Listener Feedback #172

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-415.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-415-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. He's going to answer 10 of your questions. He's going to talk about security issues. Yes, there's another slide from the Edward Snowden deck. We'll talk about what that all means, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 415, recorded July 31st, 2013: Your questions, Steve's answers, #172.

It's time for Security Now!, the show that protects you and your loved ones and your privacy online and your security online. Couldn't better be a better time to do a show like this, as we've said for the last six years. Steve Gibson's here, the Explainer in Chief, from GRC.com. He's the creator of SpinRite, which is his bread and butter for many moons now. Is it 20 years now, Steve?

Steve Gibson: 25, my friend.

Leo: Holy cow. Holy cow. But in the time, because SpinRite's been such a nice little daily earner...

Steve: Purring on.

Leo: Purring on.

Steve: Also thanks to our listeners, many of whom have purchased it just to support...

Leo: Isn't that nice.

Steve: Yeah, it really is.

Leo: It's given him a little time and the inclination, I think, to investigate, first spyware. He was the man who coined the term "spyware" many moons ago when he first discovered it and created the first antispyware tool. He's created many other free tools at GRC.com. And for the last 415 weeks - that's amazing - we've been talking about security on the show. And you know, the show's gotten longer and longer and longer because there's been more and more to say.

Steve: Well, it's funny, too, because we introduced the concept of not trusting your data to the cloud several years ago and coined the term "TNO" for Trust No One. And here we are now, I mean, it's like it's come full circle because now we absolutely know, with no doubt, and we're getting increasing level of detail, in fact, that the government and global governments have for some time been recording everything that's been done on the Internet. And so there was a tweet that went by, and it didn't really catch me, but the guy was making - he was referring to our conversation, the dialogue we've been having about the whole concept of privacy, like the notion of, well, why does it matter if you're not doing something wrong? And he said, well, I don't want a webcam in the bathroom. And I thought...

Leo: It's not like you're doing anything wrong in there.

Steve: Exactly. But, I mean, there is this notion of not being watched as something valuable, just the concept of not being on some weird reality TV show. And it turns out, as far as the Internet goes, that's pretty much the situation. Just today, this morning, another piece of new information, part of the continuing Snowden drip of disclosures...

Leo: That's kind of disgusting. Okay. Yes.

Steve: Well, just say that the Snowden is melting. Yes, we have - anyway, Glenn - and it's funny because on the website it's G-l-e-n-n. And I'm very particular about getting these things right. But I'm sure I've seen it with one "N" elsewhere. So it's two N's for everyone who's as crazy about details as I am. Our friend Glenn Greenwald has been saying that there would be additional stuff coming. And every time interviewed, one of the questions that the talking heads say, well, do you have more coming? He says, oh, yes.

Well, today we learned about XKeyscore, which is the name of the program, from the Guardian. Now, I have to say it continues to ratify the theory we first put forward about what PRISM was. And nomenclature is crazy in all of this. And in fact it might have been Bruce in one of his other blog postings, Bruce Schneier, who commented that our intelligence services were using acronyms as obfuscation in order to just confuse the legal system and legislators, and also to create this deniability where they could say, well, it's PRISM doing this. And then, with a straight face, the intelligence person could say, no, that PRISM does not do that. Because XKeyscore does that, or Slimy Underworld

does that, or whatever their random program names are.

So what we have now, as of this morning, is knowledge of - on the Guardian's page there's a link to a scrolling series of slides which are amazing in detail. For example, we now know that it's a massive distributed Linux cluster is the architecture for this. So what Glenn and Snowden disclosed are slides which show that the NSA collects, quote, in their own words, "Nearly everything a user does on the Internet." XKeyscore gives "widest reaching," in quotes, collection of online data. NSA analysts require no prior authorization for searches. So they can search anything they want to, any time they want to. And it sweeps up emails, social media activity, and all browsing history. And the word "all" is, like, littered throughout this. And it's a little frightening when you see where they're saying "all."

So there are presentation training materials that have been posted showing really interesting new detail, which is the reason I'm talking about this, is it's not the same old stuff. It's like now we're getting more stuff. For example, they use an acronym DNI, which stands for Digital Network Intelligence. And in the slide it says "DNI Exploitation System/Analytic Framework performs strong (e.g. email) and soft (content) selection. Provides real-time target activity," which they refer to as "tipping." And then, get this, "rolling buffer of approximately three days of ALL" - all caps, their emphasis - "unfiltered data seen by XKeyscore."

So this is - we've never had this before. This is news. This says - now, we've talked a lot about the quantity of information that is passing through these taps which they have. And as we'll see in a minute here, the architecture as this onion is being peeled continues to substantiate my notion that this is outside of the major cloud service providers because none of this would be necessary if it had their cooperation. So this is tapping Google just upstream of the datacenter where the data is raw.

And so now what we're seeing is that they're storing everything that goes through, as they refer to it here, "all unfiltered data" in a "rolling buffer," which again, if they said, Steve, we want you to design something for us, this is the way you do it. This is how a computer science person would tackle the problem of too much data coming through to store it all, yet you need to be able to look back in time to perform searches. So the raw data is essentially in a big scrolling buffer where you always have the most recent three days. About after three days you start losing it off the end of the buffer as new data comes in because you just run out of your short-term buffer space.

So it says stores what they call "full-take," full hyphen take, so that's their jargon for "everything," full-take data at the collection site, which is then indexed by metadata. So as this all pours in, they're pulling metadata from it which are email, and actually they enumerate those in a minute, email addresses, phone numbers, names, like sort of formatted keyword searching on the raw data which is then indexed on the fly, allowing them to then do queries against the metadata and then, within this three-day period, to extract from the buffer of the so-called "full-take data" specifically what they want.

And then it says "Provides a series of viewers for common data types." And once again, that's exactly what you'd expect. They'll have an email viewer. They'll have a chat dialogue viewer. They'll have an NNTP viewer. They'll have these viewers which know how to take, which know how to format the raw data which has been just sucked up en masse out of the stream and presented in a same format. They'll have an HTTP viewer, for example, something that knows how to reconstruct the web page just as a web browser does from the raw data, and also to show the web page metadata, the query and the response headers.

Then they call this also a "federated query system," where one query scans all sites. Now, this is also amazing because amid these slides is a picture of the world showing red spots wherever the NSA has planted one of these facilities. And it's in more than 150 sites, with more than 700 servers, literally all over the globe. And so what we're saying is that they're tapping major data feeds in all of these locations. And then this federated query system allows an analyst, presumably sitting somewhere in Virginia - or wherever, apparently Snowden was able to do it in his little bungalow in Hawaii - to insert a query into the system which then goes globally, and then all of the databases in all of these systems around the world in this federated query system are simultaneously asked for matches.

