 PM

How Far: "automatically replace binaries and published hash lists?"

Some ad hoc-ish thoughts:

Let's assume they can. To detect this, the recipient could contact the originator through a secure channel (e.g., a face to face meeting, if they already know each other) and verify the hash.

Countermeasures to this could include: 1) surreptitiously changing the hash(es) they carry, 2) suppressing the meeting or the reporting of the detection of a mismatch, 3) selectively providing uncompromised versions to likely verifiers, 4) compromising the binary even before the originator gets access to it, 5) compromising the originator.

1) may be too difficult, especially if people get creative or have good memories. 2) may be an option, particularly through extortion. Likewise, 5) could work by extortion, or simply by "turning" (or having turned) the originator. 3) would depend on the NSA's capability to compromise mirrors in foreign countries.

3) would be particularly effective if a small number of downloaders could be singled out for receiving the compromised version, while all the rest (probably including all likely verifiers) would get the uncompromised version. Furthermore, this could be randomized or the tampering could be done only on the first access, so that inconsistencies that get detected would vanish when repeating the operation, get blamed on "natural" corruption, and not trigger an investigation.

4) would be the most elegant solution and could be implemented by compromising the build system or the communication to/from it. This may get particularly feasible if the build system is some compile farm or cloud service.

4) could also be implemented by compromising something that enters the binary but is not considered to be part of the source proper, e.g., libc or some other library or header.

Regarding 3), it may make sense to carry lists of hashes with you whenever you go to a meeting with like-minded individuals, then compare them over a few beers. Depending on the scenario, also peer-to-peer comparisons (as opposed to the more difficult recipient-to-originator) could be useful. Chances are there's nothing to detect, but it may still be fun to play that game for a while.

I would worry about 5). To detect tampering at the binary's origin, one would need fully reproducible build processes, so that the same source compiled in a well-defined environment would yield the same binary.

4) would be the hardest to defeat. Getting rid of untrusted compile platforms and communication paths would be a good and easy first step.

To ensure that also the trusted environment is safe, one would basically have to audit the source one has downloaded, all the code that gets pulled in, verify that the compiler generated the correct assembler (and that the assembler translated it correctly, that the linker didn't mess with it either, etc.), and also have some verification that the result doesn't get compromised on its way to the release site(s).

If the goal is to determine whether such tampering exists at all, the best place to start would be old material, released before the Snowden incident, so that NSA and friends shutting down any tampering equipment now would have no effect.

- Werner

# Steve • September 5, 2013 8:13 PM

@b f skinner:

Yes, I understand the mechanics of how information is passed along and, yes, I've read (some of) the "Pentagon Papers."

I also understand the mechanics of celebrity and how literary fortunes are made.

While I will point out that Mr Greenwald has done a great service to the world by telling us what most reasonably observant people already know in principle: governments spy on their citizens, he is also a terrible human being who will sacrifice others to reach his goal which is largely notoriety for on G Greenwald.

He (and the Guardian) badly burned Edward Snowden by not getting him to a safe place before publishing and he exposed his husband/domestic partner to inexcusable danger by using him as a courier/mule (a story, by the way, which has been played for maximum histrionic effect by the selective shading of facts on the part of Mr Greenwald's reporting).

I don't believe in "killing the messenger" but in this case the messenger does need a good swift kick in the pants for the people he's wronged in the process of telling his story.

If I were Bruce Schneier, I'd be very careful around Mr Greenwald, since I believe he'd happily toss Dr Schneier under the cliched bus if it were to his advantage.

#### Petter • September 5, 2013 8:25 PM

@Bruce

In your opinion, would you describe signed and encrypted email using CA-issued 2048-bit certs for broken or are they still secure enough?

## Carlo Graziani • September 5, 2013 8:25 PM

OK, Bruce. How about making the challenge to the IETF a bit more specific: could you name some titles of new RFCs that should be written? What are we replacing here?

SMTP obviously needs to be replaced by a messaging protocol that minimizes exposed metadata and routinizes application-layer encryption.

Do we need to go lower down the stack? Is DNSSEC good enough? Routing protocols? TCP/IP?

