What is the DoD's Position on Backdoors in Security Systems?

In May, Admiral James A. Winnefeld, Jr., vice-chairman of the Joint Chiefs of Staff, gave an address at the Joint Service Academies Cyber Security Summit at West Point. After he spoke for twenty minutes on the importance of Internet security and a good national defense, I was able to ask him a question (32:42 mark) about security versus surveillance:

> Bruce Schneier: I'd like to hear you talk about this need to get beyond signatures and the more robust cyber defense and ask the industry to provide these technologies to make the infrastructure more secure. My question is, the only definition of "us" that makes sense is the world, is everybody. Any technologies that we've developed and built will be used by everyone -- nation-state and non-nation-state. So anything we do to increase our resilience, infrastructure, and security will naturally make Admiral Rogers's both intelligence and attack jobs much harder. Are you okay with that?
>
> Admiral James A. Winnefeld: Yes. I think Mike's okay with that, also. That's a really, really good question. We call that IGL. Anyone know what IGL stands for? Intel gain-loss. And there's this constant tension between the operational community and the intelligence community when a military action could cause the loss of a critical intelligence node. We live this every day. In fact, in ancient times, when we were collecting actual signals in the air, we would be on the operational side, "I want to take down that emitter so it'll make it safer for my airplanes to penetrate the airspace," and they're saying, "No, you've got to keep that emitter up, because I'm getting all kinds of intelligence from it." So this is a familiar problem. But I think we all win if our networks are more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike on the intelligence side than very vulnerable networks and an easy problem for Mike. And part of that -- it's not only the right thing do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I'm also very confident that Mike has some very clever people working for him. He might actually still be able to get some work done. But it's an excellent question. It really is.

It's a good answer, and one firmly on the side of not introducing security vulnerabilities, backdoors, key-escrow systems, or anything that weakens Internet systems. It speaks to what I have seen as a split in the the Second Crypto War, between the NSA and the FBI on building secure systems versus building systems with surveillance capabilities.

I have written about this before:

> But here's the problem: technological capabilities cannot distinguish based on morality, nationality, or legality; if the US government is able to use a backdoor in a communications system to spy on its enemies, the Chinese government can use the same backdoor to spy on its dissidents.
>
> Even worse, modern computer technology is inherently democratizing. Today's NSA secrets become tomorrow's PhD theses and the next day's hacker tools. As long as we're all using the same computers, phones, social networking platforms, and computer networks, a vulnerability that allows us to spy also allows us to be spied upon.
>
> We can't choose a world where the US gets to spy but China doesn't, or even a world where governments get to spy and criminals don't. We need to choose, as a matter of policy, communications systems that are secure for all users, or ones that are vulnerable to all attackers. It's security or surveillance.

NSA Director Admiral Mike Rogers was in the audience (he spoke earlier), and I saw him nodding at Winnefeld's answer. Two weeks later, at CyCon in Tallinn, Rogers gave the opening keynote, and he seemed to be saying the opposite.

> "Can we create some mechanism where within this legal framework there's a means to access information that directly relates to the security of our respective nations, even as at the same time we are mindful we have got to protect the rights of our individual citizens?"
>
> [...]
>
> Rogers said a framework to allow law enforcement agencies to gain access to communications is in place within the phone system in the United States and other areas, so "why can't we create a similar kind of framework within the internet and the digital age?"
>
> He added: "I certainly have great respect for those that would argue that they most important thing is to ensure the privacy of our citizens and we shouldn't allow any means for the government to access information. I would argue that's not in the nation's best long term interest, that we've got to create some structure that should enable us to do that mindful that it has to be done in a legal way and mindful that it shouldn't be something arbitrary."

Does Winnefeld know that Rogers is contradicting him? Can someone ask JCS about this?

Tags: back doors, crypto wars, Department of Defense, encryption, Internet, national security policy, privacy, security conferences, surveillance

Posted on June 24, 2015 at 7:42 AM • 51 Comments

Comments

uh, Mike • June 24, 2015 8:53 AM

It seems that the U.S. Government simply does not believe in good security.

China stole our SF-86s! We can't get much more incompetent than that.

Perhaps the solution is to ignore anything the government says about security, and soldier on doing the good work of making strong doors.

---

uh, Mike • June 24, 2015 8:55 AM

While we're on the subject of SF-86s, some years back, mine was "lost." (And the clock stopped ticking, too. I didn't mind.) I wonder if China has it, or not?

---

wiredog • June 24, 2015 9:08 AM

Intel gain-loss. And there's this constant tension between the operational community and the intelligence community when a military action could cause the loss of a critical intelligence node.
Churchill famously came down on the intel side when he let Coventry get bombed in order to protect Enigma.

---

uh, Mike • June 24, 2015 9:14 AM

@wiredog, what would the best course of a resident of Coventry be, when their government commits treason against their small community, in order to defend the greater realm?

If someone in Coventry finds out they are to be sacrificed, what do ethics demand of their situation?

