SECURITY NOW!

Transcript of Episode #438

NSA's ANT: What We've Learned

Description: As promised last week, after catching up with another crazily busy week of interesting and fun security news, we take a deep dive into the amazing NSA ANT documentation to learn what we can of the NSA's field capabilities. What we learn is chilling and interesting, though not entirely surprising.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-438.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-438-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. All the security news, including a Microsoft Patch Tuesday update, plus an in-depth look at what the NSA is doing with its Project ANT. It's all ahead. Stay tuned on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 438, recorded January 14th, 2014: NSA's ANT.

It's time for Security Now!, the show that covers your security and privacy online with this guy right here, the only guy who could see right into the hearts and minds of the NSA, Mr. Steve "Tiberius" Gibson, working in a now undisclosed location somewhere in the Western hemisphere. What a cup of Joe that is. Wait a minute, you're not using your Contigo mug, Steve. What is that?

Steve Gibson: Oop. Oop, nope, Contigo, Contigo's right here. I just did a refill with it. Actually I've had some tweets from our listeners who have thanked us for the recommendation. They've purchased the Contigo mugs or thermoses.

Leo: I did, too. I love them.

Steve: I know. And it really - sometimes I'll knock it over. It's not a problem because it really does seal perfectly. You can drive in the car with it and open it only as you need to drink. No, it's perfect. It's like an adult sippy cup.

Leo: Not "like," it is.

Steve: It is.

Leo: You know, Wired writer Steven Levy, the guy who wrote, of course, "Hackers," one of the classics of the computer age, and also a book that I really like, and I don't know if it's as well known, about crypto, called "Crypto"; right?

Steve: Yeah.

Leo: Which was a great book he wrote about 10 years ago. He writes in Wired this week that, even when he did "Crypto," he really tried to get the NSA to cooperate and talk, and they would not. They refused. They just wouldn't have anything to do with him. But he just recently went right into the heart of the beast at Fort Meade and got interviews, in fact, even talked to the director.

Steve: They've given up. They've given up, basically.

Leo: Well, he says it's two reasons. He says, "The protocol officer told me that 'Crypto' had fans at Fort Meade," that they liked his book about cryptography. But also of course the new - and we saw it with the "60 Minutes" piece, the new attempts at PR. One of the things he got from his interviews - and he talked to the NSA's General Counsel Rajesh De; he talked to the head of private partnerships, Anne Neuberger, and Richard Ledgett, who hosts the Media Leaks Task Force, which is a task force designed to handle the Snowden leaks in the media; and he even talked to General Alexander, the head of the NSA. But one of the things he came away with was the absolute hatred of Edward Snowden that everybody shares in the NSA. He is really viewed within those walls as a total, utter traitor.

Steve: Yeah. Well, and, I mean, today's show is, as I promised last week, what we've learned from that amazing Der Spiegel set of slides about the NSA ANT program; basically, what have we learned about the NSA's field capabilities. And I do partly feel guilty talking about this, although it's out there now in the public domain, so it's no big deal. I'm just reading the specs and adding some engineering spin and understanding, some clarification. And the fact is we would hope that this is the way our tax dollars would have been spent to create this kind of technology.

But here it is, laid out, with all of their code words and their requirements, and this is how it works. And oh, my goodness, the beginning of this talks a little bit about - I mean, the beginning of our coverage on the podcast today discusses the two major big-iron router companies, Cisco and Juniper. And it's just very clear that, if the NSA ever has brief physical access to the router, it is forever changed in a way that favors the NSA's ability to penetrate it at will. It doesn't look like they can do that remotely. So I was breathing a sigh of relief. I looked, I mean, I really read these docs carefully. It looks like that Chinese telecommunications company - is it Huawei or Huawei?

Leo: Huawei.

Steve: Huawei. There's a "remote upgrade capability," unquote.

Leo: Yeah, upgrade, that's the word, upgrade.

Steve: Yes, being used in a way that wasn't intended. But I can completely understand the NSA's fury at essentially having the king's wardrobe revealed as completely as it has been. We do know, apparently, that something's going to happen on Friday of this week. The Obama administration is gearing up and is going to give some sort of presentation about how they intend to change the NSA's charter. And top of the list is rolling back or changing the way this metadata is being collected by the telecommunications carriers. Some have felt that maybe it would be held by a third party. But then again, that's been regarded as just a window dressing around the problem, and that probably the way - what the people who've been watching this and caring about privacy are hoping is that it will simply become incumbent upon a major carrier to archive their metadata for some length of time and then be able to respond to queries for specific individuals. And so the NSA would send out a blanket request to all of the carriers for a specific network and some degrees of separation. And every network, every carrier would then perform a database query on their own metadata that they are themselves keeping sole and separate and then return that data for the NSA's aggregation. So it'll be interesting to see. But today on...

Leo: Is there a sense that these, as we get into this ANT segment, that these Der Spiegel slides are part of the Snowden cache of slides?

Steve: That's a good question. I don't know. As I said last week, I wanted to be very clear that this feels different to me. This is sort of the interior workings, the cogs in the system that we would hope our taxpayer dollars are being spent to develop. Some of this stuff is extremely cool, and I'm looking forward to being able to explain what I've learned from studying that document because, I mean, it's just - it is really neat, Spy v. Spy-level technology. But that's - and I don't even think that Edward probably had a problem with this. So I would say no. I think this is other leaked documents. But I don't think this is part of Snowden because I don't think Snowden would have had a problem with this kind of stuff. This is what it makes sense for our taxpayer dollars to go to, where we want...

Leo: So where did the slides come from, then?

Steve: I don't know. But maybe it's part of it, if it was just all stuff he grabbed. But I don't think he'd have a problem with this. He had a problem with the breaches of the Constitution which he arguably felt was going on. I mean, this is juicy stuff; but this is just, like, wow, the kind of stuff we would hope is happening. And now we've got real details.

Leo: As Bruce Schneier said, this is retail spying, specific to a person or a group, as opposed to the mass collection of data that we've been upset about.

Steve: Yes. For example, now I know the oft-mentioned VGA cable that for $30 allows the NSA to somehow exfiltrate what's on the screen, I know exactly how that works now. And it's not like a Y connector.

Leo: Ooh, interesting.

Steve: You beam a 2 GHz continuous wave radio beam at it, and it reflects back a modulated signal. And it runs for years without any tending. So anyway, we'll talk about that toward the end of today. We've got a bunch of stuff to talk about: Target's PoS PoS systems...

Leo: That's point of sale, I should clarify.

Steve: Ah, well, one of those PoSes is. A bad and ultra-potent next-generation DDoS technology, which is getting a lot of press, that I want to talk about. The growing size of the RSA Security Conference boycott. We've got to some back to port 32764 because actually there was last week the readout on it that I hadn't seen, that I was immediately - it was brought to my attention by our listeners. So we have to talk about that because it turns out it is in fact a super-potent backdoor. There's a new security tool on Kickstarter. Net Neutrality took a little hit this morning, but it's not completely dead yet.

Leo: No, in fact I wouldn't mind talking a little bit about what that means. I don't think we've really got the full story there.

Steve: Yes, we will. And of course a bunch of random miscellaneous stuff that I think people will find interesting, and what we've learned about the NSA.

Leo: What we continue to learn about the lovely NSA with the Explainer in Chief, Steve Gibson.

Steve: So this is the latest possible second Tuesday of the month, since we all know that January 1st fell on Wednesday, just missing Tuesday. You can't have a Tuesday that occurs any later than the 14th, which is what has happened now. And it's interesting, it'd be interesting to go back a few years and look at the January Windows updates and see if they're all small. Because it occurs to me, it's not like Windows is suddenly better in January than it was a month ago in December.

Leo: No. Hackers take the holidays off, just like the rest of us.

Steve: Well, no. It's not the hackers, it's Microsoft.

Leo: Oh.

Steve: Because they're the ones who are having to patch the problems. So my point is the problems are still there. We just didn't get many patches this week because there wasn't much time.

Leo: They were busy.

Steve: Yeah, exactly. So we have four sort of yawners. None of them are critical. Those we'll probably get next month because Microsoft's back at work now, fixing the problems. Each of the four affects various subsets of Windows, Microsoft server platforms, and Office. And so no emergencies. Update, say yes, reboot your machine, and go about your life. And that's it. Although it is worth mentioning that April 14th continues to approach, that being 83 days away and the expiration of XP SP3's security updates. So, and that's about right. A few months from now I think I'll be ready to move to Windows 7. I've made peace with Windows 7. I like it.

Leo: Well, it's about time, Steve.

Steve: I get to skip over the disaster that was Vista. And, boy, we had some fun talking about, I remember, the security architecture mistakes that Microsoft made with Vista.

Leo: Raw sockets and all that.

Steve: And needless to say, I won't be going to 8 after 7, nor 8.1, .2, .3, .4 or anything else.

Leo: Well, the next one, we now know from Paul Thurrott, is Windows 9, codename Threshold, and that will be 2015. So you can...

