Listener Feedback #170

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-409.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-409-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. What a great show ahead. Questions, answers. We'll talk more about PRISM, more insight there. You've got to stay tuned. This is the show to keep your privacy and security up. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 409, recorded June 19th, 2013: Your questions, Steve's answers, #170.

It's time for Security Now!, the post-NSA edition. Steve Gibson is here, our Explainer in Chief, the guy who does all the security and privacy and is really our guru in that realm. Hello, Steve. Good to see you.

Steve Gibson: Hey, Leo. Great to be with you again. And we have largely, as expected, a follow-up to last week's blockbuster theory of how PRISM works, as I expected. Actually I probably had double the number of email that I normally pull from the mailbag, which would have only been in half of the period of time. So, strong response. I've never had a response, as evidenced on Twitter, like we had to last week's episode. So a lot of people who - our typical listener, who understands the technology that we talked about, and we talk about every week, understood this.

And actually another document surfaced. I have a link to it in the notes today [bit.ly/sn408n]. But it's from this Narus company, which was originally an Israeli company that produced the high-performance networking filter hardware that I referred to last week. I tracked them down after the show, and one of the - like the second page of their brochure shows a prism as - it's like, okay, yeah. That's a little too coincidental.

Leo: Well, and I've seen a number of articles that kind of seem to somewhat confirm, from the Washington Post and Declan McCullagh writing at CNET, that kind of confirm your hypothesis. And I've seen nothing to negate it.

Steve: Right.

Leo: So, but it was interesting because Apple put out a statement, I don't know if you were going to - I'll save, let's save this.

Steve: We do, we do discuss Apple's statement, and actually, unfortunately, how weak it actually is, given the evidence that they're able to provide iMessages in the backlog after the fact. So anyway, we'll talk about that. So inevitably we were going to see some jokes arise from the NSA...

Leo: You know, that's how you know something's serious.

Steve: Yes, exactly.

Leo: Seriously, when something - there's a guy named Jan Brunner [sp] who's an expert on urban, you know, those joke cycles, like remember the elephant in your refrigerator, the dead baby, all of these joke cycles? And I interviewed him once, and he said it's always the most taboo subjects. So the dead baby jokes were right about when the abortion debate was raging in this country. And so it's a way of handling very taboo subjects in a way that is not incendiary, but lets some of the steam off. And so of course...

Steve: Exactly, sort of allows sort of the pressure off of the...

Leo: Yeah, it's a coping mechanism.

Steve: So my absolute favorite actually was a photo that my tech support guy, Greg, sent me. And so there was - it was a photo of a distraught-looking woman. And across the top it said, "My computer's hard drive crashed...." And then at the bottom, and this explains why she's unhappy, "And the NSA won't send me their backup copy."

Leo: [Laughing] What backup - what are you - what?

Steve: I liked that. Then we have another one. An NSA agent walks into his favorite bar. The bartender says, "Hey, I've got a joke for you." The NSA guy replies, "I already heard it."

Leo: [Laughing] Excellent. I love that. I already heard it.

Steve: Okay. And then we have crypto humor, NSA crypto humor: Why didn't Edward Snowden ever go back to his Hong Kong hotel room to avoid the NSA?

Leo: Why?

Steve: It was a one-time pad.

Leo: As it should be if you're Edward Snowden. Never sleep in the same bed twice.

Steve: Exactly.

Leo: Wow. Excellent, excellent.

Steve: So that's our humor, our opening podcast humor, consequence of last week's certainly less than humorous disclosures and our theory about the way things may be working.

In security news it was a very quiet week. I think everybody's still in shock. No one's doing anything, good or bad, except that Oracle had no choice but to release a critical patch update for Java. This fixes 40 new security problems. 37 of these are remotely exploitable without authentication. And Oracle recommends, reading from their release news, that this critical patch update be applied as soon as possible because it includes fixes for a number of severe vulnerabilities. Note that the vulnerabilities fixed in this critical patch update affect various components and, as a result, may not affect the security posture of all Java users in the same way. So...

Leo: Posture as in bend over?

Steve: As in why, you know - oh, and there was a link, like check your current version. So I thought, okay, I wonder what I have. And of course Firefox said, oh, you have no evidence of Java. It's like, yes.

Leo: Oh, good news.

Steve: That's what we want. We have no current version.

Leo: No version.

Steve: Now.

Leo: Yeah, yeah. I was disappointed to see that, you know, I got a new Mac, and I was disappointed to see that Safari by default - happy to see Safari by default blocks third-party cookies - by default does not give you the, what is that setting that we like, Do Not Track setting. It's off by default.

Steve: Right.

Leo: And unfortunately Java's on by default. But Apple has a very good policy, which is, if you don't use it, it turns it off; and, before you can run it, it says are you sure you want to run it. So I guess it's probably all right to leave it on, but I turn it off. I turn it off.

Steve: Yeah. The problem, of course, is that people who don't know will just say, oh, yeah. They just click "Yes" in order to move on to what they want. And that's how they get owned in this day and age.

There was a piece in a Foreign Policy website. I think our friend Simon Zerafa pointed me to it. At first I was just going to give it a synopsis. But as I began to read it, in order to figure out how I would pull out from it, I thought, wow, this is just all good stuff. So I'm going to share it with our listeners. The title is "The Suddenly Booming Business of Secretive Communications." And of course the reason this is relevant is what has been the upshot of the revelations a week and a half ago. So the article reads:

"For anyone in the habit of wearing a tinfoil hat, the last couple of weeks have been ones of redemption. With a steady stream of revelations about the National Security Agency's astonishingly broad intelligence-gathering activities, conspiracy theories about its reach have been seemingly validated. Those same raise a related question: Are there ways to avoid the NSA's prying eyes?

"It turns out there are, for the most part, anyway. And for the companies selling communication tools to circumvent surveillance programs, business is going like gangbusters. Silent Circle, a company that provides encrypted email, phone, and messaging services, has seen sales increase 400% so far this month. You can now take advantage of a 50% discount on its full suite of services.

"Moxie Marlinspike, the hacker and developer behind Whisper Systems, another purveyor of encrypted communications tools, says his service has seen a 3,000% increase in its new active user rate since June 6, when the story about the NSA's PRISM program first broke, though he did not offer specifics about the number of users the company has signed up. Cryptocat, a free encrypted chat service" - which was of course the topic of this podcast a couple weeks ago - "welcomed almost 5,000 new users last week, and server traffic is currently running 80% above average for its 65,000 regular users, according to Nadim Kobeissi, the site's lead developer. And Tor, a web browser" - as this site describes it, and we know what Tor is, actually, a network, anonymizing network - "that protects its users from so-called 'traffic analysis,' has seen a 17% increase in its mean daily users in the United States. The number of users is now approaching 90,000.

"'We are running around with our hair on fire. It's insane,' said Silent Circle CEO Mike Janke to Foreign Policy. Utilizing a peer-to-peer encryption tool, Silent Circle's communication tools - which include everything from email to text messaging to video conferencing - promise near-anonymity on the web. In layman's terms, these services

scramble your communications with users using a similar encryption protocol, turning your message into a bunch of gibberish for the NSA analyst listening in.

"Silent Circle's offerings are part of a burgeoning movement online to ensure user anonymity and prevent privacy breaches, but tools such as encrypted email can only do so much to fight back against the NSA. In recent years, encryption technology has become so advanced that the agency has largely moved away from using brute-force decryption methods - that is, leveraging an immense amount of computer power to unlock a given encryption algorithm - and instead has adopted traffic analysis methods, according to Janke." This is the Silent Circle CEO guy.

"As part of this new approach, the NSA scoops up immense troves of a given type of communication and tries to spot patterns in the usage of those exchanges. That technique, known as traffic analysis, allows the agency to establish connections between people and groups on the Internet. And by identifying its targets in the morass of messages, the NSA can map a given target's entire social network. That information can often be more valuable than the content of the message itself."

And to pause here for a second, of course we noted, and I think mostly it was after we stopped recording last week, Leo, you reiterated more strongly and I thought made the very good point that the reason the NSA is sitting there tapping the communications of these major providers is they all know who their customers are, even if the NSA can't see it because it's encrypted, but they can see the patterns. Then the NSA can go to the provider, saying, well, we know this is a customer of yours because this went down your pipe at such and such a time. So we need to know who that is. And then they can go to the warranted full disclosure on a targeted basis, rather than just the wholesale sweeping of content, many people saying, well, it's encrypted, so what.