And so under Federated Query System it says, "One query scans all sites. Performing full-take allows analysts to find targets that were previously unknown by mining the metadata." So as this bulk of data goes by, it is being examined and metadata extracted from it and stored separately from this so-called "rolling buffer" of three days of everything. So under a slide called System Details, they say massive distributed Linux cluster, over 500 servers distributed around the world. Elsewhere they say 700. System can scale linearly. Simply add a new server to the cluster. And then also under system details they said "federated query mechanism," which we just talked about.

Then they talk about the analysis plugins. And these are these so-called, I would call them semantic analysis, where they need to extract the meaning from the raw data. I remember, Leo, just after we finished the first podcast you switched over to This Week in Google, and Gina had a problem with this notion that you could get meaning from the stream. And the way of course you do that is exactly like this.

The stream itself is raw data. But it's only because a web browser expects the format to be something that it's able to show it to you as a web page, or an SMTP reader, an email system, expects the format to be email, that it knows how to show it to you. So it's only a tiny step further to look at the raw data. And any human can do this. We do this all the time when we're doing packet-sniffing on the raw wire. You can see, like, what the headers are and the way it's formatted. It's like, oh, these are email headers. Oh, these are HTTP headers. Oh, these are newsgroup headers, or chat format.

So the idea is you start with the raw stream. You apply a simple heuristic recognizer to it, to determine what type of stream this is. And then you say, ah, you recognize what it is, and then you apply one of these plugins to format it for full recognition. So they say "Email addresses: Indexes every email address seen in a session both by username and domain. Extracted files: Indexes every file seen in a session, both by filename and extension. HTTP parser: Indexes the client-side HTTP traffic. Phone number: Indexes every phone number seen in a session."

And then they have in parens, "(e.g. address book entries or signature block)." So, for example, when email goes by with a signature block in it, bang, it locks onto that and indexes phone numbers and the metadata in the signature block. "User activity: Indexes the webmail and chat activity to include username, buddy list, machine-specific cookies, et cetera."

So more data is coming out. If anyone's interested, this is all over the news now, so you could go to the guardian.uk.co, or co.uk, rather, and track this down. And there's a long article where Glenn pulls this apart and essentially parses what new has been learned from this. And it is additional details that are a little chilling about the scope of this project.

Leo: Yeah. You know, I want to raise one point which - I don't know.

Steve: Yeah, do.

Leo: Maybe this is a little conspiracy theory-minded. It is in the strong interest of the NSA and the U.S. government to have terrorists believe that they know everything. Right? And I'm often puzzled. In some ways they claim capabilities far beyond those we know to be possible, like decrypting strongly encrypted stuff. I'm wondering if some of this is merely disinformation. We mentioned this last week as the "panopticon theory," that the watchers would love it if all the watched believed that the watchers could see everything. So there is a - the truth is that the NSA gains by all this information.

Steve: I don't know. I really think that our intelligence system has taken a huge hit. I mean, this has hurt the intelligence community. This is not - in no way is this good for them.

Leo: Okay.

Steve: I really think, I mean, I know I feel differently. It's one thing to sort of suspect, oh, well, maybe this is going on, and something else to just have the dirty laundry aired like this.

Leo: Right, right.

Steve: I mean, this leaves no one any doubt. And these are - it's not like this was leaked, like, oh, whoops, we gave this to a senator, and we didn't intend for him to let his staff fax it.

Leo: Yeah, that would be the easy way to do that, yeah.

Steve: Yeah, I mean, this truly was, I mean, this really was a bad guy, well, I don't mean a bad guy, a person who broke...

Leo: A bad guy only in the belief of the Department of Justice. Let's put it that way.

Steve: Yeah. As I said, I'm not unhappy that this has come out because there's no way this is not going to force a seriously necessary reexamination of the system that we had put in place post-9/11. And it may well be, as I said last week, we may just end up saying, well, that's the price we have to pay of having the surveillance that we need in order to detail with asymmetric warfare, which is the nature of terrorism. And so be it.

Leo: Well, isn't that exactly what happened a couple of days ago in the House, when they overturned the defunding of the phone taps?

Steve: Yeah, but it was, it was a close - close, Leo.

Leo: It was close.

Steve: I was very surprised that it was 215 to 210 or something like that [205-217]. It's like, wow. That really surprised me that, yeah, pulling funding...

Leo: However, the will does not yet exist to stop this.

Steve: No.

Leo: And I think it makes sense because you don't want to be the representative who voted to stop it, and then there's a terrorist...

Steve: I know.

Leo: ...attack, and you look like you're the guy who made it possible.

Steve: Yeah. I don't think blanket defunding was the solution, which is why I said last week that I thought this vote was coming up too soon. It takes, you know, these wheels do not turn slowly. And it is all politics. And I don't have any, I mean, I'm just - as an observer, it's like, well, we'll report what we know, and we'll see how the cookies crumble. And it's like, it is what it is. I have no power to change it one way or the other. My interest is in the technology, which I think is fascinating and interesting, and also in finding that the technology-driven line where, okay, email is probably not encrypted as it comes and goes. But web services increasingly are. So what does that mean?

And then we find out last week that there is in fact pressure to turn over the private keys of web servers so that they can decrypt because, as we would expect, increasingly web traffic is encrypted. So that's where I think our proper place is, rather than taking a position. I just - I have no interest in taking a position because there's nothing I can do about it.

Leo: Well, you'll be pleased to know I'm getting now a fairly steady volume of people testing out their PGP keys and saying, is this encrypted? Is it working? And I do respond to everybody. My PGP key is, if you want to get the key, is available at Leoville, my personal website, Leoville.com.

Steve: Well, we end this podcast with a couple PGP-related questions because it will take us into next week which is going to be all about PGP.

Leo: Good. Good, good, good. Okay.

Steve: Now, this is not at all security related. But I just sort of shook my head when I saw this. It's like, oh, you're kidding me. We all know how Microsoft named their new OS "Metro," and then turns out they didn't have trademark rights to Metro. Well, they just lost the lawsuit on SkyDrive. After all the...

Leo: Holy cow.

Steve: Can you believe it? After all the time and energy they put into it? So the BBC posts: "One month after a British court ruled that Microsoft's SkyDrive infringed..."

Leo: Unbelievable.

Steve: I know. It's unbelievable, Leo, "infringed on a British Sky Broadcasting (BSkyB) Group trademark, Microsoft has decided not to appeal and will find a new name for its cloud storage service."

Leo: Wow.

Steve: You know, they're paying their attorneys too much for patents and not enough for trademarks, apparently. It's like, Microsoft, get a clue. "British Sky Broadcasting offered an online storage service called 'Sky Store & Share' between 2008 and 2011..."

Leo: Really? Really?