Steve: Yeah, but it sounds like it's still an amalgamation of their old...

Leo: Oh, it's 8. It's 8+.

Steve: Yeah, yeah. So I'm just going to be camped out on 7. I think the world is probably...

Leo: You're not alone, I know.

Steve: ...camped out on - yeah, exactly.

Leo: They are bringing the Start Menu back.

Steve: Good. I hope they get rid of all the tiles, too. And if you get rid of that nonsense - just give me 7, you know, just keep fixing 7. It's just fine.

Okay. So somehow last week I forgot to mention, just because it was, like, it was too early in the dual-week cycle that we were catching up from, the massive Target breach, which...

Leo: I thought you were just bored with it. It's just another example; right?

Steve: Well, there didn't seem to be much news. And even today the only piece of information we got - first of all, Target did disclose an additional 70 million customers' personally identifiable information.

Leo: I like how the exploit grew. So it started with 40. Then they said, well, no, it's 70. Then they said, oh, you know what, there's no duplication, or little, between the 40 and 70. So it's really 110 million accounts.

Steve: Yes, yes. And what they're blaming it on, and this is where I got to the PoS PoS terminals, is malware infecting their point-of-sale terminals.

Leo: Isn't that interesting. Hmm.

Steve: Yeah. And so that's clearly a targeted attack. Now, interestingly, within the same timeframe, dating from about mid-December, turns out that brick-and-mortar, as they're called, Neiman Marcus stores have been reporting something similar. So it's not their online problems. But Neiman Marcus is talking about an - we don't have a size yet.

Leo: Oh, on PoS? Oh, interesting.

Steve: Yeah. Well, some - it's that customers who shopped at Neiman Marcus for a period of about a month, somewhere around mid-December, at their physical retail locations are having problems. So there may be a group of hackers out there who have been doing some reverse-engineering of point-of-sale terminals. And then lord knows how you got it in all these Target stores. I mean, it'll be really interesting to see whether we learn much about it. There's just, still, there's a lot of reporting of the fact of this event, but no real background information that would interest me and our listeners, like, ooh, how was this done? How did it actually happen?

However, we can make up for that because there is a new DDoS flooding technology in town, and it is nasty. To give our listeners sort of a sense of the history and scale of this, because denial-of-service attacks are something I have a great deal of prior interest and experience with, the original attacks were the so-called SYN flood - S-Y-N, short for synchronize, is the name of the packet which is first sent when a client wants to connect to a server. And if you don't use the operating system's regular TCP connection mechanism, but if you actually generate the SYN packets yourself using a technology known as raw sockets, then you can send the SYN packets off to a server at basically whatever your line rate is, as fast as your bandwidth will allow, because the packets are very small. So you can get many of them in a short period of time.

And what happens is the receiving server tries to initiate connections. Assuming that all of those packets are valid, it creates some state on the server, in the server's TCP/IP stack, to say, oh, somebody wants to connect to me. And so it allocates memory, and it kind of gets ready for a connection. And it eventually sends an acknowledgement, a SYN/ACK, back, which is its own synchronize, with an acknowledgment of the SYN that it received. And what happened in the early days is that, without too many SYNs coming in, just these fake packets, you would collapse the server. It would be unable to establish all of these pending connections and just crash. So, and sometimes very embarrassingly. Sometimes it just kind of went offline and stopped being able to accept any more. And that caused a denial of service of that service that was being offered.

So then hackers got a little more clever. They used what's called a "reflection" attack. They would send a SYN packet to some other server with a spoofed source IP. That is, they would change where the SYN packet appeared to originate. So it would go to that server, and that server would acknowledge the victim. So it would send that SYN/ACK, that second packet, that answering packet would not come back to the sender, the true sender. It would go to the target. And the reason that was clever is that, when the server that thought it was answering an initiation of connection didn't get an answer back, it would send it again, and again, and again, typically at least four times. So this was a bandwidth amplification attack. You send one small SYN packet with a bogus originating IP, source IP, to a legitimate server, and it would send four acknowledgements before it would give up. So that amplified the attack strength by a factor of four.

Next, we went to a so-called "DNS reflection" attack, which has been very problematical in the past. The idea with DNS is a very small query can generate a very large reply. And the two attacks we've talked about first were TCP attacks. DNS, as we know, uses UDP, the datagram protocol, instead of a connection. So you send a UDP DNS packet at a DNS server with, again, a spoofed source IP. And it sends a big response, it thinks answering the query; but you've placed the target's IP as your source IP, so the DNS server sends much more data back to the victim's server - again, a substantial bandwidth amplification attack.

So now we have a new protocol in the game. It uses the Network Time Protocol, NTP, and it is also a reflection attack. NTP goes over port 123, and it's built into Windows. All of the *nix OSes have it. Interestingly, it uses a 32-bit - is it 32 bits? I think it's, yeah, a 32-bit time. For some reason I'm sure there's also a 64-bit component. Anyway, the point is that something is going to wrap with network time protocol in 2038. And even though the Y2K problem with the year going from 1999, wrapping around to zero, didn't cause a huge problem, if there's any old equipment still, that is still using the original 32-bit NTP, we're in trouble because sometime in the year 2038 that 32 bits wraps around to zero. And that may be the most significant 32 bits of the time protocol. I haven't looked at it for a long time.

Anyway, so the Internet is covered with network time protocol servers. They're everywhere. It turns out there is a command which has actually not been supported in the NTP software since around March of 2010. Two years, well, now, what, four years ago, yeah, update myself. Four years ago, nearly, it was understood that the so-called "monlist" command was a bad thing to have. It was subject to abuse. What can happen is a 234-byte packet, so 234 bytes in a UDP packet, can contain the so-called "get monlist" command. An attacker sends that to any identified network time protocol server on the Internet, with a spoofed source IP, again, with the IP set to the victim of this attack. A "get monlist" command will return the IP addresses of the most recent other network time protocol servers that it has had access to, up to 600 of them.

Now, six IP addresses fit in a packet, so that's a hundred packets. So, first of all, we have a packet rate amplification, one to a hundred. The attacker sends out one packet to an NTP server, and it generates a hundred packets in return. But it's also a bandwidth amplification attack because they're maximum-sized packets. And in fact this 234-byte small packet requesting a network time protocol server to list the 600 most recent other servers it's had contact with can result in over a 48K reply. It's a 206x amplification. And unfortunately the Internet is full of big-iron network time protocol servers.

Many big routers on the Internet just offer NTP as a public service. So they are very well connected and have very high bandwidth connections. As a consequence of this, what we are beginning to see now is 100Gb DDoS attacks. And the key is, since we're getting a factor of 206x bandwidth amplification, a relatively small set of, for example, a relatively small botnet can be used to send these "get monlist" commands, spraying them out over the Internet to known and identified NTP servers, which then innocently generate a reply and get a huge scaling of bandwidth. So this is the attack that we're seeing more and more.

Now, the US CERT has been talking about this for a while. As I said, this command was understood to be a problem four years ago. But as we know, if it's not broken, it often doesn't get fixed on the Internet. And it's the case that there will probably always be old-iron, functional, never-touched routers with network time protocol running on it. It's easy to find them because they all respond to port 123 over UDP. So anything that scans the Internet can find network time protocol servers. Then you send it a monlist command, see if it responds. And, if so, you add it to your attack directory. It's going to be tough to mitigate this new attack.

Leo: That's, of course, the worst thing you could tell me, but go ahead. Because what, now, how do you normally mitigate an attack? What did you do, for instance, when you got DDoSed? You throw bandwidth at it; right?

Steve: Well, for example, the early DDoS attacks used ICMP, Internet...

Leo: We should know that. Internet...

Steve: A management protocol. Internet...

Leo: Ping. It's ping.

Steve: Well, yeah, it is. Well, but actually it's many different things.

Leo: Internet Control Message Protocol.

Steve: There we go, yes, Control Message Protocol, thank you. Ping uses it. Traceroute uses it. Many different - it's like low-level plumbing. The key is, though, you don't absolutely have to respond to a ping. And many servers don't, specifically because it can be used as a way to map the interior of a large ISP's network or a corporate network. So, for example, ping is often blocked at the network boundary. Old-school Internet gurus are annoyed by that because part of the original spec says that every Internet endpoint should respond to an ICMP, to a ping, because it's really useful for, like, figuring out what's gone wrong with the 'Net, why it's not working. I mean, the ping command is a critical tool in the repository of commands.

Leo: It's gone the way of finger, I'm afraid.

Steve: Yes, exactly.

Leo: That command is no longer used.

Steve: So, for example, so if somebody were flooding you with a ping attack, you just - you ask your ISP to please drop all the ping packets at their border that are aimed at you, and then they won't get through and be able to flood your bandwidth. But the problem with these monster, 100Gb attacks is that you need to - if you tried to filter the attack near you, then 100Gb would be getting to the point of the filter and probably crash all the incoming links. So you really need a huge ISP who's able to filter the attack at all of the ingress points in their large network before the bandwidth gets concentrated down to a single location.