Give those guys a specific agenda. You read the documents, you're in a good position to draft one.

#### Britt • <u>September 5, 2013 8:27 PM</u>

You have confirmed my deepest fear... Thanks for your Call to action.

(I'm thinking; what could I do?)

#### Rudd-O • September 5, 2013 8:27 PM

"The good guys".

LOL. How deluded, that jingoistic commenter.

#### GreyGoose • September 5, 2013 8:32 PM

MarkH, couldn't have said it better. Thank you.

## Zooko • September 5, 2013 8:34 PM

Bruce:

It's too bad that people will read your warning about elliptic curve crypto and then stay away from \*all\* elliptic curve crypto, even <u>Curve25519</u>, which is not subject to the possible backdoors which you are warning against. This might cause people to distrust tools that use Curve25519, such as future versions of Tor and future versions of my project — <u>Tahoe-LAFS</u>.

We need to move to elliptic curves because RSA and integer discrete log are so inefficient, at the desired security level, that they make our tools less usable for actual use. For example, in LAFS we generate a new public-private keypair whenever a user creates a directory. Currently this is a 2048-bit RSA keypair, and so this is a real performance issue. I believe similar efficiency issues (especially with respect to size of public key) are pushing Tor to move to Curve25519.

Regards,

Zooko

#### Maxfactorx • September 5, 2013 8:34 PM

Bravo! Bravo! Bravo! Bruce you are truly a national treasure. Thank you for taking this position publicly and being such a strong voice for liberty and progressive cutting edge technical, moral, analysis. Yours a real patriot! And we love you brother!

#### underscore • September 5, 2013 8:44 PM

Thank you Bruce for your work on reviewing the documents and especially the advice and additional viewpoints you have provided.

Here is a question I wanted to ask anyone who might know: When discussing the encryption that Laura Poitras would need to have configured, Edward Snowden had told her to "assume that your adversary is capable of a trillion guesses per second"

My question is, is this realistic? Can it be realistically assumed that NSA has the capability to go through a trillion guesses per second? Or was Ed Snowden perhaps exaggerating to ensure that Laura selects a really strong password?

# David • September 5, 2013 8:44 PM

Bruce,

In your article about taking back the internet, you talk about needing more whistleblowers.

Given the current high profile of this topic, do you have any recommendations on how to even start the process cold? How does one, without just exposing their jugular, start to pass along a tale? With Whom would you recommend starting the conversation, especially since there seem to be so many conflicts of interest, unreliable reporting, and laser-like focus on the current actors (Greenwald, Poitras, etc)?

I'm not asking about specific techniques, or a how-to; rather, I think the biggest block to telling the world is that those who know have a hard time answering the question, "How do I even start?"

#### Douglas Knight • September 5, 2013 8:49 PM

Does NIST 2006 standard with a backdoor found by 2 MS cryptographers in 2007 uniquely identify Dual\_EC\_DRBG? If so, why not just say it?

#### Buck • September 5, 2013 8:54 PM

@Bruce

"Could the NSA be intercepting downloads of open-source encryption software and silently replacing these with their own versions?" Yes. I believe so.

I am also interested in learning more about this particular revelation. I (along with many others here) have assumed the existence these types of interception techniques for years... Surely the NSA isn't the only entity that has been developing such capabilities.

I do wonder for whom, how, when, and why these listening posts become active in their MITM attacks. Obviously, open source software wouldn't be the only bits of bytes subject to a surreptitious manipulation of information streams...

Should public leaders have any reason to believe that their digital communications have not been altered before receipt? Can the intelligence community make the same claim?

These backdoors are in place, and someone must have the keys... Who's to say that they've kept these secrets better than some of their others?

Seems that these surveillance capabilities have vastly expanded vulnerabilities to national security. We decided yes, we can spy on everyone; never stopping to consider whether or not we should... I'd bet that money would have been much more beneficial to security if it had been put towards developing secure systems!

Of course some of it has been... Apparently, Alamos National Laboratory has been running a quantum network for almost 3 years! So perhaps institutional communications have been secured to a reasonable degree... Still though, I'd have to assume that their agents remain vulnerable. Do they not use 4G, Facebook, and Gmail in their personal lives? If not, that would seem to be a great way to blow one's cover! :-P

Also of great interest will be the hardware-based backdoors...