Steve: "...and it has trademarks such as Sky+, Sky Digital, Sky Broadband, Sky Go, Sky Mobile, Sky Bet..."

Leo: They own "sky," huh?

Steve: Yeah, and Sky Photos. And so Microsoft tried to get SkyDrive, and they said no. The press release quotes...

Leo: I'm actually feeling sorry for Microsoft, to be honest with you.

Steve: ...British Sky Broadcasting saying, "We are pleased to have reached a settlement after Microsoft agreed not to appeal the trademark infringement judgment in relation to its SkyDrive service. We will remain vigilant in protecting the Sky brand and will continue to take appropriate action against those companies who seek to use our trademark without consent."

Now, of course we know Microsoft would have been every bit as crazed if anyone called Windows something, Windows this or Windows that.

Leo: Yeah, oh, yeah, yeah.

Steve: They would have stomped the crap out of them in a heartbeat. So it's like, but, you know, come on, Microsoft. Do your homework. So I just wanted to let our users know SkyDrive - what happened is there was an undisclosed payment made - oops - and Microsoft has been allowed to continue using the name while they phase in their replacement name.

Leo: Wow.

Steve: So they're going to have to go find one. It's like, oh...

Leo: It is tough nowadays. I remember even back in 1994, when we were trying to - or '95 - create the site for MSNBC, they needed a name that hadn't been used, wasn't trademarked, and had a dotcom that they could use, et cetera, et cetera. And it's always getting harder, it seems like. That's why - people wonder why all the baby talk names with new startups. Now you know. Because you can't use a real word. They've all been taken.

Steve: Yeah.

Leo: So Microsoft's going to call it "Ishkabibble" or something, and we'll all get used to it.

Steve: Leo, that's been taken.

Leo: Yeah, it has, actually, the 1920s movie star.

Steve: And you just said it.

Leo: I own it now, baby. Prior art.

Steve: Yeah, I mean, it is the case, I know that when I've been looking for product names and associated domains, I've kept it quite close to the chest until I nailed it down because...

Leo: It's become amazing.

Steve: Yeah, it is crazy. So in crypto-related news, some researchers in the U.K. and the Netherlands cracked the crypto, and unfortunately it's an RFID standard, known as Negamos, or, I'm sorry, Megamos, Megamos maybe, crypto, which is used by a whole slew of Volkswagen-owned luxury car makes and others. They gave Volkswagen and companies nine months' prior notice that they were going to explain what the problem was. And this was going to be a paper presented next month at the USENIX Security Symposium, and it got stomped on a couple days ago by a judge.

The BBC reported that "The researchers said they'd obtained a software program from the Internet which contained the algorithm devised by [a defense company] Thales to provide the security feature. They said it had been on the 'Net since 2009." So they discovered a weakness in the code which had been published on the Internet, showing that it could be compromised, and added that there was a strong public interest that the information be disclosed to ensure the problem was addressed.

"However, VW and Thales argued that the algorithm itself was confidential information" - once again, even though it had been on the Internet since 2009 - "and whoever had released it on the 'Net had probably done so illegally." Therefore, they said, "there was good reason to believe that criminal gangs would try to take advantage of the revelation in the academic paper that was going to be released to steal vehicles. The researchers argued that this risk was overblown since car thieves would need to run a computer program for about two days to make use of the exploit in each case." So this was a brute-force crack against a specific instance of the RFID crypto used on a given car. Which still doesn't mitigate it. I mean, if this is a Lamborghini, and by the way, that was one of the brands...

Leo: It was very high-end cars. It wasn't cheap cars.

Steve: No, no, no. And so they said that removing the sections - so first it was asked if they could redact their paper to remove, like, too much information.

Leo: The how-to, yeah, yeah.

Steve: Like the real - well, actually what I first read, this was a couple weeks ago, was the codes themselves, they wanted to say, here's a code of some sort. And I don't know how that would be generally useful. I didn't dig all the way in because I figured something like this was going to happen. "They said that removing the sections which VW and Thales wanted expunged..."

Leo: I think it's Tah-leeze [ph], by the way.

Steve: Oh, Thales?

Leo: Or Tahlz [ph].

Steve: Oh, okay, thank you - "would mean their paper would have to be peer-reviewed a second time, and they would miss their slot at the conference as a consequence. And

they argued that their right to publish was covered by freedom of speech safeguards in the European Convention on Human Rights. However, the judge ruled that, pending a full trial, the details should be withheld."

Leo: This is really security through obscurity.

Steve: Yeah, it is, unfortunately. "Tom Ohta, an associate at the law firm Bristows," which was not in any way involved in the case, "said the way the researchers discovered the flaw proved their undoing." He said, "'An important factor here was that the academics had not obtained the software from a legitimate source, having downloaded it from an unauthorized website. This persuaded the court,'" he said, "'that the underlying algorithm was confidential in nature, and bearing in mind the public interest of not having security flaws potentially abused by criminal gangs, led to the injunction.'" So, eh, I mean, this is what the law helps us do in these cases, or a judge is trying to judge, is where the public interest falls. And without knowing more fully - the problem with nine months' disclosure in this case is it's not like Microsoft or Sun with Java or Adobe with Flash, where they can fix it and push out an update and hold their breathe it'll actually happen. I mean, unfortunately the Lamborghini has left the showroom, and it's got flawed crypto.

Now, what we do know, and the gangs know it now, too, the bad guys know it, is this crypto is weak in some fashion. And there are lots of other smart people out there. So I don't know at what level you can fix the algorithm. It's probably embedded in silicon, not flashable, not updatable. So now you've got all these very high-end cars...

Leo: [Laughing]

Steve: Yeah, that are protected, I mean, and this is open - this is unlock the doors and start the engines. I mean, this is full enablement of the car when you crack this. So this is not like you can tweak where the mirror is pointed. This is you can get in and drive away. Whoops.

Leo: Wow, wow, wow. Do they have a list of all the makes?

Steve: Yeah, I saw them. There are several articles about this. And, I mean, it is a Who's Who of, like, Porsche, Lamborghini, and a bunch of others. It's like...

Leo: Yeah. But Volkswagen makes the software, or...

Steve: Volkswagen is the parent company of a lot of these.

Leo: Ah.

Steve: They've sort of been purchasing them quietly.

Leo: They own Porsche, right, yeah.

Steve: Yeah, and Lamborghini, apparently.

Leo: Lamborghini. I don't know if Audis - I want to know because I'm about to buy an Audi.

Steve: I don't think Audi.

Leo: I don't think I saw Audi on the list.

Steve: No. And by the way, Audi's really - they've really got their act together, Leo. I'm very impressed with what Audi's been doing lately.

Leo: Come up and take a ride when mine comes.

Steve: I think it makes a great - you mentioned this before, and I thought, ah, that's a smart...