Leo: You can do it upstream where there's a big pipe, as opposed to...

Steve: Precisely.

Leo: ...downstream where it could block the pipe. And you can no longer do it by IP. You mentioned it, but you can't do it by IP address because of raw sockets. You can't ignore SYN requests, or you'd be offline anyway. So these are very effective.

Steve: Well, and so that's, yeah, so that's one of the - if there is, to the degree there's an advantage, it's that this is over this UDP...

Leo: This could be ignored.

Steve: Right, UDP 123. So in the same sense that, if you had to, you could ignore incoming ICMP, you could just say, okay, I'm just not going to allow - I don't need external Internet NTP service. I can get that from my own ISP or just set my clock correctly. But the problem is this is being used, apparently, to blast gaming sites off the Internet in specific instances where it's embarrassing to the gamers or to the sites that are offering that service. So another powerful tool in the hands of hackers.

Leo: It's going to get worse. I've been thinking about it. I was just talking with Mike Elgan about it, actually. I think it's going to get worse because what we've created, unfortunately, is a whole generation of people who live in their basements, who don't really have a direct connection with people. So they don't really understand fully what the personal impact - you think technically, I think psychologically - what the personal impact of this kind of attack is. And I think in many cases these are unempowered people, anyway. Whatever, they're nerds, they're outcasts. And so this is a way for them to get power. And they don't really understand the real consequence, real-world consequences of their actions. And so as these tools - and they're script kiddies, right, because these tools - they're not building these tools. I think it's going to get worse, I really do. It was script kiddies attacking you; right? There was no real reason.

Steve: Well, the one attacker, whose first name was Michael, who I did find and track down, was certainly that. He didn't really know who I was.

Leo: He didn't know what he was doing; right.

Steve: Someone told him something about me, and so he said, oh, I'm going to blow Gibson off the 'Net.

Leo: I have power.

Steve: Yeah.

Leo: And it's sad. I mean, I don't - I just don't know. I just feel like we're going to see a lot more of this. A lot.

Steve: Yes. I'm afraid that's the case. And the beauty of the Internet, the power of the Internet, is this notion of autonomous routers where we just drop packets into this incredibly interconnected network, and they...

Leo: They're breaking something gorgeous.

Steve: It is, it's a beautiful, fabulous solution. But the nature of it fundamentally creates this weakness, which hackers are increasingly clever about exploiting.

Leo: Yes, kids, you can tear the wings off a fly. It might make you feel better, but it's not - you may see a beautiful flower and tear the petals off. That might make you feel better, but you've destroyed something gorgeous. You've destroyed a free and open Internet. Well done.

Steve: Yeah. There was, in the actual book "Under the Dome" that Stephen King wrote, I can't give it away, but we're reminded of how, as children, some of us would get a large magnifying glass for Christmas, and it turns out that you were able to focus sunlight from a large surface down into a small spot. And ants kind of snap, crackle, and pop when they are exposed to that kind of heat.

Leo: Mm-hmm. That's kind of a spoiler right there, if you just think about it. And I haven't even read the book, and I have a feel I know what you're talking about. Continuing on.

Steve: So the list of security speakers who have formally announced that they're going to boycott this upcoming RSA security conference at the end of February has reached nine and is continuing to count upwards. So, I mean, they're...

Leo: No surprise.

Steve: People are - no, it's really not a surprise. It'll be interesting to see how it actually goes. Certainly there are people who have strong commercial interests in presenting to RSA. And so they represent companies that are saying, "You're going. We don't care." But there's also a community, much more sort of the black hat sort of group, who are able to say, forget this, I'm not going to speak to RSA. I just want to show my outrage at the idea that they would have knowingly, willingly, allowed the NSA to influence them and accept money in return, if that's indeed what they did. We still have no formal proof of that. But, boy, talk about a nearly smoking gun.

Leo: Yeah.

Steve: One other little blurb crossed my attention in the last week, which was that another former well-known ex-NSA, really well regarded, 32-year employee, who was highly placed within the NSA - and that's William Binney. He famously resigned in 2001, so about 13 years ago, after 32 years being with the agency. He was regarded as one of their best mathematicians and code breakers in NSA history. And in fact he wrote some of the software code that's being used today to spy on Internet traffic around the world. He spoke a few months ago at a conference in Switzerland. And what he had to say I thought was interesting and hardly surprising. He said, apparently from first-hand knowledge, said that, "The NSA knows so much that I can no longer understand what it has."

Leo: That's what happens. You gather everything...

Steve: It's classic information overload.

Leo: And yet I think they know that. And the reason they do it is they presume, probably correctly, that, well, eventually we'll be able to figure it all out. Or when we need to we'll be able to figure it all out.

Steve: Right. Thus that monstrous data storage facility in Utah where, you know...

Leo: Let's just save everything in case.

Steve: Exactly, yeah. Crazy. And I mentioned at the top of the show that apparently Friday we are going to get some new directives from - we, the NSA and the country. The Obama administration is expected to disclose what it intends to do in terms of issuing some directives. So I'm sure I'll have a note about that on this podcast next week.

There was a really interesting piece in the Security Watch column of PCMag.com. Max Eddy wrote, on January 8th, about, well, the title of this column was "What It's Like When the FBI Asks You to Backdoor Your Software."

Leo: We kind of - we heard a similar story when we were talking with, oh, what's his name, the guy who killed his email service.

Steve: Oh, Ladar.

Leo: Yeah, Ladar Levison.

Steve: Levison, yeah.

Leo: On Triangulation, what it's like when the FBI comes to call and says, hey, would you mind if we just - just give us the keys, and then we won't have to bug you again.

Steve: So a female security researcher, Nico Sell, N-i-c-o S-e-l-l, was the subject of Max's story, and I'm just going to share two pieces of his report. I tweeted the link to this this morning. And I'm sure if you googled "What It's Like When the FBI Asks You to Backdoor Your Software," you can find the whole article. But he said: "At a recent RSA Security Conference" - well, now, okay, it had to have been a year ago because they're around this time each year. The 2014 conference is end of February, so probably around this time last year - "Nico Sell was onstage announcing that her company, Wickr" - W-i-c-k-r - "was making drastic changes to ensure its users' security. She said that the company would switch from RSA encryption to elliptic curve encryption, and that the service would not have a backdoor for anyone. As she left the stage, before she'd even had a chance to take her microphone off" - and I was thinking, whoops, you'd like her not to be mic'd anymore when this occurs - "a man approached her and introduced himself as an agent with the Federal Bureau of Investigation."

Leo: So boneheaded. Boneheaded.

Steve: Yeah. Speak into the mic. "He then proceeded to 'casually' ask if she'd be willing to install a backdoor into Wickr that would allow the FBI to retrieve information."

Leo: Now, is this - people are hearing this through the microphone?

Steve: No, no, no. I think it was just an aside that she hadn't...

Leo: That would be cool.

Steve: Oh, it would be very cool.

Leo: Let me turn on my mic. So would you ask me that again?

Steve: Hello, this is the FBI. Would you be willing to install a backdoor in your software?

Leo: Oh, man. But for all they know, they don't know; right? She's got a mic on.

Steve: Yes, yeah. So apparently this is a common practice. The story goes on to say: "This encounter, and the agent's casual demeanor, is apparently business as usual as intelligence and law enforcement agencies seek to gather greater access into protected communication systems. Since her encounter with the agent during the RSA conference, Sell says it's a story she's heard again and again." Quoting her, it says: "It sounds like that's how they do it now," she told Security Watch. "Always casual, testing, because most people would say yes."

Leo: Sure. Most people are patriotic.

Steve: I wonder, though, if that's still the case. We're hearing, for example, stories of the recruiting that the NSA routinely does on university campuses, and there it's not the way it used to be a year ago any longer. They're getting an awful lot of flak from students who...

Leo: Oh, yeah. I saw the recruiter was, like, chased off, right, by a mob of angry students.

Steve: Yes, yes. So I skipped a bunch of this interesting story because I love this one paragraph from Max. He said: "It was clear that the FBI agent didn't know who he was dealing with because Sell did not back down. Instead, she lectured him on topics ranging from the First and Fourth Amendments to the Constitution, to George Washington's creation of a Post Office in the U.S."

Leo: Ben Franklin, but okay.

Steve: Huh?

Leo: It was Ben Franklin, but okay.

Steve: Oh, yeah. The article says George Washington. But anyway, so she said: "My ancestor was a drummer boy under George Washington. Washington thought it was very important to have freedom of information and private correspondence without government surveillance."

Leo: I can just see the agent going, oh, god. Oh, lord.

Steve: So that's a no?

Leo: I'm thinking you're not interested. Would you like to have a cup of coffee, then? We don't know. I mean, let's not project too much. This guy could have been just some dude, some dufus. We don't know.