Anyway, just to wrap this up, it says, "All this means that encryption tools like those offered by Silent Circle are only a first step, a reality that Janke fully acknowledges, and that email is particularly vulnerable to NSA snooping. 'Due to the physics of email'" - I'm quoting somebody. "'Due to the physics of email, how a server needs to take that data and send it down to someone else'" - ah, it's Janke again, saying, "'it is vulnerable to metadata, and it hangs around forever,' Janke said, referring to secondary data, the contents of the 'to' and 'from' fields, say, or routing information" and so forth.

Anyway, so I thought that it was interesting that here we're seeing in the popular press, first of all, we've seen what we would expect, which is a massive rush to adopt these technologies, more so than previously. I mean, they're out there. They exist. But people are like, oh, well, I'm really not sure that I need it. Suddenly hundreds of percent increases in actual usage by people who really want to be secure. And I ran across one that looks very nice called Threema, T-h-r-e-e-m-a. It really looks like they've done this right. It's secure instant messaging. Not quite support for BlackBerry yet, but it is multiplatform, and BlackBerry support is reputed to be coming. So that's a nice thing.

But the other thing I thought was interesting was that they're recognizing that it's possible to leverage traffic analysis, much as I talked about last week when I was trying to say, wait a minute, it's not like the metadata is not useful. It's incredibly useful, so notwithstanding the various attempts to minimize its impact that we saw from the various people, the politicians who were the talking heads last week.

And I did, I thought this was interesting, for those who aren't following me on Twitter, there is a bit.ly link I created. Leo, you might want to bring this up just to look at the top right of the second page. It's bit.ly/sn408, which is the Security Now! episode number last week, all lower case, and then "n" as in Narus, N-a-r-u-s, which is the company

which we're almost sure, well, we know for sure that they were the traffic analysis provider years ago in the secret NSA room at the AT&T building at 611 Folsom Street in San Francisco [bit.ly/sn408n]. There's every reason to believe that that relationship has continued. And in fact they are now a subsidiary of Boeing.

Leo: I like this prism.

Steve: Yes, there's a prism.

Leo: Wow. Okay. Yeah, network traffic beam, split it into three planes.

Steve: Yup.

Leo: I mean, that's not really what's going on with our PRISM.

Steve: No.

Leo: But it is ironic.

Steve: And in fact I think actually it's probably a half-silvered mirror. I don't know exactly how a fiber optic beam splitter works. But I would think they'd be using a partially silvered mirror so that half the photons bounce off; half go straight through. And so it actually is a beam splitter rather than a prism. But prism splits a light into different frequencies, and here it is in the Narus brochure. It's like, okay.

Leo: Yeah, first page.

Steve: You could be just a little - could be a little more subtle, maybe.

Leo: You know that PRISM thing? Yeah, we invented it.

Steve: Yeah, exactly.

Leo: That's funny. That's funny.

Steve: I did want to make a mention, just to tie this up, because I've mentioned it in the past on the podcast, did finally - the BlackBerry I was waiting for, the Q10, which is the keyboarded version of the Z10, got into the stores. And I owned it for two days.

Leo: Two days.

Steve: And I returned it.

Leo: You lasted longer than I did.

Steve: Oh.

Leo: Yeah, you got a Q, though. That's the one with the physical keyboard.

Steve: Well, and I know what they did. And unfortunately they've ruined the BlackBerry now. So I doubled down. I got myself a second Bold 9930, Verizon unlocked, just so I have a spare, because this is...

Leo: You nut. You nut. You...

Steve: Hey, wait a minute. How many MacBook Airs do you have?

Leo: Well, I always - but I get one, I get the new one. I get the latest, not - I don't get the old, I'm not putting old MacBook Airs in the freezer. You crack me up. That's hysterical.

Steve: What they did was they of course went, they decided, okay, everybody's going touch, so we're going to do that. And so they designed a new OS that no longer required the hard keys that the original BlackBerry has always had. I mean, the very, very old BlackBerrys, you'll remember, they had like a scroll wheel on the side, and you could scroll and then push in, in order to, like, select and then enter.

Leo: That's how the pagers worked. I loved that.

Steve: Oh, it was - it's a beautiful interface.

Leo: Yeah, it was a good system.

Steve: I mean, one-handed, thank you very much. And then a menuing system was designed. The point is, yes, there's some learning curve. But the flipside is, once you have learned it, it's the best thing there is. I mean, it's like, it's the answer. And that's what you want in a communications device you're going to be using, essentially plugged into your spinal cord, in the way you want to operate. So instead they said, oh, well, we need touch. They had that awful first attempt to do touch where the whole screen kind of clicked in. It's like, oh, goodness, no. So then they had the Z10, which required them to

design a UI that no longer needed the little - first we went from the scroll wheel, then we went to a track ball, then to a track pad where you go - you have cursor positioning up, down, left right. And then you push in to select, or you've got a back arrow. And then you've got a couple hard buttons for, like, answer the phone, hang up the phone and so forth.

All that's gone. Everything's now touch. And it's awful. I have lived with it. I learned it. I lived with it for two days. And I brought it back. And I said, here, hook my old one up. It's better than this. Oh, and it wouldn't do - the way I was able to get out of it, although I didn't really have to have an excuse, it would not allow me to have distinctive tones for my various conversations. Any time that Jenny is sending me email or text messages, there's a Jenny sound. And my best friend Mark, there's a Mark sound. And we know that there's "Yabba-dabba do." All of that is text messaging. They lost the ability to set up individual ring tones, essentially, for those, believe it or not. It's not there. And it's hugely controversial on the 'Net that it won't do that. And I said, well, it won't do that. And they said, oh, of course it will. Well, they couldn't make it work, either.

Leo: Yeah.

Steve: It's like, okay.

Leo: I don't know. Get an Android phone. You might actually like it.

Steve: No, I'm done.

Leo: I know you want a keyboard, but...

Steve: Unh-unh. I need a keyboard.

Leo: No more touch, he says.

Steve: And I want real buttons. I'm sticking with what I've got. You know, many times - look at Windows 7 compared to 8. You know, they get it right, and then they just can't leave it alone. And we've talked about this. They have to keep up...

Leo: No, that's true. Yeah, they have to put fins.

Steve: Yeah, right [laughing].

Leo: Or you won't buy a new one.

Steve: Now, I just wanted to do a shout-out to all the great listeners who sent me news from this morning of the fact that Canada needs PDP-11 programmers.

Leo: Okay. Why?

Steve: Turns out their nuclear reactors have robotic systems running on PDP-11s.

Leo: Sure. Not a surprise, no, yeah.

Steve: And they're going to until 2050. Two zero five zero.

Leo: Hey, if it ain't broke, don't fix it.

Steve: Exactly. And...

Leo: Of course you can't fix it because nobody knows how to write software for it.

Steve: No one knows how to program it anymore, right. So it's like, okay, just leave it alone. But I guess maybe they do need to add some features or, god help me, they...

[Talking simultaneously]

Leo: ...code fixes. Maybe they want to get it ready for the year 2000.

Steve: Well, so they're looking for PDP-11 programmers who can also train several...

Leo: Wow.

Steve: They're saying 2050 is several generations of programmers.

Leo: Yeah. Kids being born today will need to know how to write code for PDP-11s.

Steve: Now, I figure if I keep taking this level of supplements that I am...

Leo: It's only 37 more years, Steve.

Steve: I'm going to be there.

Leo: You'll be 90. It's good.

Steve: When they decommission those, I want those PDP-11s. I can get a bigger refrigerator, Leo.

Leo: Now, do they - what language are we talking? It's not assembler.

Steve: Yes, specifically stated assembly language programming.

Leo: Aw. But that was, as you said, a very nice orthogonal instruction set, simple, yeah.

Steve: Oh, my god, it's just beautiful. It's a beautiful instruction set, yeah.

Leo: They should learn it. They should learn it.

Steve: Yeah, I have PDP-11s so that I can spend some time programming.

Leo: I know you do. That's what those blinking lights are back there.

Steve: No, those are 8's.

Leo: Oh, I'm sorry, pardon me. Oh, how could I be so stupid?

Steve: Yeah, we've got - they're going to have to be later.

Leo: You should send them a note. Do you need any "8" programmers? We're not dead yet.

Steve: And we already talked about it. I have notes here. We already talked about "Man of Steel." Without a spoiler, and this doesn't spoil anything, I loved the first three quarters of it, and I just was annoyed with the latter...

Leo: I'm exactly with you.

Steve: Yeah.

Leo: It felt like I was watching "Transformers" 3 or 4.

Steve: Yes. It was really just - it was ridiculous.

Leo: Yeah.

Steve: So, right.

Leo: Did you catch all the - and this is not a spoiler, either. And I guess this is not unusual, it was in "Superman Returns," too, all the kind of crypto Christian, you know, he's 33 years old. He emerges like this. There was, in fact, apparently in the early days of Superman, the first Superman that Shuster and Kane were writing, his mother's name was Mary. They changed that to Martha. But there's a - as I'm watching it, I'm going...