Leo: I may actually drive down to see you. I have to do something with the thing.

Steve: [Laughing]

Leo: I'm going to get mine pre-hacked. No, the good news is I'm getting a 2014 model. So I'm hoping that they will not use Thales, or they'll update it.

Steve: You'll have the latest update.

Leo: Oh, criminently.

Steve: Oh, goodness.

Leo: Holy moly.

Steve: Mm-hmm. That's why I'm happily driving an '01.

Leo: Yeah. With a key. With a physical key.

Steve: Physical key, yeah. So, following up on last week's ridiculous DHS email, I got many very good comments from people in the defense industry who understand this more than the common man would, only because they're subjected to the inanity of it. And it's funny, too, because I have two - the email coming in sorts into two folders, anonymous and not. And we know that it's nice to, as we're reading the Q&A, we like to say, oh, Scott Wilson from wherever he is said this. It just sort of humanizes it more. But as I was closing the folders - and as a consequence I tend to pull from those. But as I was closing them before shutting down my email client in order to clean things up for the podcast, I looked in the Anonymous folder. And that's where all of the reports about the DHS email were. That is to say, anonymously submitted to me, rather than not so. Anyway...

Leo: Makes sense.

Steve: Many of them said different things, summarized by this one. So I just pulled one from it. And he used the initials "CC," and he's in Northern Virginia, is all he wanted to say. He said, "Steve, even though the Snowden documents are publicly available, they are still classified." Okay, so some of this still seems odd, but this is the view...

Leo: This is how it works, yeah.

Steve: This is how it works. "Even though the Snowden documents are publicly available, they are still classified. I work as a contractor to a government agency (not the NSA), and we are also forbidden from even doing a search on the word 'Snowden.'"

Leo: Wow. That's ridiculous.

Steve: I know.

Leo: Can they do it at home, or only on government computers? Sounded like in that memo you couldn't even do it at home.

Steve: The machine - you're right, the machine at home would have its classification level raised if it received the document and, presumably, if the web browser displayed what was classified.

Leo: Right, right.

Steve: So going on, CC says, "Until the President or someone in authority declassifies a document, it can only be viewed on a device that is cleared for the same classification as the document itself. Viewing any Top Secret document, even one that is publicly available due to a leak, on an unclassified computer is called 'spillage.' The system receiving the spillage remains at the classification level of the document until it is sufficiently scrubbed, and it must be immediately disconnected from an unclassified network. The DHS memo may seem stupid" - may? - "but it is a standard policy that all

contractors and government agencies are required to comply with or face very stiff penalties. 'Availability' does not modify the classification of the document."

Leo: I believe I got similar emails from a number of people, one of whom said the originator of a document is the only one who could declassify it. So you probably don't want to really reveal who you are. Also we have somebody in the chatroom who says he's a government contractor, and he cannot look at them on his home computer, either. He can't make those searches either. So if you're a government contractor, you're really enjoined from doing anything, looking into this at all.

Steve: Wow.

Leo: I suppose you can't go to WikiLeaks, I mean, the whole thing keeps, in a way, keeps our government in the dark. They can't find out about this stuff.

Steve: Several people did explain, in longer email that was really too long for the podcast, actually, why it is this way, and why it's as rigid as it is, and that it cannot - you can't make exceptions. You have to have it this way.

Leo: Chain of command stuff. You've got to do it this way. I understand.

Steve: Yes, yes. If it becomes soft and porous, then the whole system, the whole system crumbles and collapses. So I do understand. Okay, now, in this - we're into miscellany. We only have one topic in miscellany. And this is one of those things where I just wish - okay.

Leo: Hey, what if you read it in a newspaper? I mean, what if you got the Guardian, and you saw it in the Guardian?

Steve: I don't think it matters.

Leo: I guess that's okay.

Steve: Because they can't get it legitimately.

Leo: Yeah, right. That's right. Yeah, yeah, yeah. Wow. All right. Sorry.

Steve: So this is another juicy Kickstarter item that makes me wish, I don't know what, there was more of me? I had multiple me's? Actually, that's one thing that is introduced in "The Void," the notion of multiple people, multiple bodies in a single brain. I guess that wouldn't work. I don't know. Well, anyway...

Leo: Multiple bodies in a single brain [laughing]. Could be problematic.

Steve: So that's very handy, it turns out. Okay. This is just, oh, my god, do I wish I had time to play with this. It is too cool. If you google "HackRF," all one word, H-a-c-k-R-F," you will find Michael Ossmann, who's been working with so-called SDRs, software-defined radios.

Leo: Almost all ham radios are currently software defined, by the way.

Steve: Oh, Leo. And in his blog he explains it. He says, "I'd like to take a moment to properly introduce the project that is consuming most of my time this year: HackRF, a software radio peripheral." So this is a gorgeous-looking little surface-mount technology circuit board with an RF connector and a USB plug. So you plug this thing into your computer.

Leo: A reminder: You need an amateur radio license to transmit on these things.

Steve: Oh, well.

Leo: That's going to - there it goes. Shot to hell. Wow.

Steve: So it says, "Software radio or Software Defined Radio (SDR)" - and get this, I love his analogy - "is the application of Digital Signal Processing (DSP) to radio waveforms. It is analogous to the software-based digital audio techniques that became popular a couple of decades ago. Just like a sound card in a computer digitizes audio waveforms, a software radio peripheral digitizes radio waveforms. It's like a very fast sound card with the speaker and microphone replaced by an antenna."

Leo: Here's a clip of him showing this on Hak5 to a...

Steve: Yes. "A single software radio platform can be used" - and this is what I love - "to implement virtually any wireless technology (Bluetooth, GSM, ZigBee, etc.)."

Leo: You'd have to have the stacks on top, though. Merely being able to do the frequency is not sufficient.

Steve: Well, and everything - this has actually been churning along, as I'm sure you know, for many years now. And all of this is open source. All of this is freely available. So this is the hardware end. And then the software end. And, I mean, I've seen pictures of this where just beautiful-looking GUI instrumentation, where you're, like, looking at the whole spectrum of everything coming in on the antenna, and then you're able to, like, zoom in on it and find specific things and then decode it. Oh, it's just great.

Leo: I have, you know, over here in my ham shack, a very expensive, something like $10,000, Icom high-frequency ham radio receiver, transmitter/receiver. And I was told by the Icom guy, it's basically all software. Nowadays you'd be crazy to do it all in ICs. Do it in software.

Steve: So as quickly as you can, you digitize the incoming signal. And then from then on you just handle it in a DSP, in digital signal processing.

Leo: That's how all modern ham stuff is done, as well.

Steve: Yeah. And this is, so anyway, this is a $200 project. He has several successful Kickstarter projects in his past. Remember that wacky Throwing Star network tap?