Steve: Well, I know some FBI guys. And, I mean, I'm completely sympathetic to the situation they're in. There are bad guys who are using this technology and using encryption. And I'm not bothering with any encrypted texting because I'm just arranging what time I'm going to meet Jenny this afternoon. But certainly bad guys would be wanting to use this recent explosion in secure messaging. And in fact, in response to my tweeting this article, I got a bunch of people who said, hey, what do you think about Wickr? Is it secure? And I said, I'm sure it is. I haven't looked at it closely. My favorite is Threema, T-h-r-e-e-m-a, which you and I have talked about, Leo. That's the one with the cool little three blips, and you get either red, yellow, or green, depending upon the level of verification that you've made about the other person's identity. And I know how that technology works, and I know it's secure.

So, I mean, I don't mean to be laughing at our law enforcement. I recognize they have a legitimate need to solve this problem. And it's tough. And a lot of this is backlash. This is backlash from us having discovered that our government is doing everything in its power to fulfill the charter they were given, and they interpret that as meaning collect everything from everyone and try to find a needle in a haystack, if it's there.

Leo: It's amazing.

Steve: I saw another little piece of interesting miscellany which was that the GSM digital encryption, which is of course so common for cell phones, was deliberately crippled from the beginning. Its team of designers wanted to use 128-bit keys. And it was backlash from the British government back in the early '80s that wanted to be able to crack it for surveillance purposes. So they wanted it, again, they wanted it to be good enough that individuals couldn't afford to crack it, but easy enough that they could. West Germany, on the other hand, wanted strong keys to keep East Germany from snooping. So there was a bunch of back-and-forth. And the key length was first cut in half, from 128 bits to 64. But still that was felt by the governments to be too strong. So under, as I understand it, pressure from the British government, and we talked about this once a long time ago because I remember mentioning this bizarre fact, the last 10 bits of the key are always set to zero.

Leo: I say, would you mind terribly? We just want to set those last few bits to zero. Be so much more aesthetic.

Steve: And of course that renders it - I'm sure that they said we want fewer. And the crypto guy says, well, no. Our algorithm, we've already cut it in half.

Leo: To 64 bits, yeah.

Steve: And they said, well, just set 10 of them...

Leo: Do you mind? Ever so [indiscernible], just put [indiscernible] to zero.

Steve: Rendering it as a 54-bit effective...

Leo: Let's not forget that really people do this because they're patriotic. They want to protect their nation. They want to protect their - they want to cooperate with law enforcement. And it's not a bad instinct, I think.

Steve: Yes. I agree.

Leo: That's a natural instinct.

Steve: Yes. I mean, if - yes.

Leo: They're on our side.

Steve: Yes.

Leo: It's not like the Russkies came to us and asked us to do that.

Steve: Now, port 32764, which we talked about last week, is such a problem that I have created a bit.ly shortcut to GRC's own port scanner.

Leo: Oh, good. So people go right to it.

Steve: So that everybody can check it. You absolutely have to: bit.ly/port32764, all lowercase, just bit.ly/port32764. That will immediately check that port on your router. You need it to either be closed or stealth, not open. Open is the problem. Now we know, because it actually had, last week when I talked about this, already been reverse-engineered. There was something happening with GitHub where I was unable to download the file. It was saying that it couldn't deliver files of that size right now or something. Anyway, I finally got it. There are, from the reverse engineering of the firmware - and as I mentioned last week, firmware, there's a whole culture that is reverse-engineering router firmware, where they take the file, they unzip it, essentially.

It uses LZMA compression, so they decompress it. And then they run reverse-engineering tools on it, figure it all out. That was all done. And what was found is as bad as it could possibly be.

Thirteen commands have been identified which will respond if that port is open. Command 1 is a dump the configuration. You send a Command 1 to that port, and it dumps this huge blob containing things like the admin username and password and the WiFi preshared key. So complete access to your router, if someone can get that. Command 2 allows them to specify a configuration variable. Command 3 allows them to set a configuration variable. Command 4 writes any changes to nonvolatile RAM. Command 5 turns bridge mode on. It wasn't clear exactly what that meant. Command 6 shows the measured Internet speed. Command 7 gives them a command shell prompt. Yes, from which you can then execute any Linux-style command of your choosing. Command 8 writes a file. Command 9 returns the version. Command 10 returns the modem's router IP. Command 11 restores the default NVRAM - which, it happens, turns WAN admin back on. So if the user had properly disabled wide area network administration, as everyone should because why would you ever want that...

Leo: Why would you need it, yeah.

Steve: Yeah. The first thing that happens is you issue a Command 11 to restore the NVRAM and restart the router. Now WAN administration is on. Now you give a Command 1, which dumps out all of the data, including username and password. And I don't know whether restoring the default nonvolatile RAM would reset the username and password to the router's default. Maybe it does. If not, Command 1 gives you the username and password. So then you login remotely, and you've got full HTTP-style admin access to the router. Command 12 reads some blocks, and this guy was unsure exactly what. And Command 13 dumps the nonvolatile RAM to the internal file system and commits it.

So, I mean, this is the definition of a backdoor. So again, bit.ly/port32764. That's, as I mentioned last week, four fewer than exactly half of 64K, 32768. And so this is four back from that midpoint. Make sure you and everyone you know has this port closed. You should get back either closed or stealth. If you get back open, then you need to deal with it immediately.

Cisco has issued a statement saying that they will have a firmware update for their affected routers by the end of the month. In their statement they said: "An attacker could exploit this vulnerability by accessing the affected device from the LAN side interface." Remember that few routers did have this exposed by default on the WAN, on the Internet wide area network side. Huge number, like I don't remember, it's like 30 different models have been identified that had it on the LAN side. And so Cisco is noting that: "An attacker could exploit this vulnerability by accessing the affected device from the LAN-side interface and issuing arbitrary commands" - just like we enumerated - "in the underlying operating system. An exploit could allow the attacker to access user credentials for the administrator account of the device and read the device configuration. The exploit can also allow the attacker to issue arbitrary commands on the device with escalated privileges." Yeah, the privileges of the administrator.

So this needs to get resolved. But mostly, our listeners need to make sure it's not exposed on the public side because I'm sure scans are already occurring to find that port open, just as they were when we discovered that Universal Plug & Play was open as widely and commonly as it was over on the WAN side. So this needs to get fixed.

So I know you've got some stuff that you want to say about this, and I'm glad. What happened was the news this morning was that the Washington, D.C. Court of Appeals rejected the FCC's proposal for their implementation or their rulings on 'Net Neutrality. And the Boy Genius Report story was gloom and doom. But Tech Dirt did an article which explained that it's not as bad as it looks.

Leo: Right.

Steve: That essentially what the D.C. Court of Appeals was saying was that the FCC didn't have the authority under the provisions that they were attempting to exercise it, but that they probably do have the authority in some other - by taking some other approach. So it wasn't that it was dead forever, but that they just didn't ask right.

Leo: The issue has been all along an issue of jurisdiction, pure and simple. So of course we want 'Net Neutrality. You and I and anybody who's sensible listening to this show loves the idea that - really, I don't even like the term "'Net Neutrality" because it doesn't say it. What we want is no discrimination on the 'Net. We want bits to be equal. We don't want an Internet service provider to say, well, I'm going to let YouTube go through. But TWiT, I want to slow them down. We want - we don't want discrimination. That's how the 'Net was designed. The FCC has in its mandate, as part of their broadband plan, they also want to fight for 'Net Neutrality.

The issue is, and this is what Verizon - this case was a lawsuit by Verizon. Verizon asserted the FCC doesn't have jurisdiction. For instance, they don't have jurisdiction over TWiT. It's a podcast. They have jurisdiction over my radio show. It's a broadcast. In this case, the issue is, is a broadband service provider a common carrier? So the FCC regulates common carriers - telcos, radio stations, stuff like that. And up to now, the FCC has not said that the broadband - and there's good reasons for them not to say that the broadband providers are not common carriers. Even though Verizon is a common carrier in wireless telephony, they're not in wireless data. So that's what the court is saying: According to your own rules, you don't have jurisdiction.

However, the court says the FCC does have the right to oversee the Internet. So they're not saying no. The court said that the 1996 Telecommunications Act, quote, "vests the FCC with affirmative authority to enact measures encouraging the deployment of broadband. It even said that the agency reasonably interpreted the law to empower, to promulgate rules governing broadband providers." But - and that was the good news. The bad news is the way they're doing it, they don't have jurisdiction.

Steve: Right.

Leo: But the attorney who represented the FCC did say, well, we know now where our jurisdiction lies. I'm still worried about the FCC because you know the new chairman is a former cable company executive. That bothers me a little bit.

Steve: Well, yeah. And I'm worried that there's any thinking or logic to the idea that, well, consumers have a choice in how we get our broadband connectivity. That's absolutely not the case.