---

d33t • June 24, 2015 9:22 AM

"NSA Director Admiral Mike Rogers was in the audience (he spoke earlier), and I saw him nodding at Winnefeld's answer. Two weeks later, at CyCon in Tallinn, Rogers gave the opening keynote, and he seemed to be saying the opposite."

I've seen this kind of tactic too often to think it is a mistake. It boils down to a form of the old "good cop / bad cop" act and is done throughout the government today (historically as well). It is done commonly so that information which is in part true and comforting to the questioner can be handed out as a public offering to gloss over an uncomfortable question as well as pre-acquit criminal acts by an ally. It sometimes is so effective that it can make a criminal act look like an accident or misunderstanding or even make something that is done by the ally look like it is in the public interest. A classic propaganda / social engineering / information warfare strategy. "Doublethink" as a tool for today's politician, military or otherwise, is a commonplace, powerful weapon against the public.

A good example are most political references to the FISA court as an "oversight" body, when in fact it is, and is also not there for oversight. Actually it serves multiple definitions of the term "oversight". It's there to keep people from asking questions and to keep the paper work flowing.

I highly doubt there is ever actual conversation or cooperation between Winnefeld and Rogers that includes language about concern for civil rights or strong encryption for use by the public as a priority. If there is, the conversation only addresses political damage control if they get caught violating the constitution by actively undermining standards. There is no fear for them of indictment by court-martial, that is for sure.

Clive Robinson • June 24, 2015 9:29 AM

@ Wiredog,

> Churchill famously came down on the intel side when he let Coventry get bombed in order to protect Enigma.

That is most definitely a black myth and was disproved over fourty years ago.

If you want to know more, part of the story is in Prof. R.V.Jones's book "Most Secret War : British Secret Intelligence".

J. Angleton • June 24, 2015 9:55 AM

Honestly, Bruce. Do you actually believe that spies would *not* lie in public. Spies are defined by their secrecy, manipulation, and deception. It's was they do (as JTRIG leaks recently illustrated).

This was clearly a public relations stunt and Winnefeld was feeding you talking points.

Of course they contradict each other. It helps to muddy the water and keep the proles guessing.

Anno 2015 • June 24, 2015 10:27 AM

Has anyone considered how many people could be potentially blackmailed now? The answer is approximately 14 million.

Has anyone also considered what consequences this could have? At what levels and for how long?

That's my most important argument. The rest is less important.

- The Russians got the message all right. They are now using typewriters and paper for their top secret stuff.

- In a more advanced country the people who are responsible for the infrastructure in where such a data breach could take place would be shot. Heck they would be shot for a lot less. In an even more advanced country the responsible people would just kill their selves. It's about taking responsibility and shame.

Not a historian • June 24, 2015 10:36 AM

@wiredog - I think the official stance with Sir Winston was that the intelligence wasn't communicated to him in time, i.e. he didn't know.

Question • June 24, 2015 10:39 AM

I see that Bruce's SSL certificate was renewed on 16/06/15 (expires: 17/06/16) with GeoTrust Globl CA.

Can anybody else confirm that the correct fingerprint is:

F9:1C:51:73:17:C2:86:87:02:86:AB:FF:9D:28:CD:09:C9:85:73:02

Thank you.

Bob S. • June 24, 2015 11:14 AM

Mr. Rogers like his predecessors gives the impression of a prevaricator for hire. Also that he's not very good at it. I wouldn't trust him swore on the Bible the sun would rise tomorrow.

I guess that's how the NSA views the job description of it's leaders.

That would be fine in some dictatorial police state, but for a non-elected, thus non-representative appointee to be allowed such a privilege in a so called democratic society is....unbecoming. One of the problems becomes we must grant license for all nations to act accordingly.

I confirmed the schneier.com fingerprint at https://www.grc.com/fingerprints.htm

---

paul • June 24, 2015 11:55 AM

There's one more really stupid assumption in the Rogers position: that government and law enforcement are the smartest guys in the room. Even leaving aside the incredibly bad operational security the US government keeps demonstrating (think: all of that stuff collected through back doors and protected by OPM-level safeguards) there are plenty of other smart folks around in other countries and large political/economic entities. Not only can they walk in through any back door that's opened for law enforcement and intelligence collection, they can also use their own tech and operational security to close backdoors other people leave in their systems. (Maybe not all of them, and maybe not with immunity to targeted attacks, but enough to disrupt plans based on easy backdoor access.)

So if the serious baddies can mitigate the back doors, who is it they're going to be useful against?

---

name.withheld.for.obvious.reasons • June 24, 2015 12:02 PM

@ Question

The certificate for the site where CN=www.schneier.com and OU=GT85546578 consists of:

CA Identifier:
c3 9c f3 fc d3 46 08 34 bb ce 46 7f a0 7c 5b f3
e2 08 cb 59

Signature(s), Fingerprint(s);
SHA-256:
0D:87:F5:DD:6F:86:89:0D:59:8F:95:CD:57:1B:74:DA:67:6F:F8:17:9B:22:37:A6:F5:6C:8E:E9:81:99:89:B2
SHA-1:
F9:1C:51:73:17:C2:86:87:02:86:AB:FF:9D:28:CD:09:C9:85:73:02

If others post certificate data or if you see a variant, this could expose a network transient/anomaly consisting of a MITM type intercept.