[Talking simultaneously]

Leo: And then at one point General Zod says "I am evolution. This is - evolution will win." And Superman responds by punching him out. So it was kind of interesting. I don't know what it means. And it was apparently even stronger in "Superman Returns," which I missed. But Superman is a god, after all; right? They say that over and over again.

Steve: Oh, watch "Superman Returns." It's got a fabulous opening sequence. Oh, goodness. I mean, I've watched it, like, seven times. It's just wonderful.

Leo: I do love, and I'm with you, and I think you and I might be...

Steve: Well, I love mythology.

Leo: Yeah, but you and I might be in a small minority because a lot of people didn't like - the people who liked "Superman" didn't like "Man of Steel" as much. I like how it was shot. I like the grittiness of it. It feels like the film was processed. It's very grainy.

Steve: Yes, I agree. I thought it was - I liked everything about it until this ridiculous extended battle scene. It's like, eh.

Leo: They could have left that out. I have to agree.

Steve: And also it made a huge amount of money. It was $125 million in its first weekend.

Leo: Oh, yeah, very big opening weekend, yeah.

Steve: And unfortunately, "Iron Man 3," which was also ridiculously violent in the same way, was similar. So maybe that's what they have to do now in order to cross the million dollar threshold, the hundred million dollar threshold.

Leo: Yeah, people want - and it's kids.

Steve: It is. It's not our...

Leo: It's not us old farts. It's young people. They want all of the action.

Steve: Yeah. I'm going to completely miss "Pacific Rim." I am not - that doesn't even get in. I'm not even going to try.

Leo: It looks like a lot of blowing things up on that one, yeah.

Steve: Oh, it is, actually, just transformers, robot-controlled transformers.

Leo: Yeah, right, yeah.

Steve: It'll sell in Japan, I think.

Leo: Yeah. I've never been a fan of comic book movies. I have to say I liked "Man of Steel," and I liked how they handled the back story. I didn't even - people complained about the first 40 minutes on Krypton, and I actually liked that stuff.

Steve: Oh, it was wonderful.

Leo: I thought that was quite good.

Steve: Yes.

Leo: But you and I are the only ones, I guess.

Steve: Yeah.

Leo: All right.

Steve: Now, I got a neat tweet from someone who said, "Steve, I would normally thank you for the fact that I have lost 50 pounds and have kept it off."

Leo: All right.

Steve: And he's of course referring to getting rid of starch from his diet. He said, "However, mostly I want to thank you for 'Justified.'"

Leo: "Justified." What was that?

Steve: That was - it's the...

Leo: Oh, the show, yeah, yeah, yeah.

Steve: It's the series on FX...

Leo: Love it.

Steve: ...which I turned a bunch of people on to, and they're like, oh, my goodness. I mean, it is really excellent. So I have another one. I just finished watching the first two seasons of this in a multiday marathon. They're both out on disk. I bought the Blu-Ray on the first season, the DVD the second season, but of course you can get them wherever you get your media. And this is an AMC production called "The Killing."

Leo: Oh, yeah, that's - whoo.

Steve: Oh, Leo.

Leo: Yeah, yeah. That's free on Amazon Prime for people.

Steve: Oh, my goodness.

Leo: I bought it, too, and then I found it on Amazon Prime streaming for free. But, yeah.

Steve: It's top - my top recommendation for incredibly good television. Again, Jenny recommended it to me. She said, "Steve, you've got to watch this." The third season is now airing. So my box is recording Season No. 3 and has been. Meanwhile, I watched the first two seasons. Oh, goodness. I mean, it is - so I read one comment that referred to it as sort of like reminiscent of "Twin Peaks" without the crazy.

Leo: Yeah.

Steve: And I thought, well, that's interesting because the music is sort of reminiscent. It's a murder mystery, so it has that in common with "Twin Peaks." And but the writing and the acting, it is spectacular. So anyway, I just wanted to, for people who care about my opinion on these things and have succeeded in following it in the past, "The Killing" on AMC is, oh, wow, it's really good.

Leo: It's a Danish TV show.

Steve: Well, it's based on a Danish series. And so it's a remake of...

Leo: Oh, yeah, yeah, yeah. But it's from a - yeah, yeah.

Steve: Yes, absolutely.

Leo: It's not actually Danish, yeah.

Steve: And I had a - I ran into, in the mailbag, a question and comment that opens up a topic that I sort of started, I stepped into last week when you were asking me about SpinRite and Mac. And this is Stuart Rawling in Merced, California. He said, "Steve, great to hear you're working on an OS X SpinRite. I have a late 2008 iMac with a failing hard disk drive that was a part of a recall from Apple that I missed. I'm not sure of the exact nature of the failure the Seagate drives are having," which apparently were being recalled, "but I'm suspecting that running SpinRite on Level 2 may be sufficient to prolong the life of the iMac. I'm currently toying with replacing the hard disk drive with a solid state drive, but would be willing to give any beta of SpinRite a try to see if it makes a difference before I do so. Of course, I have this fully backed up, Time Machine, Carbonite, et cetera, et cetera.

"I'm already a long-time owner of SpinRite and the proud owner of a hard disk drive that was previously completely recovered, and I would be more than happy to buy another copy to pay you for your additional work that you are undertaking for the Mac version. This offer stands with or without a beta. So make sure this does not go the way of CryptoLink. Cheers, Stuart."

Okay. So I have a couple things to say because many people have been excited by the news of a Mac version. So, first of all, there will not be a Mac version. It will just be the one SpinRite, which will now also work on the Mac. So there actually is no need for there to be a SpinRite Mac. So the good news is, for people who are multiplatform, you'll be able to run the one version you get, you'll be able to run on everything. And that's of course because all I care about is the chipset, is the underlying Intel processor which the Macs that are Intel Macs are able to operate on. So this will not work on a PowerPC Mac, and I'm sure there will never be a SpinRite for PowerPC-based Macs. But I can do it relatively easily for Intel Mac because I'm bringing my own OS along.

Relative to betas and so forth, I'm going to handle this the way I did SpinRite 6, which is it's being developed right now pretty much in the open, I mean, in an open, public dialogue over on GRC's news server. There's a newsgroup, grc.spinrite.dev, and we've already got people playing with code right now. It's not SpinRite code. I just finished some code to fully enumerate the PCI bus in order to find all the mass storage controllers

because it turns out that there are - the newer controllers have a mode of operating called AHCI, which is the Advanced Host Controller Interface. And then there's IDE and ATA and DMA and Ultra DMA and all this.

So I'm working on code to begin to sort of create the low-level technology which will allow SpinRite to bypass the BIOS. And we'll have code running as I'm writing my own drivers. And this will all be tested in the open. So if anyone's interested, this is the GRC discussion groups that we've had for a decade. And there is a SpinRite development subgroup off the SpinRite group, and it's open. Anyone who is interested is welcome to join us over there.

The way I handle pre-release is that, if you're an existing owner, you'll be able to use the URL that we can provide you, that we do provide you, to download your copy of SpinRite anytime, and you just change the URL, and you'll be able to get pre-releases of this. I'll let people know what's going on. People in the development group will always know what's going on. But so essentially I've got the existing licensing technology which has been in place. We use that, for example, to allow people to download SpinRite 5, if they actually want to run it on an 8086, because in SpinRite 6 I began using 32-bit code much more aggressively, and so we ran across people that actually still had non-386-based hardware. And it's like, oh, okay, you can have SpinRite 5. You just change the URL to a 5, and then you get a copy of SpinRite 5, using the same approach. So we'll be doing that and, therefore, allowing people to play with SpinRite as it comes along.

And I actually am deliberately planning several releases of SpinRite because doing the native USB support is probably going to take a lot longer. There doesn't seem to be the same uniformity in USB chips that there are in the hard drive chipset. So SpinRite 6.1 will have a whole bunch of new features, including it'll support the Mac and support all the latest hardware, large-format hard drives, UEFI file systems and BIOSes and so forth. But I'm going to deliberately not delay that in favor of working on USB. That'll be probably 6.2. We thought that 6.2 was going to be the AHCI controller, which is a far more sophisticated controller than IDE, except it turns out all the - and this was the result of this weekend's, this past week's and weekend's experiments - all the AHCI controllers can be told to behave as an earlier generation controller, so I'm not going to have to explicitly support AHCI nearly as soon as I thought.

So the point is, since it's all going to be free, and that's the answer to Stuart's question, is I'm not going to charge anybody for this. I'm happy to do it. I'm enjoying it. I'm happy to keep SpinRite alive, and everyone has been supporting me by buying SpinRite. So this I how I return that favor.

Leo: Very nice.