Leo: Yeah. That was him?

Steve: That was him, yup.

Leo: That one got funded, didn't it?

Steve: Oh, yeah, yeah. And this is well on its way to be.

Leo: So here's the Icom I was talking about, which is the - actually this is the 7600. I have a little higher level. Dual DSP for transmitter/receiver and spectrum scope. 32-bit DSPs. That's, I mean, it's all done in those DSPs; right?

Steve: Yup.

Leo: I mean, there's other stuff, obviously, filters and so forth. But it's all done in software now.

Steve: It's funny, too, because a lot of the current music synthesis is they'll give you a keyboard with knobs, but the knobs, all they are is, like, digitizers that go to the board, and everything is digital. The fact that it's a knob is just because that's a convenient user interface to people.

Leo: And they go to 11.

Steve: Yes, because they are extra. Would you like the one that the knobs go to 10, or the extra?

Leo: Extra. The funny thing is, when Ray Novak from Icom came over to install it, he put in some additional modules. You can buy modules that will give them additional extra...

Steve: Extra features, yeah.

Leo: And it's just software, just more software. We're moving from the analog to the digital world, and that's how it is, you know?

Steve: Okay, Leo.

Leo: Yes?

Steve: Do I look a little tanned to you, a little brown?

Leo: You look good. You look like you've been - where did you go, Hawaii?

Steve: I walked 17 miles yesterday with my Kindle.

Leo: Why?

Steve: Because I can't stop reading the Void Trilogy.

Leo: I love it. You mentioned last week that you picked this up, yeah.

Steve: I picked it up. And I tried to put it down and work on SpinRite, but then I just - normally when I'm reading I get to a point where it's like, okay, I'm kind of like - you kind of get tired of reading for a while. I don't - I'm not - I haven't reached any point like that. So then I gave up on SpinRite. Not forever. I'm now at 40 - as of last night, I'm a few pages past 45% of the third book.

Leo: Wow. Holy cow.

Steve: Oh, no, it's all I've been doing.

Leo: No wonder you walked 17 miles. That's a trilogy.

Steve: Yeah, and 10 on Monday.

Leo: That's a long-ass trilogy.

Steve: It is a monster. But oh, my god. I'm taking the wraps off of any reservations I had about recommending this. You absolutely have to read the first two. This is really - it's better to stay...

Leo: Is this the one - I'm trying to remember the story. Is this Ozzie going around - what is the story here?

Steve: No. So I'll get to that in a second.

Leo: Okay.

Steve: So it is better to think of this as a quintology where, I mean, really. I mean, just - and, okay, a quintology where "Pandora's Star" is the first one, and "Judas Unchained" is the second one.

Leo: Right, which we loved. I remember that, yeah.

Steve: And that's we're introduced to Nigel Sheldon and Ozzie and Paula Myo the investigator and Oscar Monroe and the Guardians and the Prime intelligence that evolves differently than organic people do. And, oh, I mean, all this fabulous, I mean, it...

Leo: Love the Prime. Love the Prime. They're the worst villains ever.

Steve: Yes. And so that's the first two books. So I was a little put off by this notion of a dreaming void. It seemed a little too, I don't know. Anyway, it's not. It is fabulous.

Leo: So I'm just looking at the Audible lengths for these. And you have read now - the first book's 22 hours. Second book, you know, from a reader who's reading probably a little slower than you because he's speaking it out loud, second's 25 hours. So that's 47 hours. And you said halfway through the next one. You've read 57 hours' worth of content here.

Steve: And I am so glad. It is so full of just, I mean, just thrilling parts. When I was - I was finishing the first one, and I was out in the park. We have a park nearby, which is why I'm getting the sun because I just want a chance, after five hours in one place, I want to go somewhere else to keep reading. And I seriously considered getting Peter to read the end of the first book to us. He would. He and I have been in touch.

Leo: Oh. Oh. You know Peter F. Hamilton?

Steve: Well, yeah.

Leo: Can you arrange an interview with him on Triangulation? Introduce us via email, would you?

Steve: Okay.

Leo: Because we, I mean, look, we've probably sold a few books for him by this point.

Steve: Oh, that's how he tracked me down. He said, "Steve, thank you for loving my books." I said, "What choice do I have? They're fantastic."

Leo: It's not just him. It's not just him.

Steve: They are - it is storytelling, Leo. It is...

Leo: He's a wonderful writer. And that's...

Steve: It is world-class storytelling.

Leo: Yeah. That's what makes this stuff so good is that...

Steve: Oh, my god. I mean...

Leo: ...he's got a great imagination, but he can write.

Steve: ...deep characterization. Also there is very amazing insight into the nature of human politics in this. I just - anyway, if anyone loved - you cannot read these without reading first the first two of the so-called Commonwealth. He creates this notion of a commonwealth which is our future. And that is established in "Pandora's Star" and "Judas Unchained," which are themselves fabulous sci-fi. But it doesn't stop. You have to continue because everybody's back. Paula's back. The Silfen Paths and the Silfen, and Bradley's back, and Oscar, and we're on our way right now to go visit Ozzie. We're not sure what's going to happen there.

Leo: Oh, I do remember this, yeah. I've read all of these. I'm just - there's so many of them that I - but it does all fit together, doesn't it. Even "Great North Road," which I'm reading now, fits into this.

Steve: And this weird void, we learn what that's about and why it's a problem and that

it's a - oh, anyway. Oh, it is - anyway. So I just - I gave up. It is consuming my life. I eat, I sleep, and I read this. Mostly now because I'm desperate to get back to SpinRite. I mean, I'm...

Leo: Oh, come on. You're not abandoning SpinRite for this.

Steve: Completely. I have no...

Leo: Dude, you've got a job to do.

Steve: I have no control over it, Leo. I can't - where I was with SpinRite requires a hundred percent of my concentration to take us to the next phase.

Leo: Oh, dear.

Steve: And I was unable to split myself. So I am reading about 18 hours a day.

Leo: At least you're doing that. You're getting through it.

Steve: Oh, no. I'll be done - here we are Wednesday. And I'm not getting much reading done. I'm talking to you right now. But all of Monday, all of Tuesday, all of Saturday and Sunday, all of the end of last week, basically it just took over. And I'll be done in two more days because I can do 20% per day. I started Book 3 on Monday and read. And now at the end of Tuesday I was at 45%. So two more days I'll be done. I just - I'm going to - I have to finish it. Then I'll be back a hundred percent on SpinRite.

So it just - I never take a vacation. I work seven days a week on SpinRite. So it's like, okay, I had a forced vacation. I just didn't have any choice. It is too good. It is, I mean, people look at me strangely because I'll, like, exclaim something. Where was I, and people - oh, I was outside yesterday afternoon and giggling. And they're like, why is that guy giggling? Because it's just - it's so good. So, unreserved recommendation.