Anura • June 24, 2015 12:34 PM

@name.withheld.for.obvious.reasons
@Question

Part two of this exercise is this: How do you know the NSA is not altering the posts so that they are confirming bad certificates that were created by the NSA? DUN DUN DUUUUUUUN!

CallMeLateForSupper • June 24, 2015 12:38 PM

@all re: claim that Churchill allowed the bombing of Coventry in order to protect Ultra. It is presented as fact, even in some books - notably in the first printing of "The Ultra Secret - but is false.

In communications, the Germans referred to a bombing target by codename, for obvious reasons. Most of the time, a codename began with the same letter as the real name of the target. Once the correlation became clear to the British, they were able to mount various defenses for the target. But the codename for Coventry happened to be "korn" (English "corn"), and that accident of languages is the reason that Coventry did not receive special defense.

TheArdentGlazier • June 24, 2015 12:55 PM

There is less cognitive dissonance than you might think. The reality is that, from the Government perspective, the statements can both be true.

Very few dispute that technical security needs to be improved in all systems. In their NOBUS view of the universe, however, containing Government-only backdoors isn't, in their view, poor security, but rather a matter of access control, which to them is a policy problem. As long as Government continues to view technical security separate from access control policy, they can speak out both sides of their mouths (from our perspective) and not be intellectually dishonest.

History, however, has not proven kind to this separation of function. Experience has shown that getting the implementation correct for simple secure channels with fixed keys is hard enough, and getting correct the implementation of exception, special cases, and keymat control for anything (much less access policy) is exponentially more difficult, not to mention the threat from bad inside actors.

The vast majority of people in Government, alas, don't view security as a continuous process but think of security as a widget you buy. I've given up hope trying to explain the distinction.

---

rgaff • June 24, 2015 1:16 PM

@Bruce bruce bruce.... you are so innocent and naive, it's so cute... :P

Regarding Admiral James A. Winnefeld's answer you said: "It's a good answer, and one firmly on the side of not introducing security vulnerabilities, backdoors, key-escrow systems, or anything that weakens Internet systems."

NO IT IS NOT.... And that's because of... spin and weasel words. You don't think he's using any? Why do you think NSA Director Admiral Mike Rogers was nodding in the background, yet seemingly contradicted him later on? Spin and weasel words! That's why! Don't think those only belong to the NSA and nobody else ever uses them.

Here's where his weaseling is located: He's not approaching it from the perspective of "this is right, this is moral, this supports human rights and the constitution, this is all that technologically makes sense".... no no.... he's approaching it from the perspective of "balance".... His own emitter example illustrates what I mean. There's no moral imperative that the emitter must live, it's not "right or wrong" if the emitter blows up or stays forever, there's no USA creeping toward dictatorial worldwide dominating naziism if it blows up (unless we just randomly blow up stuff we're NOT at war with, but a military emitter itself isn't so obviously intrinsically part of that issue like a whole country's general non-military population is). He's still treating people like the moral equivalents of emitters! We're his cattle. He's our God. We are his slaves. And this is the basis of his weasel words! Only they're not just weasel words, they're weasel sentences and whole weasel concepts, you see.

So, looking at this from another perspective: assuming you (Bruce) are NOT quite so naive....

then that means that YOU are using weasel words, you are spinning his answer as this great godsend when it's not and you know it's not...

In all cases, ACTIONS speak louder than words. When someone is up against the wall, and chooses what's right even if it's seemingly to their own detriment... THAT is what shows if they were really using weasel words/sentences/concepts/spin/etc or if they really meant literally what they said. So we'll see, eh?

NSA • June 24, 2015 1:46 PM

@@name.withheld.for.obvious.reasons

You are too paranoid, if we wanted something, we'd send our rubber hose crypto analysis team to your place.

ER • June 24, 2015 2:43 PM

I do not see a necessary contradiction here, perhaps it's not the backdoor, but the frontdoor (access) and data management he's suggesting.

@name.withheld.for.obvious.reasons • June 24, 2015 3:29 PM

@ Anura

> How do you know the NSA is not altering the posts so that they are confirming bad certificates that were created by the NSA?

Already considered the issue, an attempt to "test" applications based on in transit packets to a TLS session could work much like a "discovery" packet ejected from a Tor exit node. Using a combination of network abstraction (VPN, Tor, etc.), session layer translations (proxy, agent), and application proxies (translate raw packet, convert in-line data, and rendering tools) go a long way to "protect" a remote client during some sort of "network discovery" phase...

---

koanhead • June 24, 2015 4:25 PM

A back-door is just another door. The only thing that makes it a 'back' door is the fact that its presence is not advertised (which is obviated by the presence of a law or a rule that mandates the presence of such a 'back-door'.) It's not any more secure than a regular door (or API, or socket, or other access method) unless that regular door is inadequately secured- in which case a back-door is not needed. In fact, the very *existence* of a back door reduces the security of the regular door. To believe otherwise is to believe that obscurity adds a meaningful amount of security to a system- that is to say, it is to believe something that is known to be wrong in a world where a machine can automatically enumerate all the doors, hidden or not. It is to believe in magic.