Are IC manufacturers reasonably secured?

How easy would it be to plant some small secret circuits (in an incredibly complex chip) just prior to production and remain undetected for lengthy periods of time?

What kinds of transmissions can be used to defeat air-gapping via subverted silicon?

## Figureitout • September 5, 2013 8:59 PM

What a monumental task, rebuilding the internet. I really don't know if we're all up for it and how we could organize the project? Surely you all would know that you would very likely be working along side an agent trying to subvert your project. Where would you secure your work? Physical compromise, if you've never seen it, is now an issue. This will scare away a lot of people and it will ruin the atmosphere of working on the project.

Almost like a NASA problem or making your computer almost entirely from scratch, just using many basic parts you can't fab but they will be visible.

Anyway, this just sucks. How quickly did the internet and all its infrastructure go from "Holy Cow!" to "That's creepy scary".

## lan • September 5, 2013 9:03 PM

Would it be worth buying old 386 machines for encryption purposes?

## tazman • September 5, 2013 9:09 PM

I find it humorous that you express concern over government spying, and yet link directly to a facebook page for readers to follow... The irony is immense.

There are social networking platforms built on Free/OSS, that are decentralized, federated, secure, and with varying degrees of privacy, that respect users and do not spy on them, collect their information, or spam them with advertisements (indeed, as they are user owned and operated, not operated by corporate behemoths who have a strangle-hold on so much of the rest of the internet) such as <u>friendica</u>, diaspora, pump.io, statusnet, libertree, and most amazing, the up-coming <u>redmatrix</u>.

#### Sharon Kramer • September 5, 2013 9:14 PM

Thank you for all your hard work.

I'm waiting on the info to come to light of the US Chamber of Commerce's involvement/access to private information in this debacle.

If you remember, Annonymous hacked HBGary Federal in 2011 and found info of the US DOD introducing them to the Chamber as a potential client to spy on US activists. The intent was to use the info to set up fake social media identities and character assasinate US citizens to cast doubt on the validity of their words, that are typically adverse to the interest of US industries.

HBGary was purchased by ManTech International, of Fairfax, Va in 2012. It ranks No. 22 on Washington Technology's 2011 Top 100 list of the largest federal government contractors. The Chamber is the first lobbying group to top \$1B in DC lobbying dollars.

I'm betting its just a matter of time before the dots are all connected back to the NSA aiding US industries to spy upon and discredit US citizens.

Good article from the Nation on the subject. <u>http://www.thenation.com/blog/174741/...</u>

## None • September 5, 2013 9:16 PM

Hi Bruce - any suggestions on a BleachBit alternative for OSX? Likewise, TrueCrypt seems to be abandonware on that platform - thoughts on how secure FileVault 2 is?

#### underscore • September 5, 2013 9:18 PM

@tazman:

There are social networking platforms built on Free/OSS, that are decentralized, federated, secure, and with varying degrees of privacy, that respect users and do not spy on them

That brings to mind the "de-centralized version of Facebook" called Diaspora that received some good Kickstarter funding a couple of years ago.

What came out of it? Nothing much. One of the developers (supposedly) committed suicide and the others released v0.10 which they then left in the hands of the community...

#### Jonathan • September 5, 2013 9:39 PM

> Encrypt your communications. Use TLS. Use IPsec.

Loved the two articles. I just hope people who read the articles know what TLS and IPsec are/stand for.

I know what TLS is but to be honest I'm not sure if I use IPsec. If I use OpenVPN am I using IPsec? I'm not sure.

Keep the articles coming!

This is a very interesting post on the Intel built in random number generator with responses from the generator's designer.

https://plus.google.com/117091380454742934025/posts

Theodore Ts'o:

"I am so glad I resisted pressure from Intel engineers to let /dev/random rely only on the RDRAND instruction. "

#### Engy • September 5, 2013 9:48 PM

If they are in fact installing backdoors, this leaves huge vulnerabilities in everything. This isn't going to end well for anyone, including the NSA.