Steve: And I'm glad to do it.

Leo: Very, very kind, Steve.

Steve: And consequently, since it's free, I don't have to hold everything back waiting for one big release. I can release it sort of incrementally as I get chunks of work done. And it's looking like it will be able to do - I have done a Level 2, 2TB drive in five hours, and I'm going to be able to make it faster than that because we'll be using much larger buffers and something called "extended real mode," a different way of allowing the real

mode instruction set and chip to access all of the machine's memory, to use 32MB buffers rather than 32K buffers. So anyway, if anyone wants to follow along, it's grc.spinrite.dev. You do need - we do not have a web browser interface. We use old-school NNTP, the Network News Transfer Protocol. But, for example, the Mozilla folks have an NNTP browser. And even Outlook, I think, is able to do old-style newsgroup, which is really a terrific way of operating.

So that's what's going on. I'm working on it. There's no way it's going to go the way of CryptoLink. I should mention that, I mean, I stopped CryptoLink because I felt what was happening with encryption. We keep seeing there being this tension where the government is beginning to - is still making noises about wanting to force backdoors on any encrypted technology. And so it may well be that a commercial encrypted solution won't be viable unless it has a backdoor. And I just have no interest in doing that. So anyway, SpinRite needs some more of my time, and I'm happy to give it to it. That's all I'm working on now. So I'm - and I'm really enjoying it.

Leo: I'm thrilled to hear it.

Steve: And I saw a tweet that I just wanted to comment on. Someone sent - he said, "I listened to the Distributed Hash Table episode [SN-398] of Security Now!, and it was an hour and a half before getting to the main topic." And so I just wanted to say, you know, the whole podcast is the main topic. Everything we've been talking about, and all of the news of the week - and obviously this is a Q&A, and we're about to get to the Q&A. But this is what we're offering, not just whatever we happen to be focusing on on our non-Q&A weeks. So sometimes we have a lot to talk about at the top of the show; sometimes we don't have that much going on. So we just play it by ear.

But I know that our listeners have sent a lot, we've had a lot of feedback saying they just love the whole thing. I mean, they love us talking about what's going on with the strong sci-fi and security and science, and sometimes it's how capacitors store a charge, and what supercapacitors are. I mean, we've had very popular podcasts where our top-of-the-show stuff hasn't even been about security. So that's what we do. And I think we're largely giving people what they want.

Leo: And I might point out that there is something called a fast-forward button on almost all podcast players. And I, personally, I won't spank you if you fast-forward. It's quite all right. So you can go to any part of the podcast at any time. Just think of it as an extra, extra jam-packed, full-of-goodness show, and listen to the parts you like.

Steve: Yeah.

Leo: I can't - I don't even understand why somebody would complain that it's an hour and a - I don't even understand that. Just go to where you want it to begin. Which is very odd to me. It's like, I was forced to listen for 90 minutes. I don't understand. Go get some fresh air, kid.

Steve: Yeah. I think he actually likes the whole thing.

Leo: Yeah. I think that's probably it. That cracks me up. Now, on the other hand, if you're watching live, you're stuck. That's why we want you to watch live. You have to watch, and you have to listen to the commercials. And I don't think that's a problem at all. All right. Are you ready for some - and by the way, we thank them for their support of Security Now!. Are you ready for some questions, Steve?

Steve: You bet.

Leo: Let's see, here. Question Numero Uno comes to us from Chiang Mai, Thailand. Wow. That's cool. Bill Dahm wonders about DNS order of precedence. Oh, this is a good question.

Steve: Yeah.

Leo: Could you explain the order of precedence in determining the application of DNS settings? Which of these three, the OS on the computer, the modem settings, or the router setting, gets to call the shots as far as DNS is concerned? My setup is as follows: I have both a Mac desktop and MacBook Air. I also have a CP-Link modem and an Apple AirPort Express WiFi router. I have a single Ethernet connection between the modem and the router, so both of my computers utilize the WiFi connection.

I can see DNS settings in each of these configurations. The question is which one should I be using to control my DNS settings? Maybe not even that, but which one will the computer use? I'm not sure if I can change the DNS setting - I haven't tried, though I see that they're in the configuration settings - of the modem since it was supplied by my ISP. If I can't, is it game over? If I can, and I know I can change the network setting on my Macs, of course, and my AirPort Express, where would be the best place to do this?

This is a great question. You know, I'll add to this because I just got the new AirPort Extreme router from Apple, the 802.11ac version. And I took that as an opportunity to put OpenDNS in my DNS settings in the router. I've always used DHCP on the computer, so I know at least the computer's not overruling it. But he raises a good question. What if you have a router that's supplied by your cable company, and it has its own settings?

Steve: So, okay. In Bill's case, what he described to us is sort of a three links in the chain; right? He's got a modem and then a router and then his computer. The way to think - I think the best way to conceptualize this is as sort of a, I don't know, like a waterfall or a linked chain. The idea is that, if you leave everything alone in its - everything in sort of the default, the DNS servers are provided by the ISP. And so when devices get turned on, the device nearest the ISP asks the ISP for its information. And this uses a protocol called DHCP, Dynamic Host Configuration Protocol. So the device closest to the ISP says, hi. What should I use for my IP? What should I use for my DNS settings? And is there anything else I need to know? And so sort of the furthest away entity, the ISP, provides that to the next closest to you device.

And then, in turn, the next closer device says to that one - asks the same question: Hi

there. What should I use for my IP? What should I use for my DNS settings? And so that device gets them from the one next upstream in the direction of the ISP. And similarly, when you turn your computer on, it says to your router, which is typically the thing the computer's connecting to: Hi there. What should I use for my IP, and what should I use for my DNS? So it's sort of a hierarchy of the same question being asked each stage up the chain.

Now, again, if everything is left alone, then the typical default is to ask for your IP and ask for your DNS settings. And that's probably across the world what the vast majority of systems are doing. But our listeners know, for example, they say, well, my ISP's got really slow DNS servers. I want to use OpenDNS. So they know that they can change - in Windows it's called "Obtain DNS settings automatically," or I will provide the DNS settings. And Apple certainly has the same ability to override the automatic sort of waterfall of the DNS settings coming from each level down to the lower level. You can say, no, I don't want the automatic ones, I'm going to put in my own.

Now, you could do that on each computer, and then the computers would ignore what the router was saying. Or, if you are able, and Bill wasn't sure he was, but he saw these settings in the router, if your router lets you change them there, then the benefit is you don't have to also change them on all of your computers. That is, you sort of stop the waterfall higher up in that chain, and then everything downstream of that point, where you say don't be automatic, don't accept the setting from who's upstream. I'm going to override it at this stage in this hierarchy, in this chain, and then everybody below will use those.

So, for example, if the modem allows you to set those, that is, set the DNS, then the router would ask the modem, and it would get the ones you set. And your computers would ask the router, and they would get the ones you set. So I think that's really the best way to think about it is that, when everything's automatic, those settings propagate from the ISP all the way down to the computer. And anywhere in that chain you can say, oops, stop listening, stop asking upstream. I'm going to tell you the answer I want for everything downstream. And so there's a sort of a comprehensive answer to that question.

Leo: Good. Easy enough.

Steve: Oh, and my goodness, I just saw the name on Question #2. Have you seen the video, Leo?

Leo: I did.

Steve: Oh, lord.

Leo: So weird. He has turned - he's turned into the "Two and a Half Men" guy. Winning.

Steve: Okay.

Leo: Blessedly blanked his name out. Charlie Sheen.

Steve: Charlie Sheen. Now, okay. Now, we can't air it on the podcast.

Leo: Oh, it's full of profanity and sexuality. We're talking about John McAfee. By the way, the one good thing about that video is I now know how to pronounce "McAfee."

Steve: Although he doesn't tell us how to spell it, although we do know how to pronounce it, yes.

Leo: Right, right.

Steve: So, yeah, it's not Mc-AF-ee, it's MC-a-fee.

Leo: McAfee.

Steve: Yes. Now, so for our listeners...

Leo: And it is him, by the way, and it's just weird. He does a video on how to uninstall McAfee. He says, "I wrote this great program, this simple little program, 15 years ago. I haven't had anything to do with it in 15 years." In fact, IBM owns it now, I think. Oh, no, I'm sorry, Intel owns it now. But so he cashed out 15 years ago. And so he says, "But I keep getting email all the time from people saying, how do I uninstall McAfee?" There are scantily clad women, much profanity. There's a fake nerd who supposedly is telling you.

Steve: There's a face full of cocaine.

Leo: No, it's not cocaine. You'll notice the soap, the bath salts boxes.

Steve: Oh, I saw - oh, okay.