Leo: Right. And that's because of the FCC, frankly, that awarded, in effect, duopolies, monopolies to the cable company and the phone company. Now, in this case we're talking about wireless Internet. We're talking about Verizon is - we're talking about cell phones. And even Google, even Google said that broadband should be treated differently on a cell phone carrier than it should be on a cable company, the thinking being that there are some actual physical constraints to the bandwidth available on a cell phone, right, because they have to get the data out to each head end individually. There's lots of technical reasons why it might not be regulated the same way a cable company is. So this is a deeper, much deeper question than just this decision. This decision doesn't change really that much. It gives, in some ways, the FCC more direction about how it should proceed.

Steve: Right. Right, it's like, okay, strike one. Try again.

Leo: Right, right. And the court seems to me, and I'm not an expert, to be supportive of the idea of 'Net Neutrality. The judge who wrote the decision said Internet service providers can damage players on the edge.

Steve: Good.

Leo: So that he recognized that there is a public interest in protecting neutrality on the 'Net.

Steve: Yeah. I think there's only one way this can ultimately turn out, and that's the way we believe it should; that even if it stumbles, and there are some mistakes made along the way, I just think the idea of allowing an ISP to discriminate in any fashion about the way you're connected to the Internet is doomed to failure, as much as they may want to.

Leo: Well, and they protest. I mean, Verizon says, oh, we don't want to harm the Internet. But look what AT&T's doing with their subsidized broadband plans. They're saying, hey, if Netflix wants to pay your broadband bill, then we won't count it against your cap. But if TWiT doesn't, then we will. And that's what I mean by 'Net Neutrality isn't a good way to express it. Internet discrimination is the way to do it. If you don't pay us, if you don't subsidize our customers' broadband bill, then, I'm sorry, we can't - we're going to have to count it against the customer. So I do expect the FCC to get involved in this.

The court, you know, the judge further wrote: "The Commission (FCC) has adequately supported and explained its conclusion that, absent rules such as those set forth in the Open Internet order, broadband providers represent a threat to Internet openness and could act in ways that would ultimately inhibit the speed and the extent of future broadband deployment." The Court sent a very clear message: Don't do this. Now, in this particular case you're going to have to do it differently, FCC. But we're watching you, you broadband providers. That's good.

Steve: Yeah. That was some good language.

Leo: Yeah, it's a good decision. I don't think it's a bad decision. But it doesn't mean we're done. You know, we're never going to be done.

Steve: So I have two links which I just decided to make a "techie bonus" for our show note readers.

Leo: [Laughing]

Steve: Because I don't know what else to do with them, but I just couldn't throw them - I couldn't throw them away.

Leo: It's our bonus round.

Steve: Yeah. So the first is "A (Relatively Easy-to-Understand) Primer on Elliptic Curve Cryptography." And this was written by Nick Sullivan, who is over at Cloudflare. And so it's the blog.cloudflare.com. And then his more recent one, the one that really caught my eye, was very interesting: "How the NSA May Have Put a Backdoor in RSA's Cryptography," and he says, "A Technical Primer."

Leo: I like this Nick Sullivan guy. We've got to get more. We've got to get him on our shows. He's smart.

Steve: Yeah, it's good. It's very smart. He knows his crypto. He's got nice pictures with everything. But there's nothing I can really do with it on the podcast except to aim people at it. So anyway, so it's in the show notes, if anyone is interested. Or you can just google "How the NSA May Have Put a Backdoor in RSA's Cryptography," and I'm sure Google will take you to it because all that text is in the URL.

Leo: We should mention that Cloudflare is one of those companies that provides DDoS protection. You run your stuff through Cloudflare. And if suddenly there's bandwidth hits, they'll take over.

Steve: Right. I ran across an interesting Kickstarter that I thought certainly some of our listeners would be interested in. An individual is putting together a universal bootable Windows password reset key. So for anyone who...

Leo: Oh, what a good idea.

Steve: Yeah. So it's all integrated into a neat, looks like a little key, a USB, essentially, memory stick. You can buy the software only if you want, once it's finished; or you can purchase the actual hardware key. And the idea would be you stick it into any Windows machine, I think it runs through all of them up through 8.1. And as long as you don't have full-disk encryption - that would defeat it; but, unfortunately, still very few people do - this allows you to go to a screen. He shows some screenshots which are a little unnerving. I've actually done this before myself. There was a - actually one of my Starbucks regular morning friends is a schoolteacher who needed some things done that her district was unwilling to do. Actually it was just to get some of her equipment working. So I needed to be able to log in with administrator privileges, but she was locked out of that. So, well, it turns out it's not very hard to do.

But, yeah, you could see it's just a matter of putting the key in, boot the machine, and up comes a dialogue. You select the account you want to log in as, and it does it for you. So anyway, so you can just google "password reset key." And this is not something you have to pay for. There are free, like, CDs and software kits and things available to do it. I just think it's very neat that this thing will all be prepackaged on a key that you just stick into a Windows machine, turn it on, and you're in. So certainly useful for people who are doing recovery and forensics, or if you get, like, who knows, used computers that you want to be able to get back into in order to recondition them or something. So I wanted to point our listeners at that.

Let's see. This is totally random, also. And I mentioned this already to you, Leo. I wanted to tell our listeners that the TSA PRE program is an incredible win. When I was flying up over the holidays with Jenny to Northern California, she had TSA PRE, and I didn't. And she was, like, sitting at the gate waiting for me to catch up for half an hour. Essentially what it is, is it's a time machine that sets you to pre-9/11. There's no one in the line because no one else is clued in to this. So you go immediately to security. You're in your own security area. And all you do, there's no body scan, there's no physical pat-down, again, it's like pre-9/11. All you have to do is take metal out of your pockets in order to go through the magnetometer door, and that's it. You don't have to take your clothes off, I mean, nothing. You just need to be able to go through the magnetometer like in the old days. You can sign up online. I did.

And in fact, when I came up for the New Year's Day with you, Leo, I already had TSA PRE qualification, and I experienced this for both directions of my trip to Northern California. So, oh, my goodness. Even if you only fly, like, once a year, as I do, to my way of thinking it's absolutely worthwhile. There's an interview that you need to have, and it costs, like, $85 or something one-time fee to cover their expenses. They just need to see you in addition to filling out the form. And you do need proof of citizenship, but a valid birth certificate or passport. You need more than just identification. And then you can get this. So for anyone who hasn't take the jump...

Leo: How much?

Steve: I think it's $85, if I remember right.

Leo: And how is it - when we talked, you hadn't yet been interviewed. How was the interview?

Steve: Actually, that's tomorrow. I don't quite understand how it is that this appeared on my boarding pass. And then I half figured that maybe it wouldn't scan. But I got green lights at - so maybe they were able to do enough from the form I filled out. I filled out the online form, scheduled an appointment for, like, a month and a half in advance - this was after Christmas, but before New Year's. And I was surprised when I printed out my Southwest Airline's boarding pass that said TSA PRE on it. And I was really delighted. And it worked. So because there's a chance it may have, like, been a fluke, I'm going for my interview tomorrow because I don't ever want to lose this. It's just too valuable.

Leo: It is 85 bucks. And does it expire, or...

Steve: I don't think so. I think the one-time fee, just to cover the cost, and also to set the bar. I think they don't want to get flooded with people doing this. They'd like to say, well, it's going to cost you $85. We need to see you. And then it'll happen. I can't explain why I got it prior to the interview. Maybe I'm in some database somewhere where I'm on some level pre-cleared. Who knows? But I'm doing the interview tomorrow anyway because, oh, my goodness, it was a win.

Leo: I'm enrolling right now, Stevie.

Steve: It was a real win. A brief SQRL update. I mentioned I'm still at it. That's what I'm doing. We've just been benchmarking the Scrypt, the password-based key derivation function. You'll remember that one of the things we're deliberately working on is making brute-force attacking, user password cracking, extremely difficult. And so, again, all of the crypto code is done. We're just nailing down the protocol for exactly how to delay the recognition of the password in such a way that GPUs, FPGAs, and ASICs cannot be employed in a reasonable fashion to accelerate that process. And that's happening.

And the other trick is we want to be able to have this be a dynamically adaptable process so that, for example, on your cell phone, even if you have an underpowered smart phone and you wanted to use this, you would type in your password, and it would show you a progress bar and take five seconds just for you to authenticate. The point is we've made it take five seconds because we want a brute-force technology that is super resistant to someone guessing all possible passwords. And the idea is, if you type your password incorrectly, five seconds with a nice progress bar isn't too long to wait to prove to your phone that you are you because of course your phone, what SQRL does is absolutely empower your phone to represent your identity on your behalf. So it's necessary for us still to prove that we are who we are, until we get, like, bulletproof biometrics or some other authentication approach to use. So that looks like it's pretty much nailed down, and then I'm going to continue coding. So that's what I'm doing before I return to SpinRite.

Speaking of which, I just found - actually this was dated the 21st of December - a nice note from a Ron Kurr who's in Auburn, New Hampshire. And I thought this would be of interest to our listeners because many people are having very good experiences with SpinRite in VirtualBox. Virtual Box is a free virtual machine technology that is also cross-platform - PC, Mac, and Linux. And he said: "Steve, I've stumbled upon something that I think others might be interested in, but I wanted you to clarify something first.