#### CivLib • September 5, 2013 9:52 PM

Bruce,

Adding my voice to the chorus, and enthusiastically echoing MarkH's sentiments, I simply say :

Thank you, Sir.

Let us know when we need to initiate your legal defense fund.

## Julien Couvreur • September 5, 2013 9:58 PM

Bruce Schneier says: "Basically, I'm just playing the odds here. I think TrueCrypt is less likely to be backdoored than either PGP Disk (what I was previously using) or BitLocker.

Here's a proposal to improve the odds: chain encryption.

Use a PGP disk inside a TrueCrypt archive on a BitLocker drive. If any of them is not backdoored (and your OS isn't compromised), then the result should be secure.

## para.noid • September 5, 2013 10:04 PM

So if they can replace executables during a download then I guess they can replace web pages (or PDF files) too? I mean if they want a person to get other information than what s/he thinks they are getting.

#### Johnston • September 5, 2013 10:05 PM

Worth noting that the author of Curve25519 does not trust NIST curves.

Hopefully we see Curve25519 more and more. It has been selected for use in DNSCurve, CurveCP, Tor, Tahoe-LAFS, and Google's new QUIC protocol.

#### gonzo • September 5, 2013 10:13 PM

@julien courveur

I would be reticent to try to overlap three softwares each of which are doing their best to grab all low level disk accesses and convince their respective operating systems that the encrypted containers are logical discs.

Ever see how computers (mis) behave when two virus detection suites are installed at the same time and don't know how to play nice?

#### Gomer • September 5, 2013 10:20 PM

Bruce, you didn't even get the signals intelligence directorate name right in your guardian article. What other things don you assume you know that u botched up? Pompous and assuming.

#### Dan • September 5, 2013 10:35 PM

Hello Bruce Schneier,

One simple question:

As simple user, that don't implement the security itself on websites (or VPN systems), I don't have what to do about it.

the only thing that I have control is when i'm using cloud-hosting: till day, I mostly used WINRAR (from RARLAB) encryption password (on document stored on cloud, that I didn't want to be digged on)

Now, I think maybe to change my software that I use to encrypt personal files (becuase WINRAR could have backdoors as it's aren't open sourced)

Should I change to 7zip? you have better offer?

Truecrypt actually sounds too good to be true ("Plausible Deniability" - Like they want illegal things will use it). the developers are even anonymous, so, it's even rational (after latest NSA leaks) that maybe NSA behind it. I think that it's even easier to backdoor opensource like Truecrypt than actually force company to implement it. (considerate the gigantic budget NSA has) What do you think?

BTW: Truecrypt founded before 9.5 years, right after NSA start finance the anti-encryption programs..

## AdamB • September 5, 2013 10:49 PM

Could the recent discovery of Barracuda firewall backdoors be work of NSA ?

https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories\_txt/20130124-0\_Barracuda\_Appliances\_Backdoor\_wo\_poc\_v10.txt

Adam

## Doctor Memory • September 5, 2013 10:52 PM

This seems like as good a moment as any to remind people of some pertinent facts:

http://www.coresecurity.com/files/attachments/... http://www.slideshare.net/endrazine/...

Draw your own conclusions.

## GregW • September 5, 2013 10:58 PM

I think the comment that "Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted" underplays the likely implementation vulnerabilities that are neither subverted code nor math.

E.g. known plaintext in protocols and documents (e.g. HTTP headers encrypted within SSL, known HTTP text within specific target HTTPS websites, known byte sequences within Word documents, etc).

## floppy • September 5, 2013 10:58 PM

remember the old days when we had to transfer data by putting it on a floppy disk and hand it to a friend? guess what, what's old is new again. now the Internet is only good for sharing pictures of our cats.

I just hope that old computer in the closet and the stack of floppies still work.

## DB • September 5, 2013 10:59 PM

I wonder if the NSA has forced a designed-in weakness in things like Intel's digital random number generator built into every modern intel computer (Intel's Ivy Bridge DRNG).... which would therefore weaken every encryption key generated on every modern intel computer, for example...