Leo: That's what he was into was inventing this new thing called "bath salts." And he gets high in it. And eventually - there's lots of guns, and eventually he shoots the computer and says, "That's how you uninstall."

Steve: But it is the most bizarre thing. You know, we...

Leo: It's not funny, I don't think. But lots of people found it funny. I thought it was

sad.

Steve: We shared the bizarre adventures in Belize and his blog that he was doing for a while, where it was just stranger than truth. But anyway, so...

Leo: He's Charlie Sheen. He's become Charlie Sheen.

Steve: So it's...

Leo: Winning.

Steve: For people who think they might enjoy what Leo just described, it is - really you have to see it. It's bizarre.

Leo: It's on YouTube, and you can search for "YouTube John McAfee."

Steve: Yep, John McAfee.

Leo: He's got his own channel.

Steve: Wow. Well, maybe there's more...

Leo: [Groaning]

Steve: Oh. So our listener said my name is - this is John McAfee. And he says, "No relation, thank god." And this was before - maybe this was after the video. Maybe he knew about the video. I don't know.

Leo: You don't have to.

Steve: No.

Leo: Actually, in some ways he's more coherent than I thought he would be, McAfee.

Steve: He, yes, I agree. It's like, okay, well...

Leo: He's not quite as out of it.

Steve: He's very, very serious.

Leo: And at least is making fun of himself a little bit. I think. It's hard to tell.

Steve: I found myself thinking, oh, my. I actually spoke with that guy on the phone once. It's like...

Leo: Did you really?

Steve: Oh, yeah, because...

Leo: That was a different guy.

Steve: Because I was writing the InfoWorld column, and I made up three columns about the theory of viruses, and he assumed I had them. So he wanted copies of mine. He wanted to exchange them. And I said, I'm sorry, John, I just - I'm a programmer. And in the same way that I know how I would bug companies if the NSA told me to, I know how I would write viruses if someone told me to. There's only one way you do these things, or the best way you do them. And so he was disappointed he couldn't get copies of viruses from me. This is back when he was actually writing antivirus software. I don't know if he was ever actually a programmer.

[Talking simultaneously]

Steve: I don't think he's a...

Leo: I don't know what the story is.

Steve: I think he's a systems guy.

Leo: Yeah, I don't really know. Supposedly he started writing this to target a specific virus at his place of employ, and it became an application. But I don't know.

Steve: Well...

Leo: Read the Wikipedia article. That's - who knows how accurate or whether he's gotten into it or not. I know he's gotten into the bath salts. So this John McAfee of Oakland, who's no relation, and probably...

Steve: Our John McAfee.

Leo: And he probably pronounces it Mc-AF-ee, just to be different.

Steve: Yeah, so people won't say, oh, my god.

Leo: Yeah. Steve and Leo, fascinating podcast last week, the best one ever. But you never told us where "zetta" fits in with mega, giga, and tera. Oh, and let me see if I know. There' a megabyte, gigabyte, terabyte, peta - what's after terabyte? Petabyte?

Steve: Yes.

Leo: Exabyte.

Steve: Yes.

Leo: Is it zettabyte next?

Steve: Yes.

Leo: Okay. And then there's just zottabyte, isn't there?

Steve: No, there's yotta.

Leo: Yottabyte, that's it, yottabyte.

Steve: Yottabyte.

Leo: Okay.

Steve: Okay. So we know mega, giga, and tera. And so each of these is a 10^3, so comma zero zero in English notation. So we've got - we all know a terabyte is like - now big drives have terabyte-sized platters. So, and the reason this came up is that the NSA storage facility outside of Utah will be able to store five zettabytes of data. So that is five billion terabytes.

Leo: Five billion terabytes.

Steve: Five billion terabytes.

Leo: So you know that terabyte drive, or maybe you have a 3TB drive, you're, like, living large in your computer?

Steve: Yeah.

Leo: Imagine at several billion of those. Wow. Billion. Not zillion.

Steve: Five billion terabytes.

Leo: You can find, of course, Wikipedia has all of the definitions, if you really wanted to know. So let me just - and by the way, if you go the other direction...

Steve: You mean mic...

Leo: Yeah, nano, micro and all of that. There's a whole thing for that, too.

Steve: Yeah. Milli, micro, nano, pico...

Leo: Pico, that's right. I don't know what's after that.

Steve: Really small. Really tiny.

Leo: There's IEC binary preferences, too, which are different.

Steve: Oh, of course. Really?

Leo: It's a, yeah, kibibyte.

Steve: Oh. Oh, okay.

Leo: And a mebibyte and a gibibyte and a tebibyte and a pebibyte.

Steve: Well, and the other problem is there's always been this, is it a thousand, or is it 1024?

Leo: Right, is it binary, or is it...

Steve: Yeah. And some of the, I mean, there's been some controversy with, like, hard drives because they just squeaked out all zeroes. They weren't able to squeak out the 1024 binary size K. They used the decimal size K. It was like, yeah, okay, well, that's cheating. But, you know, maybe not. I don't know.

Leo: I'm pleased that I was actually able to remember that order.

Steve: Very good job.

Leo: I forgot kilobyte, which is where it all begins. Byte, kilobyte, and then on.

Steve: Yup. Yup.

Leo: Good question. How many libraries of Congress - now, I don't know how big the Library of Congress is. Somebody told me once 7TB. So it's roughly a billion Library of Congresses. A billion Library of Congresses. A billion. Isn't that - yow.

Steve: Yeah, of, like, nonsense. I mean, of, like, just crap. It's just crap.

Leo: Well, that's the other thing. It's not...

Steve: It's just like it's, we're going to record every - all the noise on the Internet, and then...

Leo: Yeah, good luck.

Steve: ...we'll filter through it. Okay.

Leo: That's, to me, that's hubris. That's overweening pride. We do it because we can. Joeri Sebrechts in Belgium wonders, is SSL secure if the certificate authorities cooperate? Steve, thanks for your podcast about PRISM. Very informative. I can imagine how people outside of the U.S. must feel about this. Geez, Louise.

Steve: Yeah. Yeah.

Leo: One thing I was wondering, and maybe it's my lack of understanding of SSL speaking here, why SSL offers any protection at all? Wouldn't it be possible for the

government to get the private key from the certificate authority and decrypt the traffic when they splice it? Suddenly JavaScript-based encryption doesn't seem so crazy to me anymore.

And along with that comes Jimmie Andersson from Sweden - what an international show we have here today - wondering about SSL encryption: Thanks for your great podcast. What would happen if the NSA got a copy, for example, of Facebook's SSL certificate? Wouldn't they be able to decrypt all the traffic into and out of Facebook?

Steve: Now, these, I think, are very important questions. First of all, let's talk a little bit about the protocol of SSL because it is secure against eavesdropping, even if you have keys. And that's important. So the keys, the public keys that these questions are worried about are used for authentication. And let's remember that. Authentication only proves that you're talking to who you believe you are. It is the authentication that prevents the man-in-the-middle attack, where somebody intercepts the traffic and then can view it and alter it and then send it on. So authentication is separate from privacy. We need to keep those two things separate because they are cryptographically almost unrelated to each other. You can easily have one without the other is my point.

Now, the way the SSL protocol works is it is secure against eavesdropping, meaning, and we've talked about this many times, each side generates a pseudorandom number that's with a high level of entropy so it cannot be guessed, and it's back - it was because some random number generators used to be poor that SSL, that was an SSL vulnerability that eavesdroppers could take advantage of. We've solved those problems long ago. So they each generate a random number. And they send a derivative of what they each generate to each other. And through that exchange, and then combining it with the information they did not disclose, they each are able to arrive at the same private key, the same symmetric key, which is then used for the crypto. The point is, though, nobody monitoring, nobody who is a passive eavesdropper gains any useful information from that. So that's key. So as long as the conversation is eavesdropped on and not intercepted, we're okay.

Now, as far as we know, this is all passive eavesdropping. The technology that we believe they're using for hardware, the concept of a fiber optic splitter, now, this is all passive monitoring. And, boy, it really, I mean, that's caused enough trouble. Can you imagine if the government were actually intercepting connections and performing man-in-the-middle attack? But that said, it is chilling, I think, to recognize the legal authority that the U.S. intelligence agencies have been given to compel private commercial entities to divulge information on the grounds that it's required for national security, and those agencies are prohibited from disclosing that.

Now, of course in the news since, there's been a lot of conversation about these agencies really pleading for the government to let them talk, to let them talk about the national security letters that they've been receiving. And I know that that's been a focus of yours, too, Leo, for some time, I mean, that aspect of it. But also remember that a certificate authority never receives the private key of the entity whose certificate they're signing. They're signing the public key to say, yes, we're asserting with our certificate authority integrity, that this public key belongs to, for example, Facebook. They never see or get the private key. Facebook - well, because they don't need it. Facebook holds onto that very closely. And in fact it's Facebook's private key that allows them to make their assertion, coming in the other direction, that they are Facebook because nobody has Facebook's private key. It never needs to leave Facebook's control.