Leo: Not just Kindle, by the way, and I should mention also Audible has a good selection of them, including this trilogy.

Steve: Yeah. Yeah, by all means. And I'm not...

Leo: That's how I listened. It's much easier for me. They're too long. I can't...

Steve: I'm not picking up the "Great North Road." It's sitting there in the Kindle. I am not going to start. I'm going to go back to SpinRite and get this next major rev done. And my treat will be picking up the "Great North Road." I tweeted yesterday when I was at - I think I was at 30%, and I just had to tweet because it was like, oh, my god, this is

so good. I mean, it's just incredibly good. And I got back some responses saying that the "Great North Road" was as good. So it's like, okay. I have something to work for. When 6.1 is released, then I'm going to - then I will pick up the "Great North Road."

Leo: I'm not sure that you'll like it as well. It's a mystery, you know. It's more of a mystery novel than anything else.

Steve: I just - he is just, oh, my god, hats off to him.

Leo: Really good writer. It's beautiful writing.

Steve: It is world-class storytelling. I just - I'm stunned.

Leo: Apparently he's doing it - I was looking at his web page, which is PeterFHamilton.co.uk, and he's doing a children's book right now.

Steve: He is. But he also has two more in the Commonwealth. We're going to get this Commonwealth continued, also.

Leo: He's smart because he's really created a very rich universe. And there's a lot of material to be mined there. You might as well just stay there.

Steve: Well, I love it, too, because each of these different authors creates a universe that they work in. And so like the Honor Harrington universe, Weber's universe had the set of technologies that they are then faithful to. And in Hamilton's, they have the so-called "TD," trans-dimensional links. And it's a little unnerving that, no matter where you are anywhere, you can have a real-time conversation. So you have to kind of get used to that. It's like, oh, okay. Because, for example, I just came from - where was I? Oh, it was the Alistair Reynolds where they had the notion of deep time, where they had never broken the light barrier. Whereas now we have both hyperdrive and ultradrive over in Hamilton's universe where they talk in terms of, like, 45 light years per hour is the rate at which they can travel. So they're super hyperluminal speeds, but also instantaneous communication. And so they're just opening up links to each other across the galaxy. It's like, whoa, okay.

But again, it's all - so that's the universe he created. And he's absolutely faithful to it. But, oh, just fabulous storytelling. That's how I would have to summarize it. Just, I'm just - and you, like, you see something building, and you go, oh, please, please, please, please, please. And then it happens just like we want it to. It's like, oh, yes.

Leo: [Laughing]

Steve: Wow. Okay, I'm...

Leo: Okay, enough, yeah.

Steve: I do have a very nice note from a Brian H. in Omaha, Nebraska, referring to SpinRite, the SpinRite we have today. He said, "Several years ago I worked for a company whose IT shop rolled out whole drive encryption to all desktops and laptops and USB devices," he says, parens, "(until one exec got his iPod scrambled)." So then they decided, oops, we're going to back off on that, apparently. He said, "A colleague of mine was having issues that caused his machine to run slow, then blue screen. I told him about SpinRite. But we were required to go through the normal IT processes for any software touching our machines. They told him that the hard drive was a total loss. I said, then why not try SpinRite? They swore it wouldn't work, due to the whole drive encryption.

"After much debate, where I told them SpinRite doesn't care, they decided to humor me and try it. After less than a day of SpinRite's processing, it was still cranking away. But I suggested noting where it was and rebooting the system anyway to see if it had fixed enough. It had, and the system rebooted normally, worked perfectly. My colleague got all of his relevant data back, and they replaced the hard drive. Moral of the story: SpinRite sounded too good to be true to everyone in IT, but we know better." So thank you, Brian.

Leo: Yay. Steve, we've got questions. You got answers?

Steve: Yay. You bet.

Leo: All right. Let me pop up the...

Steve: It's the last day of July.

Leo: Golly, how did that happen? We're almost to the fall.

Steve: What's the weather been like up there? We're having this weird, like, never really got to be summer.

Leo: It's like cloudy, muggy. Yeah. We had a very hot two weeks, or three. Really, really hot. And then we're doing what you're doing, which is it's just kind of odd. That's all right. That's all right. I'm happy because when the fall gets here, I'm going to Europe. So September - and I should tell you, I don't know if I've told you, I'll be out of the studio September 17th through October 8th, but we will have somebody wonderful hosting your shows, probably Iyaz.

Steve: Yeah, Iyaz is great. Because I know that Tom's now down here, so...

Leo: Tom may be a sub, too. We don't know. We haven't figured that out.

Steve: ...Iyaz - oh, okay.

Leo: Actually probably Lisa has, but I don't know because I just kind of...

Steve: You haven't been told yet.

Leo: I roll in here and say, what do I do next? Point me.

Steve: Where do I go?

Leo: Point me at the right microphone. Where do I stand? Question 1, Barry Ball, Woodstock, Ontario, Canada has some thoughts on Lavabit. We were talking about Lavabit, I even signed up before I heard you talking about it. Steve, I love the show, blah, blah, blah, my favorite of a dozen podcasts I listen to, blah, blah, blah, especially love the propeller hat episodes, blah, blah, blah, love SpinRite, blah, blah, blah, keep up the good work. A couple of years ago you mentioned a small news item - a couple weeks ago, a small news item stating that Edward Snowden used Lavabit. While you didn't actually say you were skeptical of the news, you sounded skeptical as you described in detail how the email is encrypted at rest, but still unencrypted server to server. And of course we know the NSA is collecting that unencrypted traffic.

Since it's encrypted on the server, and if done properly, and it sounds like they are, all the authorities could get with a warrant is a blob of pseudorandom noise, which makes it better than Gmail at least in that respect. This fits very nicely with a technique I learned about for the first time on your podcast a week or two prior, that of drug dealers sharing a Gmail account - drug dealers and/or CIA chiefs - sharing a Gmail account and having emails for each other in the draft folder. It never leaves the server. Even though the reporter is not willing to put the effort into setting up PGP, I'm sure he'd be willing to log into a mail server and look in the drafts folder. Just a thought. Have I missed anything? Does that work?

Steve: Okay. So there's a couple things going on here. And I wanted to kind of clarify because there was some confusion about Lavabit because it is - this all is confusing about, like, when it's encrypted and when it's not encrypted and so forth. So...

Leo: It fooled me. I bought a 10-year subscription. But go ahead.