"A little context seems appropriate. I'm a Linux weenie and noticed that most of the directions for getting SpinRite to operate within VirtualBox were all Windows-based. Having an hour to spare, I decided to try to get SpinRite to run under VirtualBox on my Linux i7. In a nutshell, Linux makes it much easier to do than Windows does, and I was able to run several SpinRite virtual machines concurrently as I did real work. As an experiment, I tried using the SpinRite/VirtualBox combination with some of the USB hard drives I carry with me to and from work. Normally, SpinRite doesn't see the drives, so I could never exercise the disks like you recommend. But the SpinRite/VirtualBox combination saw it like any other hard drive.

"So here's my question: Is SpinRite able to use the same deep scanning techniques with a virtualized USB drive as it does with a standard SATA drive? I know in the past you have recommended that people extract their USB drives from the enclosures and attach them directly to their motherboard's drive controller so SpinRite can perform its deepest scans. Does VirtualBox's drive controller emulation actually allow SpinRite to treat the USB drive as if it were a native SATA drive? Or is the emulation just tricking SpinRite into thinking that it's doing a deep level scan when, in fact, it is not? I'm very curious to hear your thoughts. Thanks, Ron Kurr."

So, as I said, many people are having success with SpinRite in VirtualBox. And in fact, it is a way to get SpinRite running on Mac drives on Mac machines natively, essentially, because it solves the one problem SpinRite 6.0 has, which I've already resolved in 6.1 here in the lab and will be incorporating into 6.1 as soon as I'm able to get it finished. And that is that the Mac uses a USB emulation that does not emulate the PC's hardware, and VirtualBox provides a BIOS that solves that problem, that does emulate the hardware by virtue of being a virtual machine. So SpinRite runs just fine on a Mac inside a VirtualBox.

Leo: Interesting.

Steve: I can't really answer Ron's question definitively because I'm not sure we're ever going to get the same level of communications through a serial interface like USB, with a physical connection. That is something I'm putting off exploring until v6.2 of SpinRite, just because I don't want to slow down the release of 6.1 any further. So I'm going to get all of the low-level, super high-speed SATA stuff operating, both with the older IDE and the newer AHCI hardware, and release SpinRite 6.1 like that, and then tackle immediately the USB side. I'm a little concerned that it may not be possible to communicate through the serial interface and do things that SpinRite does for some of its really, really, like, down-to-the-hardware, low-level stuff. There are ways, for example, that SpinRite is able to truly read a sector which is unreadable.

But I'm afraid that the USB interface is always going to just, I mean, it's going to be - it's a barrier that nothing could bypass, that it just won't allow me to issue those commands to the hard drive. If I'm limited to read and write, then I can't do the fancy things where I'm taking advantage of the entire ATA vocabulary of commands that are available. So the good news is you can run SpinRite in many more places under VirtualBox, and it will likely do as much as is possible, for now. And then 6.1 will push it further, and SpinRite 6.2 will - and actually 6.1 will eliminate any need for VirtualBox stuff because it'll run natively on the Mac and on Windows and Linux and so forth.

Leo: I just - a couple of things. Five years on the TSA PRE.

Steve: Oh, really.

Leo: Yeah. And I've just looked at it, and you have to be able to go to - what are these? They're not in airports? What are these centers you have to go to?

Steve: Yeah, I'm going to Long Beach, which is the closest...

Leo: The nearest one to me is Sacramento. There's nothing in San Francisco, San Jose, or Oakland. So it's not convenient.

Steve: You know, Leo, I would fill out the form and just see if you get it. I got it.

Leo: They say if you have a criminal record, you shouldn't bother.

Steve: Don't bother giving us - don't bother submitting, yes.

Leo: They say no refunds.

Steve: Yes. Although you're able to pay with a credit card, and you take it with you to the interview, so that you don't have to pay in advance. And I got PRE somehow.

Leo: I'll fill it out. They say don't do it if you don't have - you can't get to a center within 120 days. So that gives me four months. I guess worst case I'd drive to Sacramento.

Steve: I agree. I've driven to Sacramento, and it's not fun.

Leo: Somebody's saying, and somebody mentioned that they got it through Delta, that some air - maybe through frequent flyer programs some airlines will facilitate it. I'll have to look. Time to talk about ANTs.

Steve: Okay. So my goal here, you know, last week we had fun running through the crazy terminology which the NSA uses. I would almost think that they have some random word-pairing software that takes two words, like as if you had a big bowl...

Leo: I think that's the case. It's a code generator.

Steve: Yeah, exactly, except that some of them really do, okay, it's like BananaGlee. Okay, it's not clear at all what that has to do with exfiltrating data from target networks, which is what it does. So that one, oh, and JetPlow, same thing. But there are some where there may be just a coincidental naming, or maybe the person who requests a code word for their project is able to sort of say, well, it's kind of about this and this and this, and the selector helps you, comes out with something a little more memorable. But we have some terminology we need first.

"Interdiction" is the terminology they use for physical access. So anything requiring interdiction means that they had to visit the hardware and, like, physically do something. So, for example, installing that VGA cable that I mentioned at the top of the show, that would be interdiction into the system, where they would presumably sneak in at night and swap the VGA cable with their own. Nobody would know the difference. It all works fine. Except that, as I mentioned, in this case there's a passive RF ultra-high frequency reflector which modulates itself based on the video signal going down the cable, and it doesn't itself radiate any RF energy.

So that's clearly where the technology has gone now. The ANT documentation is full of these passive RF reflectors, the idea being that they can, if they need power, they only draw a few microamps so that the battery's own self-discharge, it just loses its charge over a couple years, that's a greater effect than the actual drain on the battery itself. So for all intents and purposes they run for many years without ever needing to have the battery changed, and they do not radiate. So all of the movies we see where someone, like, sweeps the room to check for bugs, well, that doesn't work here because there is nothing that a receiver can receive.

It's not until somebody deliberately decides now they want to obtain information from some distant location, they send a focused beam of radio frequency energy targeted at the location of where this passive re-radiator is. And while it's always been running, it's not until it gets illuminated by this coherent wave, that is, a non-modulated RF energy, that it then reradiates back to the receiver. The receiver picks that up and mixes the outgoing signal with the incoming signal. And Leo, you'll remember this from your ham licensing days. It heterodynes the reflected signal with the outgoing signal, and it uses the sum and differences of sines. There's a law there where you're essentially multiplying two sine waves on a log function to get the sum and difference. The sum will be like, if you've got a 2 GHz carrier, the sum will be up at 4 GHz of the two. And the difference is what you really want. That will be the original frequency which is doing a modulating of this passive reflector. And that's, for example, a video signal that is going through the cable.

Then they have other technologies that are enumerated in this document that, for example, allow them to capture the audio, if it's a bug. One of these things is a passive bug. It is, like, half an inch in size. And I noted in there that it talks about its COTS, which is the acronym for Common Off The Shelf, and they specifically say so that there will be nothing tying it back to the NSA. So it uses just generic components. And so if someone did discover it, it's like, you know, what's this? And there's nothing to tell them where it came from.

So in these cases they do need so-called "interdiction" in order to plant this initially. But once done, these things can run for years. They do not give off any radiation themselves. And of course, if they were radiating actively, that would inherently mean that they were consuming more power. So this is part of the cool architecture that they've got where the thing doesn't generate power, so it can't be found. And it will only generate a signal when it is itself essentially being illuminated by this remote source of detection. They call it radar. It's not technically radar. It's just a 1 to 2 GHz beam of RF energy that this thing modulates and reflects.

Then the other term that they use is an "implant." And implants can be hardware or software. And that's just something implanted into another device. They're big on persistence, meaning that it survives a reboot or OS upgrades and so forth. There's even mention of their ability to have an architecture of exploits where, if they install this in a router down at the lowest level, like down in the BIOS, yet the router's software, the OS running on it, they don't have an active exploit for yet, their persistence allows them to automatically reacquire access to the router if at some future point that router is upgraded, that is, the router's OS is upgraded to one that they do have an exploit for. It'll automatically recognize that and then exploit that OS during boot. And it talks about how it's able to modify the in-memory image on the fly of Cisco and Juniper network routers, which are pretty much what glues the Internet together at the high end.

So these documents talk about, as I was mentioning before, this BananaGlee is a portion of sort of an exploit stack. In the work I was doing, trying to understand this, I ran across some terms that I didn't know. For example, one was "DNT Payload." And I thought, well, what is DNT? So in googling for that, I discovered that there was another source of this information that has been put together, sort of a coherent document that runs through all of the acronyms we know of, over and beyond what has been revealed by this NSA ANT.

So I created a bit.ly shortcut. The bit.ly shortcut I created last week was all lowercase, bit.ly/nsa-ant. This one, the new one, for another cool page, I called nsa-ref. So bit.ly/nsa-ref, obviously short for reference. And this is an incredible page of this NSA jargon. And through that I learned that DNT is actually a commercial company, Digital Network Technologies, that is a subcontractor of the NSA. So there's a commercial company that is generating these technologies for the NSA's use in doing this. And so, for example, this BananaGlee acronym says - it's on that nsa-ref page - a software exploit made by Digital Network Technologies (DNT).