Now, Jimmie, the second question, said, well, what if the NSA got Facebook's private key? Well, then they could pretend to be Facebook. I mean, they would be Facebook, for all intents and purposes. And that's been, you know, we've talked over the years about various private key leakages which have occurred. And the industry immediately reacts. All the browsers instantly revoke those certificates. I mean, Google, because it's open source in the Chrome browser, we see the list of absolutely assertively revoked certificates. Never allow any of the following certificates to be regarded as secure. Microsoft has a certificate manager, and you can see in there a list of revoked certificates. DigiNotar is famously there. And even, embarrassingly, some Microsoft certificates that in the past have gotten loose which are affirmatively revoked.

So Joeri finishes saying, "Suddenly JavaScript-based encryption doesn't seem so crazy to me anymore." And I would say, for listeners to our podcast, what we've always been talking about: Pre-Internet encryption means you are not only relying on your connection security. You are relying on encryption that you control absolutely, with a long private key that isn't relying on any other entity. And ultimately I think that's where we come back to.

This Threema instant messaging client, T-h-r-e-e-m-a, looks really interesting to me. I think they've really done it right. They have varying levels of security, and they grade the security that you've established with the other endpoint. And, for example, the highest level of security you get when you put your phones together and they scan each other's barcode, physically being in proximity in order to perform the secure endpoint negotiation they need in order to never have had this information go through a nonsecure channel. It's going visibly through the air only when these phones are together. Anyway, I'm hoping that they're going to be adding more support, as I said.

But this is an important question, I think. It absolutely puts a chill on the whole, I mean, all of this, what we've learned about the depths to which the NSA has "obtained authority," and I put those in air quotes, and the weakness of the public key infrastructure from certificate authorities up, and what it is that they may be compelled to divulge. And the fact that we've been - we know we've been relying on a system which requires absolute security, absolute watchfulness, which the bad guys have wanted to penetrate and have successfully penetrated.

Unfortunately, maybe it's not just the bad guys. I mean, I don't - I'm not doing conspiracy theories here or anything. And I think it would be very difficult to imagine that it would be possible for law enforcement to make a case that they should get access to the public key infrastructure. But we also know that they're really, really unhappy that, as they say, the Internet is going dark. And we've got some questions that highlight that aspect of it that we'll be getting to here next. So their answer to being unhappy is generally to solve that problem. And it's like, oh, great.

Leo: Jason in Texas says: NSA spying, how can I protect myself? I've been listening to the show for a long time, and from everything I've learned from you I have many ideas about what I can do to protect myself. But I'm hoping you'll talk about this present instance in particular. What are your thoughts on combining VPN with Tor? VPN before Tor or after Tor, or even is it a good idea to combine VPN with Tor? Go ahead, Tor.

Steve: Yeah. And this is representative of many questions that I saw, so I just chose Jason's. The thing that stood out here is that there are many VPN providers that will not let you use Tor, for whatever reason. I don't know what their logic is. The Tor network

doesn't prohibit you from doing anything you want to. So the VPN, in order to - in order for a VPN to block you, you'd be connecting to their server, and then their VPN server would have to refuse to allow you to then run through the Tor network.

Turning this around, if you use Tor first, then you'd come out of the Tor network and attempt to connect to the VPN server. And so again, the VPN provider would have to be refusing to accept a connection out of a Tor endpoint. I have heard anecdotal reports that people have had problems using both a VPN and Tor through some policy-based blocking on the VPN side. I just haven't pursued it any further because it felt a little bit tinfoil hat to me, though I can recognize someone's concern.

From a broader basis, Jason is saying, how can I protect myself from the NSA spying? And I don't have a good answer. I mean, I don't think you can. I think what one of the takeaways from last week's podcast was - and the reason we did it, I mean, the reason, what we try to offer here is the technology and the solutions that that technology implies and solutions that are available thanks to the technology. We just looked at the possible compromise of the public key infrastructure. Not, I mean, seems very unlikely to me. But it's possible. And unfortunately, one of the things we always see is what is possible ends up happening.

So this is why I don't think it's safe any longer to rely on SSL for privacy. This is why I've been saying pre-Internet encryption. There the notion was not to trust the link and not to trust the cloud storage provider. Only trust yourself, or TNO, Trust No One. Unfortunately, I think to a large degree than has been felt previously, the TNO really needs to extend now to the public key infrastructure because it does rely on us trusting certificate authorities and on what they're doing. So, now, how do you protect yourself? I think you just need to - you have to assume that, unless you control the crypto, it's not in your control.

Leo: And even that might not be sufficient because of the metadata. So, for instance...

Steve: Ah, very good, very good point. Yes, I'm glad you said that. Yes, yes, yes. Yes, very good point.

Leo: So I encrypt - I can encrypt email till the cows come home. In fact, it's very easy to install GNU Privacy Guard, which is an open source PGP implementation that's excellent and simple and trivial. It's very easy to install on the Mac and Mac Mail and use it. But they can still see who I'm sending stuff to, and when, and how often. They can see who that person sends stuff to.

Steve: I think that Silent Circle may be preventing this. And I think that Threema may also be. The point is they are using, rather than doing peer to peer - the problem with peer to peer is it leaves metadata. The only way to prevent metadata is to have a metadata, I mean, have a connectivity provider who is specifically against spying. One of these, and we get to a question about it later - oh, it's the Whisper guy. We already know that that's Moxie Marlinspike. Well, I would deeply trust Moxie.

Leo: Trust Moxie, yeah.

Steve: Yes. His whole business model. And he's - was he Silent Circle? I can't remember which was which.

Leo: I think he was - Silent Circle was Phil Zimmerman was involved in that one. That's the PGP guy.

Steve: Okay. But so anyway, the idea is, if everybody connects to a central hub - and I do know that I just read, when I was looking at Threema, they arbitrarily pad the message length with a pseudorandom nonsense and length so that they - in order to prevent the association of, you know, to identify packets by size as, for example, they move through Tor. So there really are some good technologies. And I have a feeling we'll be focusing on these in coming weeks, the types of technologies that really are going to the next level to thwart passive eavesdropping and both metadata and privacy violation. It's certainly not easy. I mean, it's really going to - it ups the ante.

Leo: Yeah, I mean, so I can encrypt. And so one would want to encrypt one's data before one puts it on the Internet, pre-Internet encryption, or PIE. But then one would also want to hide the transactions themselves. So that would mean using something like Silent Circle. And then, finally, one should throw away one's cell phone because there's no way to prevent that, if you're going to be on a network, unless somebody comes along and provides a Silent Circle-like cell phone network.

Steve: Someone did mention that, in addition to connection metadata, companies were keeping, like, dynamic cell phone tower presence metadata.

Leo: Yeah, location, location.

Steve: But I don't know that, that, like, all - like right now I'm a Verizon user. Is Verizon, like, caring where I am unless they don't need to specifically look?

Leo: No, they totally store that.

Steve: Oh. That's bad.

Leo: That's the pen register stuff.

Steve: That means that they can unwind the history of your location all the way back in time.

Leo: Yes. Right. So don't carry a cell phone.

Steve: Goodness. Or just keep it turned off. Well, no, because when you turn it off they'll...

Leo: Just don't carry it.

Steve: Yeah, yeah.

Leo: You can't have it. So a pen register is this whole idea of there is no warrant necessary to request location data from a cell provider. And in fact...

Steve: But, wait, location history also?

Leo: Yeah.

Steve: Oh.

Leo: I'm pretty sure they're saving all of that.

Steve: That's just a lot of data. But on the other hand, we do have - we have five zettabytes. It's got to go somewhere. Wow. It's like, where everybody is all the time.

Leo: Yeah.

Steve: Is what this means.

Leo: Well, what that would be is a request to Verizon, AT&T, Sprint, and T-Mobile, would you mind keeping that for some length of time? And we'll just come and get - we'll fetch it. You don't have to keep it longer than how often we visit.

Steve: Well, business records. I mean, that's the whole deal is they...

Leo: Business records, right.

Steve: Yeah.

Leo: I mean, I think they've been saying all along that that is for sure there. But you're nuts if you think you're private in any way if you carry a cell phone.

Steve: Yeah, yeah.

Leo: That's nuts.

Steve: Yeah. Actually, I will say that mine, I've got apps that keep asking to turn on location data, and I just say no. I mean, I don't need - I'm not a map user, so I don't need everything. I don't want my location being tweeted out whenever I tweet something. It's like, no, no, no.