Steve: Yes. So the problem is that the SMTP protocol is not by default encrypted. Later on, the ability to negotiate encryption was added. But, and I guess we do have certificates in the public key system involved there. I was wondering whether you could do a man-in-the-middle attack on that. Well, we know that you could downgrade the negotiation, and that's a problem. Because what happens is when you initially start your

- I'm not doing anything to clarify the confusion here. When you initially start your SMTP negotiation, the server answering essentially declares the things it's capable of doing, one of which is whether it's able to initiate, to upgrade the initial connection to secure. And if so, and the connecting server is also able to, then they'll say, oh, let's switch to secure.

The problem is, anybody could interfere with that initial unsecure handshake and remove the announcement that security is available at the recipient end. And then, because no security is so widespread, they would have an in-the-clear communication. So email is just - it's a fundamental problem. And it's why, with the NSA tapping upstream, for example, of Google, they get all of the Gmail. They may not get it when it comes into Google through a web interface which is now HTTPS, but they get it the moment it leaves Google. So that was the reason that I think it was Petraeus, right...

Leo: Oh, yeah.

Steve: ...and his mistress were - they didn't let their dialogue ever leave Google. They both connected securely to Gmail and used the Drafts folder, cleverly, in order to exchange mail. And apparently, again, this is one of these things where, like, the bad guys know this, and the good guys never really bothered with it. And so we're the ones having all of our traffic captured by the NSA. So the problem is, it's nice that Lavabit encrypts the mail that they receive for your pickup. But as they're receiving it, it is unencrypted. So it's true that they probably cannot decrypt it until you log in to provide the credentials required to decrypt it, and then you're able to retrieve your email that's in the mailbox. So that aspect is good.

The troubling part is that - and the only reason I really brought this up was so people didn't assume it was some sort of panacea that solved email encryption. It isn't. Because nothing coming into it will be encrypted unless it came from Google, for example, because Google does support SMTP encryption, and Lavabit does also. However, among all the major email providers, Google, Yahoo!, Microsoft, and I can't think of the fourth one, there were four...

Leo: Yahoo!?

Steve: Oh, Hot - well, no, Hotmail is Microsoft.

Leo: Yahoo!, must be Yahoo!.

Steve: Hotmail, Yahoo!, Gmail, oh, and Yahoo!, yes. Only Google does. So none of the other ones do. And again, I expect - one of the nice things that we may see come out of this whole Snowden NSA debacle is the providers actually taking efforts, making efforts to be more secure for us. Much as we heard the rumor, there was a piece of news that I think CNET carried last week that Google was exploring encrypting Google Drive. So it's like, oh, okay. And of course it will need to be vetted to see whether they've done it in a useful fashion. We know it's possible. So it may be that all of this scrutiny that is being put on the major cloud providers, because encryption is completely possible, they may actually step up and do it. Which would end up giving us more security than we had, arguably, before all this leaked. So anyway, Lavabit, nice that it stores it when the data

is at rest. But unfortunately, with email, when it's in motion, it's almost always not encrypted.

Leo: Really, PGP is the solution, and we're going to talk about that later.

Steve: We're going to be doing a series, actually, on email encryption, yes.

Leo: Yeah. Sami Flew in London, England wonders about VPN versus TOR. That's good. I'm glad he brought this up.

Steve: Yeah.

Leo: Could you clarify for me, I'm a bit muddy on this: A VPN and TOR - Virtual Private Network and The Onion Router - both seem to do the same job. They allow you to anonymously surf the Internet. [Buzzer sound] Oh, sorry. So what are the differences between them?

Steve: Right. So the way to think of them both, what they have in common, a VPN and The Onion Router, I mean, he's right that there's some similarities. In both cases you use a client on your computer to securely connect to something else. In the case of a VPN, you connect to one something else, that is, the VPN server. And it decrypts your traffic and releases it onto the Internet. And it does so with essentially no performance overhead. That is, your traffic already would have bounced around a while and then headed off onto the Internet. In this case it goes to the VPN server and then is released on the Internet.

The Onion Router is very similar in that you have, as I said, a client on your machine that encrypts, and you connect to the first node of the Onion network. But your client determines multiple hops specifically for adding obscurity to you. The problem, for example, with a VPN is that, if traffic were analyzed coming into the VPN server and out of the VPN server, it's possible to correlate the public and the private traffic through the tunnel and use that to break anonymity. And because the data's not encrypted coming into the VPN or leaving the VPN on the public side, you don't have encryption there, either.

So the VPN's use is best for when you're in a public WiFi hotspot, or you want to protect yourself from your ISP, that is, you want privacy from your local region. You're in a hotel which has unencrypted WiFi or scary wired network. We've talked in the past about how a hotel's wired network is very frightening. The idea is you want to - you just don't trust where you are. So a VPN gets you to somewhere else and then decrypts your traffic and releases it onto the Internet. That's very useful, and it's efficient.

What people complain about with TOR is that it is slow because the cost of obtaining obscurity and more anonymity by hopping all over the place is a real slowdown in the overall throughput. But that's a tradeoff that you make. So they're certainly similar, but they're different in what they provide. The TOR system actively fights anyone associating your incoming public traffic to your outgoing private traffic. A VPN server doesn't do that. Its goal is to protect, to give you privacy, like privacy from where you are so that nobody in your location can eavesdrop on you. And it does so very efficiently.

Leo: Yeah. Nicely said. Let's see here. Moving on. Question - what happened to my questions? What happened to my questions? I must have closed them. Sometimes I get ambitious. Here it is. Question 3. Leo in Mountain View - not me - has heard that the NSA contributes code to open source software: Recently I read the NSA openly and officially contributes code to open source software projects like Android and Linux. Do you know and care about the functionality and nature of those contributions? Long-time listener and fan. This is well known, by the way.

Steve: Yeah, it is. And I used to be a fan of SELinux. A little hard to be a fan of that now. SELinux is the so-called Security-Enhanced Linux. And the NSA has been very active in creating a security-hardened kernel which provides much greater inter-application isolation than out of the box standard Linux. And they've then moved that over to Android. And actually, because Android is based on Linux, they've taken that technology, that inter-application hardening, basically better sandboxing around individual applications, and made that available over on the Android platform. Now, it's important to note that the NSA is not just one organization, well, it is one organization, but not just one focus.

Leo: Many missions.

Steve: Yes, thank you, perfectly said, many missions. So there are absolutely different aspects of the NSA. For example, I have a link in the show notes that Leo could bring up. There's a page of these beautiful security configuration slides...

[nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml, nsa.gov/research/selinux]

Leo: These are great. I recommend these.

Steve: Yes. For all different operating systems, Mac and Windows and all different OSes, for things to do to harden your operating system. And it even has them for all the different versions of Windows back through time and in the future, the things you should do. These are things to turn off and what to do to lock down your system. Because this country, the United States, where the NSA is and cares about, is largely Windows systems. It's better for the country's security if individual nodes of Windows are each operating more securely. So this is in the national security for the NSA to say, here's how you tighten things down.