Similarly, to believe that NOBUS can use a back-door is to believe in magic. I would need to see an existence-proof of a key that immutably binds to a singular identity, which is itself immutable- that is, a key that can't be stolen for an identity that can't be forged- in order to believe otherwise. I don't think such a proof exists, and ISTR a proof that no such proof *can* exist in principle, but I don't remember what it's called so I can't search for it to see if I'm full of cabbage.

Even though it's clearly the case that universal spying destroys infrastructure security, the 'tension' to which the General refers is a manufactured one. We aren't at war with China, nor with most of the others who have penetrated the US' networks. The actions we need to take to secure our infrastructure are the same regardless of war footing, because they don't depend on a specific enemy or specific attacks. Security that *does* depend on these things is destined to fail, so instead we secure against *classes* of attacks from classes of vectors. Infrastructure security is more important than the military's ability to strike a target in non-wartime situations, and at least as important in wartime situations. Weakening one's own infrastructure security is not a good answer, even in wartime. If it's an action that is clearly contemplated by a military authority in peacetime, then that indicates a military which is at war with its own infrastructure. Since this is clearly absurd, I can only conclude that the military authorities are befuddled about the situation, while the 'intelligence' agencies are focussing on their collection ability to the exclusion of their actual mission. I'm glad of NCBS' efforts to patiently explain the situation to them, but I would prefer either to have competent people in these positions or not to have the positions at all.

---

name.withheld.for.obvious.reasons • June 24, 2015 4:26 PM

@ NSA

> we'd send our rubber hose crypto analysis team to your place.

That's exactly what a few people at CIA said to me last year--you folks at the NSA need to stand in line. Oh, that's right--you think in-line is a compiler directive...too bad you don't know about Constitutional directives.

I'm surprised that NSA has a team comprised of all women...I thought NSA still maintains its misogynistic tech/geek culture. Non-male scientists scare the young male nerds...

Don't forget to tell the ho's to pack a few condoms--do I have to carry cash on me?

---

tyr • June 24, 2015 4:28 PM

Senior military are political animals, but they have to
trade-off between hanging on to their jobs and doing
what they think is right. You start giving bad answers
to the public and you'll be kicked out instantly. The
current POTUS is dumb as a fencepost about the military
so they have to be doubly careful. On the other hand

the US Navy has to have smart people at the top and they take their oaths to defend seriously.

Because the Pacific covers half of the planet naval top brass has to be able to think globally, its part of the job not and added frill.

You do not defeat an enemy by becoming a mirror image of what you oppose. The Axis monsters turned the Allies into monsters, a legacy we have not managed to remove yet.

The real danger of the intelligence communities is in their being able to indulge their paranoid fantasies about the world without checking them against reality once in awhile.

Once again it is about power and the model of humans they use. If you're an evolved primate and seen as such by the institutions of your society it is a far different perspective than when they assume you are a fallen from grace spirit trapped in a body which will be discarded as soon as possible. The idea that the peeping Tom is the best model for Net governance is something that needs serious consideration. Do you want to live in that world with your communications system viewed as weaponry, as a battlefield, and the lurkers of every nation and corporation spying on you every moment. One morning the catholics of France got up and massacred every non-catholic they could find. How does that fact figure into the world-wide panopticon we are building ? That's why he's assuming balance is a lot better than making Rodgers job easier to do.

---

gordo • June 24, 2015 7:17 PM

@ tyr,

> How does that fact figure into the world-wide panopticon we are building ?

As you say, it's a matter of scale and how long a group can get away with it.

As far as I can tell, human beings have a unique ability to twist whatever belief system is handy to justify their actions. If needed, make one up.

---

gordo • June 24, 2015 8:03 PM

Let me clean up that last sentence
in my previous comment to read:

If needed, one is made up.

Justin • June 24, 2015 10:28 PM

@ all

I kind of like Bruce's steadfast stance against weakening or subverting security.

In my opinion, we need our intelligence agencies to do the work they do, but at the same time at some point we also need to be able to say to them, with respect to our own privacy and our own security, "Thus far shalt thou come and no further." The Fourth Amendment says it very well.

As technology advances, it enables ever greater surveillance, but it also enables defenses for the privacy-minded individual against that surveillance. The U.S. government may be worried about "sovereign citizen extremists," but, well, we are citizens, not subjects (like the British.) The Magna Carta was a charter granted by a king, but the U.S. Bill of Rights is a recognition of unalienable rights, with which we are endowed by our Creator.

There needs to be a balance to those rights, that we hold them dear, and also hold for such necessities as the rule of law and intelligence for national defense, which are necessary to secure those rights for the people.

@name.withheld.for.obvious.reasons

> I'm surprised that NSA has a team comprised of all women...