#### GregW • September 5, 2013 11:00 PM

So Bruce, should true hackers boycott the Obfuscated C contest, since its value for adding to the NSA playbook of "accidental mistakes" outweighs the honor of displaying one's cleverness?

#### I wanna Fight • September 5, 2013 11:01 PM

How do we fight back, how do we take the internet back from this over-reach? How can we trust anyone ever again? How do we get people

above-the-law to be bound by those laws again? How do we scorch the neck stumps of this hydra? Well first, we have to cut a few heads off...

#### Michael Moser • September 5, 2013 11:22 PM

So the next time that we see a report on broken random number generator we know that the feature is by design

#### Johnston • September 5, 2013 11:28 PM

@Bruce:

You write, "...whether you're running Windows, Mac OS, Linux, iOS, or something else – and a variety of tricks to get them on to your computer... 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."

Have you seen documents about exploitation of CPU bugs? Anything about Sparc64? What about OpenBSD? I'm talking about unknown vulnerabilities of course.

Thank you dearly for all you do.

#### Long Time Lurker • September 5, 2013 11:29 PM

"I have been working with Glenn Greenwald on the Snowden documents, and I have seen a lot of them. These are my two essays on today's revelations."

I hadn't realized this. It explains a lot about the bias (and ignorance) you have been showing in your articles since this whole affair broke, Bruce.

I am a little surprised here that nobody seems to be concerned that the NSA actually has a mission: counter-intelligence, protecting US government systems, counter-terrorism, etc....

Does anybody here realize how seriously the release of this information about sources and methods will compromise that mission? There is a very good reason this stuff is classified. And all your paranoia aside, it's not because they don't want Americans to find out -- it's because they want the methods to still work against the "bad guys".

I also find it ironic that everybody is dog-piling on the NSA at the same time they anxiously wait "intel" proving who was behind the chemical attacks in Syria. You can't have it both ways, folks. There's not going to be any useful intelligence in the future if you take away all the tools.

Anyway, I hope nobody here complains the next time there is an "intelligence failure" and we don't manage to thwart the next foreign-grown threat, whatever it may be.

#### Michael Moser • September 5, 2013 11:35 PM

What happens if. Openssl now removes weak ciphers from the library? How is the NSA going to punish them?

#### gonzo • September 5, 2013 11:39 PM

@long time lurker

Stick it in your ear.

The NSA can accomplish its mission without "capturing the entire haystack."

Part of the problem with being so infatuated with devoting ever increasing resources into making a surveilence state dragnet is that the security apparatus forgets to put the due focus on the actual points of risk.

Two words: Boston Bombing.

For all the Americans' stuff being caught in the "collect the whole haystack" philosophy, it somehow was not obvious to prioritize and actually use "subject specific" tools for a guy who traveled to a radicalized area and, ahem, as to whom we had actually been WARNED through official channels by another nation state.

Finally, please explain to me how sniffing all the encrypted packets between my computer and my online banking institution provide a material benefit to the acquisition of intelligence regarding the Syrian chemical attacks. Seriously, you're reaching.

## Long Time Lurker

--I speak for myself as an American citizen as saying: "I don't give a >>>> who carried out those heinous chemical attacks. It happened in their country, thus it is their problem to solve.

If you or the other politicos who want to go to "war" yet again want to do something about it, suit up and go get killed.

Our critical systems should be shielded and isolated and localized and there are other ways to encourage this security. Centralized control will fail and I don't trust it.

## anonymous • September 6, 2013 12:07 AM

The NSA also devotes considerable resources to attacking endpoint computers. This kind of thing is done by its TAO – Tailored Access Operations – 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.

## http://www.theguardian.com/world/2013/sep/05/...

This seems like it might be more problematic than the NSA cheating to defeat global network security protocols. Can you share more about this, even if you don't want to reveal everything? Can the average user either do things or avoid things to address this?

## MarkH • September 6, 2013 12:37 AM

@"long time lurker":

Let me see if I got this right...

...we need NSA to determine who ordered chemical warfare attacks in Syria? That's news to me. I thought that observations (coinciding with the time of the poison gas casualties) that ordnance was fired from government-controlled territory into the rebel-controlled district where people were poisoned, made the case fairly well.