Leo: Some of this stuff is for sale.

Steve: Yes.

Leo: I can buy, for $50,000, SomberKnave, a software-based malware that bridges air gaps. Holy cow.

Steve: Yeah. In fact, one of these things, I don't think it's SomberKnave, I've got it in my notes down below, is an air gap-bridging USB cable, very similar to the VGA cable. So it looks like a USB connector on each end. And hidden in the connector on one end is a radio transmitter. I don't remember if it's this passive RF reflector technology or not. We'll get down to that in a second. But, yeah, you're right, Leo. And these are...

Leo: What you really want is to rent, not buy, because you can't buy it, the Typhoon HX is a GSM base station router used to collect call logs from targeted phones. You administer it with a laptop via SMS. Standalone unit a mere $175,000 for a four-month rental. So who makes this? Who rents this? Is this DNT, as well? It's crazy.

Steve: Yeah. So all of this hardware. Some looks like it's - I don't know if DNT is software. They seem to be software people. I think the NSA has a bunch of their own hardware people because it's looking like this ANT division supplies the TAO, T-A-O. That's the Tailored Access Operations.

Leo: Here's the beauty part. You could buy - you could pay for all this with bitcoin. So you really - no, I'm just kidding.

Steve: No, no, no, no.

Leo: That's exactly what you can't do.

Steve: So as I'm looking at this, I'm thinking, how do Cisco's and Juniper's corporations react to this clear, blatant knowledge that their routers are compromisable?

Leo: I bet there's two reactions - one public, one private.

Steve: Yeah. Exactly. Well, and the public one is we have never and never would provide any cooperation...

Leo: Absolutely not.

Steve: ...willingly to the NSA.

Leo: No, never.

Steve: Yeah.

Leo: Yeah.

Steve: And, I mean, I think this is all behind their back. I don't think they've done this. I think, for example, as I mentioned at the top of the show, looking at this, reading this very carefully, I don't see evidence of remote exploitation of Cisco and Juniper routers. There has to be a so-called "interdiction." So, for example, the description of JetPlow: "JetPlow is a firmware persistence implant for Cisco PIX series, a very popular Cisco product, and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BananaGlee software implant." And so that's when I said, wait a minute, BananaGlee. So then I look up - so BananaGlee, "a software exploit made by Digital Network Technologies (DNT) for Juniper NetScreen ns5xt, ns50, ns200, ns500, ISG 1000, ssg140, ssg5," on and on and on and on on model numbers, for another three lines' worth of them. "Also works on Cisco PIX 500 series and ASA," and then another set of five model numbers, "series firewalls. Used for exfiltrating data from target networks."

So there's BananaGlee, which is this technology from DNT, from Digital Network Technologies. And then JetPlow is a firmware persistent implant for Cisco PIX series and ASA firewalls. It persists DNT's BananaGlee software implant. So it sounds like JetPlow lives in the BIOS and is used - sort of hosts BananaGlee. And it says JetPlow also has a persistent backdoor capability. That's another acronym, PBD, Persistent Back Door, that we also see throughout these. It says: "JetPlow is a firmware persistent implant for Cisco PIX series and ASA" - I guess they're being a little redundant here. Yeah, it is repeating the same thing. "If BananaGlee support is not available for the booting operating system, it can install a persistent backdoor (PBD) designed to work with BananaGlee's communication structure so that full access can be reacquired at a later time. A typical JetPlow deployment on a target firewall with an exfiltration path to the remote operations center is shown above, and there's a diagram. JetPlow is remotely upgradeable and is also remotely installable, provided BananaGlee is already on the firewall of interest."

So now this sounds like I misstated it, that BananaGlee is the lowest level thing in the BIOS. And again, so notice that it's saying that JetPlow can be installed if BananaGlee is already - and remotely installable. JetPlow can be remotely installed if BananaGlee is there first.

Leo: I'm just glad the NSA pays attention to interoperability.

Steve: Well, actually I was impressed, as I'm running through this, that they really do. They have the notion of a software stack of these exploit modules which are interdependent and hierarchical. So if you get BananaGlee stuck into a router, into its BIOS somehow, which runs at a level below the OS, then it'll create a persistent backdoor, and that will then allow remote operators to install the higher level exploits as they are and become available.

So I've got so much else to talk about here, I'm going to skip over some of these. It does look like, as I mentioned before, that this Chinese multinational networking and telecommunications equipment services company headquartered in Shenzhen, Guangdong, and you knew how to pronounce it, it's not...

Leo: Shenzhen, Guangdong.

Steve: Shenzhen, Guangdong.

Leo: It doesn't matter.

Steve: Is it Huawei?

Leo: Huawei.

Steve: Huawei.

Leo: Huawei.

Steve: Their big router, and I remember seeing the name of it somewhere, well, the NSA project is HeadWater. And it appears to install 100% remotely. The document says: "HeadWater is a persistent backdoor (PBD) software implant for selected" - I just cannot pronounce this name. Huawei?

Leo: Huawei.

Steve: Huawei? Huawei routers.

Leo: Forget the H's. Huawei.

Steve: Huawei, ah, thank you. "The implant will enable covert functions to be remotely executed within the router via an Internet connection. HeadWater PBD implant will be transferred remotely over the Internet to the selected target router by Remote Operations Center personnel." Okay, so again, this implant is transferred remotely, does not require a local install. "After the transfer process is complete, the persistent backdoor will be installed in the router's boot ROM via an upgrade command. The persistent backdoor will then be activated after a system reboot. Once activated, the ROC" - that's the Remote Operations Center - "operators will be able to use DNT's" - and there those guys are again - their "HammerMill Insertion Tool (HIT) to control..."

Leo: See, they had to have planned that one.

Steve: Yeah, HIT.

Leo: HammerMill thing.

Steve: HIT, uh-huh, "to control the persistent backdoor as it captures and examines all IP packets passing through the host router." Whoopsie. And then here's another example of why it can't be coincidence: "HeadWater is the cover term for the persistent backdoor for Huawei Technologies routers."

Leo: You're never going to get it.

Steve: I am never going to get it. Whatever it's pronounced. "PBD has been adopted for use in the joint NSA/CIA effort to exploit [that] network equipment."

Leo: [Laughing]

Steve: And then here it is.

Leo: Nice. Nicely done.

Steve: Thank you. The cover name for this joint project is TurboPanda. So, okay. Panda had to have been chosen deliberately. Oh, and by the way, the status: On the shelf, ready for deployment.

Leo: OTS. But I really think these slides are old, though; right? Because the hack on the iPhone is for the second-generation iPhone, for 2008.

Steve: Yes.

Leo: I'm thinking that these slides are roughly 2008 era; right?

Steve: Yes, and they're all dated 2008.

Leo: Yeah, so...

Steve: We understand that. So this has all been going on and continuing.

Leo: It's not up to date. It's five years old. This could...

Steve: Right. And which again is another reason to think, okay, well, maybe Snowden was not the source of this. Remember that there were three Montana things that we just sort of glanced over last week: SchoolMontana, SierraMontana, and StuccoMontana. Those are, respectively, for the Juniper J, M, and T series routers. And so those are similar persistent backdoors that allow the NSA to get in.

Leo: So I sense, by the way, a naming schema here.

Steve: Yes.

Leo: Because those are all SMs. And in fact somebody did say that the military often uses a codename generator that generates, not the names, but the two letters.

Steve: Ah, okay.

Leo: And then a human will - and the example they gave, this was in the chatroom, is Operation Desert Storm was Operation DS. And they added something that actually seemed appropriate, Desert and Storm, but really the designation was DS.

Steve: Ah, got it.

Leo: So in this case I think the designation is SM, and they distinguished the different hardware that it was a hack for with different S's.

Steve: Right. And it makes it more memorable and...

Leo: Oh, yeah. The human mind loves it. It's an image.

Steve: ...and less ambiguous if it's, like, over a poor quality communications channel.

Leo: Exactly. It's like the phonetic alphabet, yeah.

Steve: So LoudAuto, here's details on a very cool passive bug, audio bug. So LoudAuto says: "Audio-based RF retro-reflector." So that's what they're calling these. "Provides room audio from targeted space using radar and basic post-processing. LoudAuto's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard office volume from over 20 feet away." That is, where this bug is located. It says: "(Note: Concealments may reduce this distance.)" Yeah, if you put it in a box, it's going to be muffled.

"It uses very little power" - and it says approximately 15 microamps at 3 volts - "so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components at COTS and so are non-attributable to NSA," meaning, again, Common Off The Shelf.

"Room audio is picked up" - and I should say they show a picture of this. It is a little over 16/32 of an inch in maximum dimension. The length of this thing is a little over half an inch. So this is micro size and uses almost no power. So you just tuck this anywhere and let it sit for years.

"Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to Pulse Position Modulate (PPM) a square wave signal running at a preset frequency. This square wave is used to turn a FET (Field Effect Transistor) on and off. When the unit is illuminated with a CW" - that's continuous wave - "signal from a nearby radar unit, the illuminating signal is amplitude modulated with the PPM square wave. This signal is reradiated" - that is, by the bug - "where it is picked up by the radar, then processed to recover the room audio. Processing is currently performed by COTS equipment with FM demodulation capability." Then it lists some names and brands.

Then it says that "LoudAuto is part of the AngryNeighbor family of radar retro-reflectors." And indeed, there are many. There's one that can be stuck in a keyboard cable or in the keyboard itself. And once again, like all these other ones, it doesn't itself generate a signal. It needs to have a beam illuminate it, a radio beam illuminate it, and that is then able to sense the signal. And notice the other thing about this retro-reflective technology. It's necessary to mix the reflected energy with the incoming energy in order to demodulate this. Which means that, even if you could passively pick up this reflection, you wouldn't be able to listen to it yourself because you need to have access to the correct phase of the incoming radar beam in order to perform this signal demodulation. So just crazy, really cool technology.

Leo: Just keep that in mind when you use the HannahMontana technology.

Steve: Exactly.

Leo: And does it strike you that it's also completely possible - you ever read any Graham Greene? One of his great stories, "Our Man in Havana" I think it was called, is about a completely innocuous, innocent tailor who is mistaken for a British spy. And they start giving him money, and so he builds a phony network of spies and all of this stuff, pretending to be a British spy, but he's not. He's just some little mousy tailor. It strikes me, this is so novelistic, that it could just be some guy, maybe even within the NSA, made all this up. Remember, this benefits the NSA. They always say, oh, this is really bad because now the bad guys know what we're up to. Well, first of all, this is five years ago, so this is - it seems to me that there could be a genuine value to the NSA in the sense that, look, bad guys, we got it covered. We can hear everything. You're screwed.

Steve: Don't even bother.

Leo: "Don't even try because you're screwed" could very well be the point of all of this.

Steve: Just buy lottery tickets and hope.

Leo: Yeah.

Steve: Because that's the only way you're going to...

Leo: Don't attempt to attack us because, god, we've got stuff in your stuff that you don't even know about.

Steve: Yeah, you're right. I mean, this is chilling.

Leo: But it could be completely made up. I mean, I don't, you know...

Steve: I'll just skim over some more of this because we're about done here. IrateMonk modifies hard drive firmware. It "provides persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through master boot record substitution." So it doesn't matter if you reformat your drive, if you low-level format your drive, if you clean your master boot record off, because underneath that the hard drive firmware has decided that it wants the master boot record to be what it says it's going to be.

"This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are FAT, NTFS, EXT3, and UFS. Through remote access or interdiction, UnitedRake or StraitBizarre [sp] are used in conjunction with SlickerVicar to upload the hard drive firmware onto the target machine..."

Leo: It's SlickerVicar.

Steve: SlickerVicar, that works better - "to implant IrateMonk and its payload," it says, "(the implant installer). Once implanted, IrateMonk's frequency of execution, dropping the payload, is configurable and will occur when the target machine powers on." So essentially it sounds like this UnitedRake, StraitBizarre, and SlickerVicar, those are PC-level, like Windows-level exploits that briefly pass through your machine, burrow all the way down into the firmware of your drive, and then persistently live from there on. And there ain't much you can do about it. Wow.

Leo: That's one SlickerVicar.

Steve: We talked about the keyboard is another one of these retro - a keyboard spy retro vector. I learned something, and that is there's a project called GopherSet. It's a software implant for GSM Subscriber Identify Module, that's SIM, the SIM card, Subscriber Identify Module. So this is a SIM card. "This implant pulls phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via SMS." So as I read that, I think, wait a minute. A SIM card is just data; right? No. "Modern SIM cards Phase 2+," I'm reading from the slide, "have, conveniently, an application program interface known as the SIM Toolkit, or STK. The SIM Toolkit has a suite of proactive commands that allow..."

Leo: When we say sweep, we mean sweep.

Steve: "...that allow the SIM card itself to issue commands and make..."

Leo: What?

Steve: Yes. Yes. The SIM card itself...

Leo: Who knew?

Steve: ...can issue commands - I know - and make requests to the handset. "GopherSet uses STK commands to retrieve the requested information and to exfiltrate this data via SMS. After the GopherSet file is compiled, the program is loaded onto the SIM card using either a USB smartcard reader or over-the-air provisioning. In both cases, keys to the card may be required to install the application, depending on the service provider's security configuration." So it's actually possible for your SIM card to run a program to query the other memory in your phone and exfiltrate that without your knowledge over SMS.

Okay, and why did I grab MonkeyCalendar, aside from the fact that it's a wonderful name?

Leo: My password.

Steve: Oh, because it goes a little further. This implant pulls geolocation information from a target handset and exfiltrates it to a user-defined phone number via SMS. So this gets loaded into your SIM card, and it's continually sending out, at whatever period they specify, your current GPS coordinates to an SMS phone number of their choosing. Wow.

There is also something called Genesis, which it takes a standard consumer handset, and they change the guts to install an SDR, a Software Defined Radio. So a spy, literally, an agent carrying this innocuous-looking standard cell phone, is able to scan, do a complete detailed RF spectrum analysis within this phone in order to record and perform an analysis on everything going on around them because this phone essentially has been retrofitted with complete RF analysis capability in something that's the regular size of the handset. And there was one last thing. Ah, CottonMouth, yes.

Leo: Which is what you're getting after this long recitation.

Steve: It is what I mentioned before, is the USB cable that is - it's a hardware implant, obviously you need to go in and swap cables - which will provide a wireless bridge into a target network, as well as the ability to load exploit software onto target PCs. So someone makes a midnight visit, swaps USB cables with this thing, and now you've got - there's an RF transceiver for so-called "air gap-bridging," software persistence capability, in-field reprogrammability, and covert communications with a host software implant over USB. And back again, Data Network Technologies (DNT) is involved, along with StraitBizarre. So, yes, this looks like to me StraitBizarre is OS-level stuff. So, yes, the NSA, as you said, Leo, the bad guys might as well read this and just say, well, okay. We're going to go straight.

Leo: Yeah. No more terrorism. We give up. We're just going to sell hotdogs in the bazaar.

Steve: Yeah. So again, I don't think that Edward Snowden would have any problem with this. This is what we would expect the NSA to do and to have, the capabilities we would like them to have, as opposed to doing wholesale data collection, which it looks like they may have less of here in the future.

Leo: Yeah, yeah. Well, Steve, this is a fun subject, and I'm sure there's a lot more you could have said. But we probably should wrap it up at the two-hour mark.

Steve: I think so. And I think we've certainly given our listeners a very good sense for what this technology is and how it works. And that was our goal for revisiting NSA ANT, hopefully one final time.

Leo: Steve Gibson is the Explainer in Chief at GRC.com. That's where you can find 16Kb audio versions of this show for the bandwidth-impaired. There's even text transcriptions written by an actual human being, one who owns her own farrier or something. Elaine Farrieris [Farris]. And you can get that at GRC.com. Will we do questions next week? You going to do a Q&A?

Steve: Yes, let's do a Q&A. It's been a couple weeks, so we will entertain questions, by all means.

Leo: So you can ask a question at GRC.com/feedback. And this doesn't have to be restricted to today's episode. Any question about security or any topic Steve likes to address, you're welcome to leave.

Steve: Potpourri, a potpourri.

Leo: That's why we like doing those. You can also find full-quality audio and video at our website, TWiT.tv/sn for Security Now!. But it's nice if you can watch live. And this is our new time. I should mention we're now on Tuesdays, 1:00 p.m. Pacific, 4:00 p.m. Eastern time, 21:00 UTC, if you want to watch live Tuesdays. And we do appreciate it when you come in live and join us in the chatroom. But again, you can listen anytime. Our goal is just to give it to you any way you want. You want it, you've got it - audio, video, black-and-white, color, I don't - whatever you want. GRC.com is also the home of SpinRite, let's not forget, the world's finest hard drive recovery and maintenance utility. It even works in virtual machines. And many other freebies that Steve gives away, including his port check. Let's mention it again: bit.ly/port - what was the number?

Steve: 3276...

Leo: 4?

Steve: 4. 32764. Bit.ly/port32764. You've got to have that closed.

Leo: Yeah. And it's an automatic check. It'll do it all for you. Just remember, 865 - no, no, that's wrong, 30 [mumbling]. It's in the show notes. Show notes, by the way - hey, thank you, Steve - now available on Steve's website, as well. He takes his notes - very nice notes this week, by the way, lots of pictures and so forth - and puts them up on his web page there at GRC.com. Steve, we'll see you next Tuesday, God and the NSA willing.

Steve: Yes, Leo. Thanks very much.