That's an odd statement to make. It reminds me of a time years ago, when my computer was being hammered by a botnet. There were a few girls' names tried as ssh logins, and then immediately after that in order, the words "team," "deep," "inside." Seemed spooky at the time. Now I wouldn't read too much into stuff like that. You sound a bit misogynistic yourself. And the idea of the NSA sending a team of women to your place, I don't know if that's your dream or your nightmare, but it doesn't sound much like reality to me. Do you really believe that comment came from the NSA, not just somebody being snarky? Maybe you shouldn't let yourself be taken advantage of by these strange women, that is, if they're not just in your imagination. Maybe they're not really from the NSA.

Maybe you *want* to believe certain things very strongly. But let's not lose touch here... The certificates reported in this thread match what I have. But neither wordpress nor php is secure. Some of my posts have been subtly altered, too. Nothing so much that I would call attention to it. Could be somebody found a way in to the blog and is just having some fun. Always think of mundane explanations, first.

name.withheld.for.obvious.reasons • June 25, 2015 1:30 AM

@ Justin

Yes, the post was a bit snarky but not so close to funny (laughing with a nod of concern) and wanted to throw a few stones using a bit of tongue and cheek.

And what, are you kidding? People in technology, the more technocratic types, demonstrate a world view that is very condescending that is flavored with a whole bunch of misogyny. Institutional and cultural misogyny is prevalent in the United States--both in academia and business. Both men and women exhibit prejudices and less that subtle biases in the form of language, gestures, and symbolism that reflect "learned" socio-cultural behaviors. Men in technological fields tend to have an enhanced view of their social-political/cultural egalitarianism. I am tired of seeing men subtly, with a wink and a nod, denigrate women in ways too numerous to characterize here.

Has anyone here, the regulars--you know who you are--genuinely engaged other female professionals in a honest and peer level conversation? Better yet, when did you take some personal time to met with young girls, teens, or women in a academic/professional setting in an apprenticeship, guild, class, or mentoring style?

Maine lobster cakes • June 25, 2015 2:00 AM

@ gordo

"As you say, it's a matter of scale and how long a group can get away with it."

Getting away is just a matter of keeping a secret. However, great works don't complete themselves. It requires a great amount of effort and, manpower and resources. As such historically has show, great effort to complete but little effort to maintain. It becomes a game of projections. Thus, the race is to the top of the pyramid.

Andrew • June 25, 2015 4:42 AM

Excellent article about surveillance and encryption:
http://www.techrepublic.com/article/defending-the-last-missing-pixels-phil-zimmermann/

Andrew • June 25, 2015 4:54 AM

French understood that they should improve their surveillance capabilities after they have been spied
http://yro.slashdot.org/story/15/06/24/2359219/france-up-in-arms-over-nsa-spying-passes-new-surveillance-law?utm_source=rss1.0mainlinkanon&utm_medium=feed

Just like in nuclear race, now every country assemble hackers team up to the point where soon

everything cripples or get stuck.
We will soon have on our devices a couple of spyware from nsa, a couple from russians, some others from Chinese and others smaller countries, all these will overlap and get permanent system crashes/failures...

Clive Robinson • June 25, 2015 5:38 AM

@ Andrew,

> We will soon have on our devices a couple of spyware from nsa, a couple from russians, some others from Chinese and others smaller countries, all these will overlap and get permanent system crashes/failures..

The most anoying thing about this is we know how to reduce the problem a lot.

There are various *nix based OS's out there that run off of CD/DVD ROMs. The base system is on the ROM the user brings their own "personalisation" via another piece of media (I once built a system based around two DVD ROMs and two floppy drives that worked well). You power up reboot between sessions and use different personalisations depending on what you are doing. Provided the base is reasonably secure and updated relatively frequently it stops most malware and other attacks from being persistant.

The downfall of this was the likes of Micr$haft and the idea of "patch every thing after release". MS NT based OS's are designed in such a way that putting them onto ROM whilst not impossible is very difficult, they also lacked important features, with the result it makes discovering malware more difficult.

Further the MS "release before ready" policy and thus it's "patch everything after release" policy forces "Write must be always enabled" on users which is just about the best gift you could give to malware writers of all levels.

This patch/write enabled problem became so endemic in the industry that when flash memory became available hardware manufactures went down the same route. So now some malware is written not to hide on the hard drive platters, but in the flash of the hard drive controller where it is effectivly impossible for all but the most skilled of engineers to find and deal with.

Thus steping back 20 years in "hardware" enables a much more secure system to be built than using modern "open to all comers" hardware.

Hopefully some "forensic hardware tools" will be repurposed to take our modern promiscuous hardware back to more chaste behaviour, thus qnabaling us to reduce or eliminate much of the malware that currntly abounds.

---

albert • June 25, 2015 9:58 AM

@Clive,

Is it possible to have a CD/DVD based system with a flash drive for the personality module? How hard is it to detect malware in a flash drive?
.
Sometime ago, the USAF* came up with a Linux OS called Lightweight Portable Security that fit on a 2GB flash drive. (They used a PCMCIA card for the 'secure' communications) It's purpose was to allow their people to use 'unsecured' computers and public networks, not necessarily for military business.