...and it is necessary for US officials to **betray their oaths** of office, and shred the 4th Amendment to the US Constitution by illegally spying on US citizens in the United States -- in order to determine who ordered chemical warfare attacks in Syria?

Are you suggesting that the orders for the poison gas attack were issued from Rapid City, South Dakota? Perhaps Modesto, California? Maybe Bowling Green, Kentucky? Or was it Terra Haute, Indiana?

Do I understand correctly that you make no distinction between the interception of foreign signals intelligence (NSA's lawful mission) and domestic spying, forbidden to NSA by both the United States Constitution and federal statutes?

Did I follow your logic correctly, or did I miss something?

## Alain from Switzerland • September 6, 2013 12:41 AM

Kudos.

Very recomforting to see this coming from an US American, gives hope. Corresponds pretty much to my expectations of how it is that I had over the years, never felt any of these systems were without backdoors etc.

One, I think, crucial question remains yet unanswered - how much data is collected and stored, resp. could be stored once the new facility in utah goes operational? How much data is on average kept per average (typically completely innocent) citizen of any country in the world...?

#### Rob • September 6, 2013 12:52 AM

From the Guardian article:

"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."

I initially felt that maybe you knew something from looking at the documents that would have backed this up. Reading your responses above though, it seems that you do not know which algorithms are safe.

Maybe reword it a bit since some will end up quoting you saying that "you can remain secure even in the face of the NSA" if you follow bruce's five point plan and use diffie-hellman. I think we are in the same position we have always been in; we have no idea what the NSA is truly capable of and have no reason to believe we are secure against them. Now we just know that they likely wield the kind of power we always

#### imagined/feared.

Love your blog though... just feel maybe we should be more explicit that we do not have any clue yet how to protect ourselves from the NSA or state powers.

## Albert • September 6, 2013 1:01 AM

Ok, on to the big question. Is AES safe?

## Jason Green • September 6, 2013 1:14 AM

Bruce,

First, I join many here in offering my deep thanks. For more than a decade you have been an all too rare voice of sanity and reason about security, helping to make important issues understandable to the rest of us.

I do have a couple of questions. In describing your own practice, you mention that you don't use all the security tools all the time, and that you use a machine with an air gap for highly sensitive material. I wonder how this squares with the notion of trying to improve everyone's security by getting as many people as possible to encrypt as much as possible. By doing this, you make it economically/computationally impractical to dig wanted data out of a huge encrypted "haystack". That kind of large scale encryption won't happen if every encrypted tweet and email has to cross an air gap.

Finally, I would like to encrypt most of my internet traffic as I see that as something an "ordinary person" can do to protest the surveillance state. Unfortunately, nobody I communicate with on the web shares my concerns, so apart from signing my facebook wall posts to make a point, encrypting will be a hassle. Since I'm unlikely to convert my social graph to the cause of encryption, what ought I do?

## Johannes • September 6, 2013 1:22 AM

> Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted.

I don't mean to offend, but at this point, I think this naïvety is either wishful thinking or it borders on stupidity.

The NSA has been involved in every major standard released by the NIST, so they should all be assumed backdoored. I mean, sure, there's review from academia (the integrity on most, including youself, is not doubted) - but: do you really think you stand a chance against all the intellectual capacity accumulated by the sheer NSA's limitless budget? I hardly think so.

It might be difficult to admit, but they've been ahead of academia forever. GHCQ/NSA had RSA long before we did. The gap only widened when academia found out about linear cryptanalasis only after the year 2000; the NSA already incorporated this knowledge when designing the DES S-boxes.

The only valid conclusion is that they are lightyears ahead by now. I feel we are facing an adversary that will not be defeated easily.

## gonzo • September 6, 2013 1:29 AM

@Jason Green

I think the key reveal is in the indications re: Snowden's comments on end point security, and the fact as Bruce says, that if the NSA wants to get into your computer they will.

An air gap is therefore crucial at least for decryption operations -- for your most secure communications, you do not want to be keying your pass phrase into a machine where the very OS, nay, even the hardware, could be compromised.