Leo: See, I don't - this is, I guess, this is the point that I've always made, which is people are so worried about Google and Facebook and other people knowing where you are. And that seems to me, I mean, that's for commerce. I don't - I'm not - I don't really worry about that. I'm much more worried about the fact that the government and law enforcement at all levels are able to get this data, able to store it, able to use it against you in the future. It's pre-crime.

Steve: Yeah.

Leo: So let's say they arrest me someday for something, and they say, we've got to build a case against this guy because this case is weak. Now they go and they request all the things I've done for years. And they shift through it, and they look for, you know, it's a federal crime, it's a felony to violate a website's terms of service. That's a federal crime.

Steve: What?

Leo: Yeah.

Steve: A felony?

Leo: Yeah.

Steve: My goodness.

Leo: So there's plenty - we are all committing felonies all the time. If you've ever signed up for a Face- you know, the kids who sign up for a Facebook account, and they aren't 13 yet, that's a felony.

Steve: Wow.

Leo: So go back through that stuff, find all these little ridiculous things, and...

Steve: Wait a minute. Is ad-blocking violating their terms of service?

Leo: I bet it is.

Steve: I'll bet [laughing]. Oh, great. Yeah, okay. That's - just take us away. Just, you know, put our wrists together. Wow.

Leo: That's the - by the way, that's - I should point out, that's the Justice Department's interpretation of the Computer Fraud and Abuse Act.

Steve: Well, and that's, of course, what the intelligence agencies would ask...

Leo: Right, well, and that's what they were getting Aaron Swartz on. Aaron Swartz's prosecution was based on his violation of the terms of service of that database that he downloaded. So, yeah. So the point being that I think, if they have enough data about what you do, they can find stuff. They could build - they could build a case against you. So it's really a question of do they want to build a case against you or not.

Steve: Right, yep.

Leo: And one of the reasons they say, they explicitly say, the reason we save this data is so we could build a case against you should we want to go get you someday. So you just really have to trust them. So in other words, I don't care if - I'll turn on location on Path and Google and Foursquare. I'm not worried about them. It's the feds you worry about, and they don't need you to say yes. They've got it all. Feds, local, whoever. "Chill" in Washington, D.C....

Steve: Perfectly timed name.

Leo: Yeah, Senator Chill. A couple of comments about PRISM. First, good catch on the importance of metadata. You missed one crucial detail: frequency. Cell phones need to send keep-alive messages to the tower every minute or so to keep registered...

Steve: Oh, great, it was perfectly timed.

Leo: ...and let the network they're still active. Location data and other info are included in these keep-alive messages, so they have more location data just than when you make or receive a call. Yeah, we've known that. Second, the device used on the AT&T network over in San Francisco was a NarusInsight Manager, now known as Narus nSystem. We've talked about that.

Steve: Yup.

Leo: And we mentioned the prism graphic. The original brochures have been replaced with something much less informative. The old ones showed something like Wireshark on custom ASICs capable of deep-packet inspection in real-time on a 10GB - what's a GbE link?

Steve: A 10-gigabit link, Ethernet link.

Leo: Ethernet. 10Gb Ethernet link with room to spare. That was seven years ago. Penultimately, how about putting a shout-out to the audience to see who can come up with a tool to rid ourselves once and for all of the Hong Kong Post Office and their ilk. My idea is a program or plugin that keeps a log of root signers of every certificate your browser encounters. Find out who's needed in the root list and who isn't, then just delete the latter from our certificate stores. Maybe a place to submit lists and create a map of certificates and their signing trees.

Finally, correcting an error. You said when an email server sends mail via SMTP it is in the clear. That isn't always true. SMTP over SSL/TLS is RFC 2487, posted back in 1999. That means SMTP-to-SMTP server communications can be set to "opportunistic," to happen when the destination server supports it, or "required," for people who are really paranoid. "Required" is a configuration used by many government agencies when sending mail to other government destinations, .gov destinations. All SMTP communication between the various .gov servers are encrypted using TLS. I bet you that's about the only place it's used. But thanks for educating the masses on the importance of security.

Steve: So, yes. Starting from that issue, there is a protocol called STARTTLS which was added to SMTP. The problem is, unless, for example, you can mandate that all .gov, exactly as you said, Leo, SMTP servers are going to only exchange email that way, you can't exchange email with the rest of the world. And my email server that GRC is using is state-of-the-art, very recent, does not offer that even as an option. So it's still not there.

I do use SSL for all - and that's one of the reasons I set it up. We've got secure connections for all of our client, you know, myself, Greg, and Sue, all of our connections to our own server are absolutely SSL. But the SMTP to SMTP, as I said last week, when the email from us leaves our server and goes elsewhere, it cannot be SSL. I mean, maybe some percentage. But you cannot require it. And, for example, I can't receive it because my state-of-the-art SMTP server doesn't even offer that as an option. So it actually has not happened effectively in the real world yet.

And this note that he has about certificate stores, there's an interesting technology that changed with Vista that never received much attention. Vista had it, and Windows 7 has it. Server 2003, I think, has it, but I'm not sure. It may not. But I know that 2008 has it because I encountered it. And that is, the Vista OS that everyone is using and Windows 7 OS and GRC's server and I'm not sure how far back it goes, they don't come out of the box with the entire, every certificate authority you ever heard of, Hong Kong Post Office and company, certificates. They start with about 12. And it's a little bit of a concern, actually, because when the server encounters an SSL connection that is anchored in a certificate authority whose certificate it doesn't already have, it goes and asks Microsoft.

Leo: We need a certificate. Hey, what have you got?

Steve: Yeah. Yeah.

Leo: You know these Hong Kong guys? Who are they?

Steve: And unfortunately this means that Microsoft indirectly is able to monitor all of their Vista and Windows 7 and late-model server connections for which certificate authorities they have ever asked for certificates from. Now, if that annoys you, you can download the master pack, which is like 400 and some certificate authorities, and not use this dynamic approach. But the default for from Vista on, on the consumer Windows and 7 and 8 and also on 2008 and on, and I think an earlier version, but I don't remember where that started on the servers, it is to ask for certificates on the fly. So you still end up with a well-populated store. It just takes a while as that sort of matures. And then of course the rate at which you're asking for ones you don't have drops off because you end up with a large collection, but, nicely, only the ones you've actually needed to use, not just every - not the whole kitchen sink collection. So a bunch of good points there, thank you.

Leo: And are we still really worried about Hong Kong when you could worry about Washington, D.C.?

Steve: It's, yeah, Hong Kong is benign. But that's where Edward...

Leo: That's where Snowden is.

Steve: That's where Snowden went, yes.

Leo: Hong Kong's the new freedom.

Steve: The protection of Hong Kong. Oh, uh-huh.

Leo: Where was it Humphrey Bogart was going, the Free French Resistance? Greg in Kansas wonders: iMessage and FaceTime secure from NSA snooping? He quotes an Ars Technica article, which probably refers back to the Apple post, but we'll see. Does iMessage utilize pre-Internet encryption like LastPass does? If so, should be secure from NSA snooping as Apple claims. But who holds the keys, Apple?

And Dustin Schumm in Michigan wonders somewhat similarly: Can Apple or cannot Apple decrypt our iMessages? In the privacy statement Apple posted on its website just this week, they say they can't decrypt iMessages. While it may be end-to-end encryption, how can they provide history to new devices if they don't have the key to decrypt? When you put a new device on iMessages, it has all the old messages on

there. I would guess that, when I sign in with a new device, I download the key and my new device is now able to decrypt the messages. Apple probably hasn't given any technical explanation. But Steve, do you know how it could even possibly work without Apple being able to decrypt my data?

Steve: No, I don't. And this brings up, I think, the next point, Leo. I'm finding myself strongly leaning in the direction you've always been, which is, if it's not open source, we really can't trust it. And that's the problem with iMessage. One of the things we know, because the protocol is closed, but there was a researcher who installed it, or like an early version of it, or I don't remember quite what the scenario was. But there was an iMessage on his Mac OS X system. And because he was a developer and had the tools, and it was on a Mac platform that he had access to, he was able to do a lot of reverse engineering. And I remember looking at the protocol, and it just made your eyes cross. It was unbelievably complicated.

Leo: Kinda not so good, either; right? I mean, kind of, like, convoluted.

Steve: Yes. Yeah, and that's a problem with crypto. The more complicated it is, the more opportunities there are for mistakes. And it isn't - it doesn't have to be complex anymore. We know how to solve these problems easily. So Apple's iMessage protocol is proprietary. They're needing to assure people that they're safe. Well, it uses end-to-end encryption, they say. And I believe them. But unfortunately, apparently it's also stored. And so we assume it's stored in encrypted format. Yet somehow, as has been observed many times, you bring a new device online, and it receives your iMessage history. Well, is it coming from other devices? Is it coming from Apple? I mean...