Having a 'fresh' install on every boot is a great way to go. Of course, 'pre-installed' malware in the computer itself is another can o' worms,

.
...
* I know, I know, they can have their own malware in there...

John Galt III • June 25, 2015 12:50 PM

@Clive Robinson

Let me help with that line of thinking:

We already have in all of our network devices a couple of hardware backdoors from nsa, a couple from mossad, a couple from russians, some others from Chinese and maybe other smaller countries, all these are working well right now, but anything can happen, and it will...

Clive Robinson • June 25, 2015 5:38 AM

@ Andrew,

We will soon have on our devices a couple of spyware from nsa, a couple from russians, some others from Chinese and others smaller countries, all these will overlap and get permanent system crashes/failures...

Misunderstanding? • June 25, 2015 2:45 PM

https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis

Justin • June 25, 2015 4:04 PM

@ Misunderstanding?

Who knows? People have all sorts of ideas. The idea of a team of women from the NSA armed with rubber hoses to beat secrets out of name.withheld, well, I didn't think of it first. From the article:

> Although the term is used tongue-in-cheek, its implications are serious: ...

Clive Robinson • June 25, 2015 5:32 PM

@ John Gault III,

> We already have in all of our network devices a couple of hardware backdoors from nsa...

Not all devices, for my sins I've built one or two that are not. Not that you would want to use them, because they are very very low --by modern standards-- bandwidth at sub 100Kbs (yes little 'b' bits nit big 'B' Bytes).

Then there is older kit I suspect most AT "cheaper net" BNC cards are immune if originally bug free as they are ROM based. You can quite easily get a pair of those running back to back with an ARM, MIPS or even 68xK 32bit single chip micro.

Some of the RTL 10Mbs chips used on the NE cards are old enough not to have been back doored and can be picked up on the "redundent stock" market if you shop around.

Also anoying as the "rip off chips" are they are actually less likely to have "state level secret back doors" for the simple reason they are made "to the data sheet" often using "stolen/knocked of libraries" by criminals with every reason to avoid having dealings with state LEAs or IC. Thus "my enemies, enemy is my friend" even if he does not know it.

For the realy paranoid I still have circuit diagrams for "Cambridge Ring", early twinax and RG53 "Token Ring" and "Ethernet" using TTL etc chips, that I designed with others back in the early 80's. I also have the design for a PDP11-70 card along with full source code for Unix that was running on it with BSD network code on fan fold print out (provided mice have not chewed it in the past twenty years or so since I stuck it in a crate in the garage). Much of this stuff is also poping up on the Internet on "historic computing" sites. For instance about a year ago I found a site with the source not just for a P-Code interpreter but an OS and networking code...

Whilst it might be a bit of an effort to get it up and running on modern microcontrolers it would be a lot less difficult than starting from scratch.

Oh and for those who like dead tree tombs there are the two "TCP Lean" books and the uCOS RTOS networking extensions. Further early editions of books by Stevens et al have SLIP and PPP implementations in them.

The game at the end of the day for the fortunate few is to be "more diverse" than the IC agencies can be, and put non visable instrumentation on stuff to watch out for "funnies on the line".

Clive Robinson • June 25, 2015 6:06 PM

@ Justin, Misunderstanding,

> The idea of a team of women from the NSA armed with rubber hoses to beat secrets out of name.withheld, well...

The rubber hose or monkey wrench treatment is actually very much a last desperate "when all else has failed" tactic. Not least because it's a grossly inefficient and ineffective use of resources, but you also have the "what do you do with the body issue". Whilst people do disappear in the West the numbers are very small compared with population size, and the more prominent the target the more likely it is to attract very unwelcome attention to the IC.

The slightly more likely attack would be a "black bag" job by independent contractors, where the "stored secrets" are targeted for "in place duplication". In the event of discovery it's fairly easy to cover up as a bungled burglary, especially when using modern "duplicate to off site" technology or more modern versions of what's in the TAO catalog. Again it's in effect a "last resort" tactic against a significant target, not just because of the "tip off risk" but also because it's inefficient and often ineffective.

Thus as difficult as it might appear to us, remote information attacks and interdiction for information or physical implant attacks are more efficient and in the case of interdiction often more effective as it's effectivly a "trusted insider attack" at the highest level.

Nick P • June 25, 2015 6:32 PM

@ Clive Robinson

I used to recommend Oberon System for that reason. Whole OS with documentation, code, safer language, compilers, and relatively easy porting. Unlikely to be subverted but will have vanilla vulnerabilities. A2 Bluebottle for the GUI one. Unlikely that it will run on a straight up microkernel but should run fine on older PC's, servers, and boards repurposed for them.

---

tyr • June 25, 2015 8:43 PM

@ name withheld

I have regularly engaged with girls and women in what was described.

I have also read the history of science and academics and seen exactly how women have been treated by the so-called lords of creation.

Anyone interested can look up Ada Byron, Grace Hopper, Emmy Noether, Lise Meitner, Rosalind Franklin, Mileva Einstein, and others. Females need to know about them and Men need to stop bullshitting themselves about their place in the world.