## Winter • September 6, 2013 2:03 AM

On the source of randomness. What is exactly against putting a microphone next to a fan and compress the sound (bzip2?) and hash it?

Air turbulence is inherently chaotic. I must be missing something important here.

# @How Far

"Could the NSA be intercepting downloads of open-source encryption software and silently replacing these with their own versions?"

Git was designed to prevent corruption of the source tree. I always understood that you could trust a git repository to detect a corrupted download. The underlying SHA1 is not considered secure anymore. But would it really be possible to replace files with functional identical code with the same SHA1 hash?

With a secure Git tree, you can rebuild the original system. And we already know how to defend against Trusting-Trust attacks: <a href="http://www.dwheeler.com/trusting-trust/">http://www.dwheeler.com/trusting-trust/</a>

Selective replacement of web pages and message digests could be easily thwarted by looking at the pages using Tor and open VPNs, changing the identity between reads.

#### Winter • September 6, 2013 2:11 AM

About covert Tor use

A long time ago (I did not check it recently), the Tor pages would say that if you ran a Tor node, all your Tor requests would be directly fed into the Tor network. So your Tor use would be hidden, and you would not be vulnerable to timing correlation attacks.

I always found that a rather dubious claim. Running a Tor node makes you visible as a "suspect" anyhow.

With Bruce' advice to hide in the network, I am still curious whether running a Tor node would help you hide in the crowd?

#### Jan • September 6, 2013 2:17 AM

@Petter: "would you describe signed and encrypted email using CA-issued 2048-bit certs for broken or are they still secure enough"

I'm not Bruce, but still: If you are relying solely on the CA to verify that you got the right key, I'd consider it broken. If they really want to, they'll simply get a CA to issue a false cert, one way or the other. It is still a hassle and a risk for them, though (you could store the message and later notice the key mismatch), so you should still use it. If they want in, they'll probably break into your or the sender's computer.

@underscore: "My question is, is this realistic? Can it be realistically assumed that NSA has the capability to go through a trillion guesses per second?"

GPUs used for Bitcoin mining can calculate hundreds of millions of hashes per second. Commercially available ASICs are in the tens-of-billions hashes per second range.

If we are talking about a trillion guesses per second on unstrengthened passwords, I would consider a trillion guesses per second a low estimate. With strengthening, depends on the strengthening and how much resources they dedicate to it, but my personal guess would be that there might be a small safety margin.

@Douglas Knight "Does NIST 2006 standard with a backdoor found by 2 MS cryptographers in 2007 uniquely identify Dual\_EC\_DRBG? If so, why not just say it?"

My guess: Because "Dual\_EC\_DRBG" confuses regular readers, and the readers who are familiar with the matter will know what they are talking about.

#### Jim • September 6, 2013 2:33 AM

"Something is seriously wrong if we have to regard an agency of our own government-- ...- as an "adversary."

It is more wrong than you think. Because this agency is just part of the US government, but not part of the government(s) of the rest of the world.

#### uwe • September 6, 2013 2:38 AM

let's ignore the commercial software aspect of this. what about open source software like gnupg? did anyone with sufficient knoeledge of that topic check the sources/commits which may point to some"crypto sabotage"? I think under normal conditions the mainter of the software in question should check commits/submitted patched before they are applied to a release bu what if the nsa gained direct repository access? I mean you can possibly eleminate backdoors in commercial software by introducing new laws because the developers know what they did but who will do this for open source software? and..hey...that is one of the ideas behind open source: everyone can check it but in my opinion this is not only a right but also a duty

## Jan • September 6, 2013 2:46 AM

@uwe: Since the Debian OpenSSL debacle went undetected for years, the answer is "no". Everyone *can* check the source in theory, in practice, nobody *does*.

Subscribe to comments on this entry

Leave a comment

Name:

E-mail Address:

URL:

Remember personal info?

Comments:

Allowed HTML: <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • • <blockquote>

Preview Submit

Powered by Movable Type. Photo at top by Per Ervland.

Schneier.com is a personal website. Opinions expressed are not necessarily those of BT.