Leo: It says Apple - they say specifically, Apple cannot decrypt that data. Yet magically unencrypted data appears on my new MacBook Air when I log into iMessages. This Air doesn't have any previous keys.

Steve: Right.

Leo: Maybe the key is stored in my Apple account? Because you do have to log in. Now, I think this might make sense. I have to log into my Apple iCloud account to use this machine.

Steve: Yes.

Leo: I have to associate messages with that.

Steve: Yes.

Leo: So perhaps there's a key there Apple doesn't have access to.

Steve: So assume, I mean, we could try to engineer a solution by saying that the end user has to provide authentication for his iCloud account, which Apple does not have. Apple has presumably hashed everything. So, and presumably...

Leo: Right. That makes sense. You could do that.

Steve: So the hash - yes. So but again - okay, yes. So Apple hashes everything. They can verify your information, but they cannot recreate your information, your authentication information. And so they've designed a system where you must authenticate yourself. And when you do, that authentication is used to decrypt your iMessage store and to then repopulate a new device's iMessage history. And so, okay, yeah, that makes sense. I'm not trusting it, not given what we know. I'm not trusting it because it's not open. I'm not trusting anything now, a messaging system that large corporate entities like Apple are hosting, unfortunately.

The good news is there are alternatives. We'll be talking about them, I have a feeling, a lot more in the future. But we know that the FBI, NSA, CIA, whomever, is able to now compel Apple to divulge information. And Apple's not telling us how their systems work, their closed protocol. As far as I'm concerned, that rules them out in us considering them sufficiently safe, when there are free known open protocol alternatives.

Leo: Like Cryptocat.

Steve: Yes, like Cryptocat.

Leo: This doesn't in any way compromise Cryptocat.

Steve: Like Silent Circle. Like what we're going to be talking about here in the next question.

Leo: Our final question, Dennis Downing, Jr., Staten Island, New York. He wonders specifically about TextSecure. It's from a company called Whisper Systems. First off, I don't know if I could get by in life without your show. I've listened to every episode at least twice. You and Leo do an extraordinary job. The shows are very informative and exciting for me. Hope many more years of podcasts to come. Wow, that's nice, thank you.

I have an Android phone. There is a free app called TextSecure. It gives you end-to-end encryption with text messages. I've been using it for a while. It looks like it might do the trick. I wanted a professional opinion, if you wouldn't mind. They have another app called RedPhone. Oh, I have RedPhone. I'm familiar with that. Does the same thing with voice calls, from what I understand. I have noticed that the downloads of these apps have soared since the NSA news came out. I'm keeping my fingers crossed that using the apps may be a solution.

I must say, if this is truly an app that works, anyone, and I mean anyone, can use it. It's super easy. You press a lock on top of the text message interface. It initiates key

exchanges automatically. There's also an option for you to verify keys with the recipient, I would assume to make sure there's no funny business with a man in the middle. If you could touch on this app on your show, if it works, I think it would be an amazing benefit to anyone who uses it. It's WhisperSystems.org.

Steve: And that is Moxie Marlinspike's app and his company.

Leo: Aha. And as we've said, and I'm glad you've come around on this one because I know when we first started this show - I've always said I don't use encryption that's not open source. And I think you now agree.

Steve: Yeah, well, I do. Well, I wanted to do a commercial one, and it wasn't going to be open source. And now it's like, I'm not doing a commercial one.

Leo: Has to be open source. And this is on GitHub. Whisper Systems has posted the source code. So that means you can validate it. You can...

Steve: So there are, yeah, he has two platforms. Right now it appears to be - I'm sorry, two apps. This is Moxie does. And his whole deal is we can make encryption, absolutely unbustable encryption, easy to use while absolutely secure. So this is Android platform only at the moment. But two apps, one for text and one for voice. RedPhone is similarly Android-to-Android audio encryption, courtesy of Whisper Systems and Moxie Marlinspike. I will dig deeper into them in the future, I am sure, and look at, for example, does it provide metadata protection. I am absolutely sure that they've solved the problem of privacy and authentication.

Leo: But the problem with metadata is, if you're doing it over a cell phone, well, of course the metadata about the transaction is still visible.

Steve: Right.

Leo: As always. I see an iOS source code repository, so there may be an iOS version of TextSecure. We'll have to look.

Steve: Now, I guess one of the things you could do with a cell phone is you are able to put it in airplane mode, or turn the cellular modem off.

Leo: What you need is a burner that's not associated to you. You need to go to the drugstore, pay cash...

Steve: Well, or use WiFi instead of cellular.

Leo: I have a feeling WiFi would be just as bad. The problem is, if you're - okay. So this phone, if I'm not on the cellular network at all, I guess I'm okay. But if I'm on the cellular network, and I use WiFi, the cellular network still sees the location given from the WiFi.

Steve: Yes.

Leo: So you have to really - I think the best thing is you need a phone that's not associated with you. But as we know, that's the problem with metadata is it only takes a few data points to start being able to figure out who's whom.

Steve: Yeah.

Leo: But that's why drug dealers throw their burner phones out every week.

Steve: Do they?

Leo: Yeah. According to "The Wire," yes. Have you seen "The Wire"? Have you watched that show?

Steve: Oh, my god, are you kidding me? Oh, wow, yes.

Leo: That's where I learned everything I know about drug dealing and burner phones.

Steve: Okay. We're glad for that. What we need is - there was the...

Leo: Remember they sent Bubbs all over town buying burner phones? Yeah, all right.

Steve: "The Wire" was a spectacular HBO series. The thing we need, there was a neat privacy guy who - he objected to the idea that the supermarkets were using the little loyalty tabs? And so whenever he was in line at the supermarket, he would exchange them with the other people in line, just to sort of scramble up the database.

Leo: There you go.

Steve: So what we need is we need a burner phone interchange system where every week a bunch of people get together in a big circle, and they hand their phone to the person on the left.

Leo: And make sure there's no cameras taking pictures of who's going in and going out.

Steve: Exactly. And then you all disperse, and that'll just scramble up the database.

Leo: Hmm. I'm just going to tell you, once this paranoia begins, it's turtles all the way down. There's no endpoint where you go, now I'm safe. Steve Gibson does his best, though, to protect us. And you know, the most important thing is to understand what's going on, what the risks are. And I hope...

[Talking simultaneously]

Leo: ...this conversation.

Steve: I should be wearing tinfoil this week.

Leo: I wore a tinfoil hat in the last TWiT.

Steve: I saw you.

Leo: [Laughing] We've got to get you on TWiT. In fact, I've been meaning to get you on. I don't know what you do Sunday afternoons.

Steve: I'm available.

Leo: I'll have Chad give you a jingle.

Steve: Okay.

Leo: Steve Gibson is the guy in charge of Security Now!. Every Wednesday he comes on here, and we - it's just - it's rapidly becoming a must-listen show for anybody who wants to understand this stuff.

Steve: It's like this. Like what you've just heard.

Leo: Yeah. Only more.

Steve: Yeah.

Leo: We will be doing this next Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 18:00 UTC, right here. So tune in live. But if you like to fast-forward through the boring bits, you can always download on-demand audio and video after the fact. Now, Steve has the teensy-weensiest audio, which is the 16Kb version, on his site, GRC.com. He also has transcripts, which make it very easy to fast-forward.

Steve: And I have to say the transcripts for last week's episode, 408, they're just wonderful because you can quickly scroll by and, like, see where there's a big blob where I'm talking nonstop. It's like, oh, oh, here's Steve talking about something.

Leo: Yeah. Yeah, you can see the little - they should make me red. And then the little black black black black black black black, red. That's GRC.com. While you're there, if you've got a question, GRC.com/feedback. Pick up a copy of SpinRite. Free upgrades forever, guaranteed by Mr. Gibson. So don't say, oh, I'm going to wait for the next - no.

Steve: You need it.

Leo: Get it now. You need it now. You should also get all the freebies, including...

Steve: And actually, if you get it now, you can play with the pre-release versions, too.

Leo: Oh, you can. Ah.

Steve: Oh, yeah. Yeah.

Leo: There you go. That's a good reason to go to GRC.com. You just have to hack the URL. No, you don't. Just add a 6; right?

Steve: Yeah. We'll provide instructions.

Leo: There'll be a link there, I think.

Steve: There will.

Leo: Thank you, Steve. What a great show, as always. My level of interest is rising as the government's level of interest in us is rising.

Steve: Yeah.

Leo: You know what I mean?

Steve: It becomes important, unfortunately.

Leo: Yeah. Thank you, Steve. And we'll see you next time on Security Now!.

Steve: Thanks, Leo.