The whole misogyny slant to moderns is a stone age myth
perpetuated by the followers of a particularly nasty
demiurge modelled on the male ego excess of the primate
animated seedpod. The old females made the decisions
and guided primate groups while the lord of creation
was humoured in his delusions of grandeur. The first law
of intelligent behavior is do not bullshit yourself.

John Galt III • June 25, 2015 9:29 PM

@ Clive - Thanks for the high-quality comments. Generally in line with my own thinking, although I don't have that depth of hardware portfolio to draw on. The spook rat bastards reflashed my BIOS and hard drive microcontrollers and I need one or more good utilities to clean them up.

Nick P • June 25, 2015 9:43 PM

@ John Galt III

Why do you think "spooks" went after your BIOS and hard drive microcontrollers? Only one's I know that do this are Five Eye's via NSA's tools. They're quite reliable and stealthy. How did you detect this and why do you think they're attacking you specifically?

---

name.withheld.for.obvious.reasons • June 26, 2015 12:41 AM

@ tyr
Good to hear! We, defenders of freedom and liberty, must aspire to not only the challenges of the day but must well spend time learning, teaching, and exercising wisdom. A life that exemplifies an honest treatment of others and gives without taking must be shared. Too often I see men treat women with a veiled level of fairness and we often cannot see the "institutional/cultural" biases that drive the behavior. I'm not claiming any "skill", just refusing to walk through life a professional politician; deaf, dumb, and blind.

Men have not championed women in the physical sciences to a degree that is measurable. I started a company back in the late 1990's that included a charter to make real people out of nerds. After starting up it became obvious that women were not being "represented/served/allowed" in technological enterprises, at least not in any numbers. I hate going into meetings and looking around the room and seeing a bunch of over-weight middle aged men that have more hubris then reason.

I vote for Abigail Adams as the female for the new 10 dollar bill. And I agree with what others have said, she could easily replace Jackson on the 20 dollar note. What I regret is not having a career that included working with someone like Grace Hooper...

Today there are few examples of courage, fidelity, honour, and integrity irrespective of gender.

We need to nominate and promote these people where they can be found.

Halo Man • June 26, 2015 1:20 AM

@ John Galt III

"We will soon have on our devices a couple of spyware from nsa, a couple from russians, some others from Chinese and others smaller countries, all these will overlap and get permanent system crashes/failures..."

THE real fight isn't on our devices. Its at the network interconnects. Routing equips with backdoors, from them, taking your traffic on a never ending loop around. Slowing it all down.

---

fajensen • June 26, 2015 1:57 AM

@rgaff

Admiral James A. Winnefeld, may very well be openly expressing his complete honest and truthful beliefs, and yet, his orders - not his beliefs - is what decides what he will actually do. That is how the military works. Since they do not actually get to act according their own beliefs, military people can be more honest than most folks ;-).

John Galt III • June 26, 2015 7:04 AM

@Nick

They got me because I am a TAILS/TOR user. Their full spectrum dominance doctrine requires them to defeat anyone exercising First Amendment rights in an unapproved way. I noticed the attack because two computers on the same day stopped in the middle of a windows boot and rebooted, something that I have not seen before or since. They were being booted after long sessions running TAILS.

@Halo Man

I believe that the real fight is over hardware backdoors on all networked devices. The fact that this is rarely discussed, e.g., by Greenwald, Lee, Snowden et al. makes me suspicious that their work is the most amazing imperial psyops mind-fuck ever. For as long as you run your traffic on their networks, you will be under their thumb. I don't want to be in the position of also running their spookware on "their" hardware - the AMD/Intel boxes with their custom-ordered and essentially undetectable hardware backdoors - as well as the Israeli, Chinese, and Korean backdoors. Having my email traffic take a few minutes longer doesn't bother me, particularly if the content hasn't been compromised. I believe that running PGP or equivalent on an air-gapped machine and heavily filtering the traffic to the internet-connected machine will produce a secure channel. I do like the idea of defeating traffic analysis, because I'd like to be able to protect legitimate business intellectual property.

The spooks have a unique carrot/stick combination with Congress and politicians around the world. They can dish the best dirt on both them and their opponents. The spooks have the best insider trading information in the world, bar none, and Congress are exempt from insider trading laws.

There is a lot more to say on many related topics, but this will have to do for now.

Light Bulb • June 26, 2015 8:16 AM

The great thing about splitting light with a prism is that it is impossible for any victim to know that their communications data is all being collected from the second beam of light for later prioritising and also any possibly required brute forcing and exploitation to be handed off to the Super Brute Decrypt Server Cluster Bunker.

Good security for everyone is not actually a problem contrary to the claims by some in Intelligence, it is a necessity. If they really need to access the communications of someone they think may be an enemy agent, Intelligence agencies have all kinds of cables and hidden devices they can plant in or near the targets home that allow for much more comprehensive surveillance and an accurate assessment, once they have followed the law of course and obtained a proper warrant to do so.

The bulk collection of totally unrelated communications of the general public is not only completely inefficient, tying up huge amounts of resources for no gain, but it also greatly increases the complexity of analysing large data sets while decreasing the accuracy of any understanding that may formed in any given situation.

Figureitout • June 26, 2015 9:04 AM

John Halt III
--Here's this guys investigation too, it takes a lot of tests and time to be sure you got some very bad malware on your machines.
http://www.reddit.com/r/lowlevel/comments/3aulbd/a_pastebin_of_the_smbios_structures_and_acpi/

Me • June 26, 2015 9:19 AM

Notary Lookup for: www.schneier.com:443,2
Browser's Key = 'a8:e7:d6:39:cc:26:27:0a:c1:07:3e:b3:b3:5f:63:f7'
Results:
Quorum Duration: none
Notary Observations:

Notary: perspectives8.networknotary.org:8080
ssl key: '7f:06:03:da:9e:a3:1d:22:10:00:5a:84:d5:06:aa:3c'
start: 1397265864 - Fri Apr 11 2014

```
end: 1435109184 - Tue Jun 23 2015
(438 days)

ssl key: 'a8:e7:d6:39:cc:26:27:0a:c1:07:3e:b3:b3:5f:63:f7'
start: 1435109185 - Tue Jun 23 2015
end: 1435325140 - Fri Jun 26 2015
(2 days)

Notary: heimdal.herokuapp.com:80
ssl key: '7f:06:03:da:9e:a3:1d:22:10:00:5a:84:d5:06:aa:3c'
start: 1429110055 - Wed Apr 15 2015
end: 1435244446 - Thu Jun 25 2015
(70 days)

Notary: nine-eyes.herokuapp.com:80
ssl key: '7f:06:03:da:9e:a3:1d:22:10:00:5a:84:d5:06:aa:3c'
start: 1401951869 - Thu Jun 05 2014
end: 1435129283 - Wed Jun 24 2015
(383 days)

ssl key: 'a8:e7:d6:39:cc:26:27:0a:c1:07:3e:b3:b3:5f:63:f7'
start: 1435129284 - Wed Jun 24 2015
end: 1435302070 - Fri Jun 26 2015
(1 days)


Notary: perspectives2.networknotary.org:8080
[ No Results ]
Notary: perspectives3.networknotary.org:8080
[ No Results ]
Notary: perspectives4.networknotary.org:8080
[ No Results ]
Notary: perspectives5.networknotary.org:8080
[ No Results ]
Notary: perspectives6.networknotary.org:8080
[ No Results ]
Notary: perspectives7.networknotary.org:8080
[ No Results ]
```

---

albert • June 26, 2015 12:08 PM

@John Galt III,

Does your Windows OS run stand alone, or in a virtual OS?

.

...

Nick P • June 26, 2015 3:46 PM

@ fajensen

"may very well be openly expressing his complete honest and truthful beliefs, and yet, his orders - not his beliefs - is what decides what he will actually do. That is how the military works. "

Excellent point. It's similar to what I say when explaining why otherwise good soldiers might do terrible things when serving in U.S. military and why I remain free instead. Another facet of this is the information given to military people. As it flows down the chain, it can get both deceptive and all-enveloping for those listening. Soon, they might be repeating it themselves esp if it seems to match what they see.

@ John Galt III

That's interesting. That would suggest they think you do more interesting stuff than merely anonymous browsing or a widespread attack on the platform. Can't be sure which. Regardless, I once postulated here that they might just start firing their 0-days at the computers of those using Tor or other security. The counter was that they're too careful and use the tech too sparingly. Yet, what you're describing might be exactly that.

Unless they have done something simpler: poison a page or service with a lower-priority exploit that Tor/TAILS users are likely to download. Corrupts the browser, downloads BIOS attack, installs rootkit, and survives reboot.

@ Figureitout

That poor guy just wants a Windows 8 box and vanilla FOSS router that can survive nation-state attack. If he succeeds, Microsoft will offer to buy his intellectual property given they haven't accomplished this after millions in investments. I image we're going to see a similar status in the future unless he discovers air-gapped, retro-computing.

Figureitout • June 26, 2015 9:39 PM

Nick P
--Well lots of work gets done on windows and foss firmware on routers are fun and interesting, it's hard to do big-time work on small micros with vi. For making and locking up small files and small experiments, good.

As usual toolchains and chips are still too large an attack surface, it's just massive work to do over all that cleanly and not go same path dealing with old problems same way...

Think serial data diode off 2nd or 3rd node of hardened router and modem that can't be remotely flashed, with strong firewall, and at least one pc with wireshark from a "throwing star" is doable and would catch a lot of sludge and sloppy attacks. Still compiled malware needs to open the file in a sandbox. This is only for file transfers, otherwise hardware goes in a safe. Targeted attacks need traps for confirmation, this is where you can "change the game" and get some revenge...

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

E-mail Address:

URL:

□ **Remember personal info?**

Fill in the blank: the name of this blog is Schneier on ___________ (required):

Comments:

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

Preview Submit

← Hayden Mocks NSA Reforms Baseball Hacking: Cardinals vs. Astros →

Schneier on Security is a personal website. Opinions expressed are not necessarily those of Resilient Systems, Inc.