Leo: You bet. You bet. And I've looked at these. I'm sure you have, too. They're fine.

Steve: They're great.

Leo: And in fact, I wouldn't worry about the NSA unless you're accepting binary files from them. That is, you can't look into them.

Steve: Exactly. And so it's...

Leo: If they offer an NSA antivirus, precompiled, you might treat that with some suspicion.

Steve: Eh, yeah. Is it going to catch the things that they don't want to...

Leo: But on the other hand, open source software, and you could bet that SELinux is looked at by a lot more eyes than perhaps other open source projects. There's no way to do anything in there without showing it in the code. Now, don't accept a precompiled version. Compile it yourself.

Steve: My recommendation is to take a good, secure UNIX or Linux and then lock it down.

Leo: Yeah. Or BSD, even better.

Steve: Yes. I'm a FreeBSD user. And basically you just don't run anything you don't need. Your firewall has only the rules you require. And sort of there are lots of hardening guides around. And I would absolutely draw from the NSA's.

Leo: Yeah. Everything in there is sensible. Question 4 is Ian W., Ottawa, Ontario. Another Canadian. He got your attention apparently with the subject line: "I think the NSA has GRC's certificates!" What? Did you get your certificates from DigiCert? How did you do that? Unless I'm mistaken, they come by email, at least for smaller businesses. So NSA doesn't have to ask for them. They already have them. Am I right? Until a month ago I would have thought I must be missing something, but this all seems kind of likely now.

Steve: The good news is no. The only thing that DigiCert ever receives is our public key, which is what our servers give to anybody who wants it.

Leo: Including the NSA.

Steve: Including the NSA. Everybody who connects over port 443 to GRC.com, first thing they get is our public key. It's signed by DigiCert, which is why it's worth trusting. So the way this works is I use DigiCert's website, and I post in a secure form my public key. And it doesn't really even need to be secure, but we want it to be secure. Why not? Well, actually so no one can intercept it. I give them my public key. They sign that and email it back. And it absolutely doesn't matter if it's in the clear. My private key never leaves my servers, and never has, to my knowledge.

And then any time someone wants to connect, I give them back essentially what I received in the email, my public key signed by DigiCert, which is a reason to trust it. So the system is beautiful as far as it goes. As we've spoken of often, it does have some

problems. And many people in the wake of this NSA Snowden business are saying are we absolutely sure that the NSA doesn't have a certificate authority of their own? It's like, no, how could we be sure?

Leo: Right, could be the Hong Kong Post Office. We don't know.

Steve: Yeah.

Leo: Marcus in Calgary is wondering about making his own secure passwords: I saw somebody suggest that you use a personalized set of rules when making passwords. That way you just have to know the rules, and you can figure out what the password was. For example, say I sign up with Amazon, and I set up these rules - and of course these are just example rules: Take first seven letters from the name of website after the www. and before the next dot. If less than seven letters, then just add 1, 2, 3, and so forth. Place a 5 between each character from Step 1. Replace all vowels with FluffyKitty27. If there are no vowels, just place FluffyKitty27 at the end. And then add a bang, an exclamation mark, after every lowercase or uppercase "F." What do you think, good way to generate a secure password?

Steve: Okay. That would be a good way to generate exactly one secure password. Because the problem is, anyone who were to capture that password, if Amazon.com were to lose control of their database...

Leo: Which happens all the time. Not with Amazon, but with others.

Steve: Not with Amazon, but unfortunately it's all too common. They could scrutinize that, knowing what domain it came from, and reverse engineer your funky little algorithm. That's why I went to all the trouble of developing the Off The Grid system, which I still need to finish the - it's all done, I mean, it's all documented. We did a podcast on it and everything. I just never took the pages public because I wanted to give it one final reading and solve a couple other - and, like, beef up the FAQ a little bit further.

But the whole concept with Off The Grid was that it was a similarly non-computer - it was an experiment. Can I develop a paper-based approach where each website encodes to something completely unique so that seeing one of them tells you nothing about any of the others. And so that's - certainly using a pseudorandom sequence and a database gives you that, no association between them. My system was a cryptographic, a paper-based cryptographic association which was strong cryptographically.

But the problem, Marcus, with your approach is that, as we said, if you saw one or a couple, you could figure out what the algorithm was and then guess your password for some other website in order to break in. And that's the weakness.

Leo: Yeah. You know, you don't have to stretch too far. It's well known how to do this. Get LastPass, which you've vetted.

Steve: Yup.

Leo: And, boy, the more I use it, the more I love it.

Steve: Same way. It is my go-to solution.

Leo: Have it generate completely random long passwords.

Steve: And then it remembers them.

Leo: And let it remember them. You don't have to. I don't know my password for anything anymore except LastPass. And that's one where you could make it something that you can generate, and that's what I do.

Steve: Really screwball.

Leo: You know, I'll use this as an example because I read it once, and I certainly don't use it. But if you go through the last eight presidents, let's say, or make it 16 presidents of the United States, uppercase the Republicans, lowercase the Democrats, and then add a number for the number of years their term stretched, now, that's a good example of you're going to have a nice long password.

Steve: And we're going to give you an "A" in political science if you've even able to do that.

Leo: I could start with Nixon and do that. So if you put the number of years of the term, that gives you, I don't know what, 10, 11, it gives you a good number of characters. That's not what I use but that's an example. You're right. You'd have to have a good memory for politics. And then that's the LastPass password. Which doesn't go out in the public anyway very often; right? You only use it - I guess you would use it when you log into the LastPass website. That would be the only place you'd use it in public.

Bill in Grand Rapids had a third-party cookie question: Hello, Steve. That's how they talk in Michigan, you know. In the past few weeks, you've been talking about third-party cookies and why anybody would allow such a thing. Well, here's a reason: I do support for a company that collects certain data about users. We're contracted by another company to display that data, the stuff we've collected, back to their customers. They want their customers to stay on their website while viewing our data. Hence, their web programmers provide a frame within which we display the person's data, an iFrame. Our web programmers claim they must use third-party cookies in order to maintain that session.

Obviously, this has caused many problems with Mac users, where third-party cookies are blocked by default, and occasionally does with Chrome, IE, and Firefox users

where they have chosen to block third-party cookies. My job has been busy showing users how to allow third-party cookies from specific URLs, like ours. I heard you made a comment once that third-party cookies were not needed to maintain session. Hey, can you tell me how so I can pass this on to the programmers or the programmers at the other end?

Steve: Okay. So there's a - so Bill's company is collecting data about users. In other words, it's tracking them somehow.

Leo: Right. We don't - we can presume with their permission. It's part of the deal. Maybe they're a rating system for podcasts or something like that.

Steve: Right. So this other company has created a frame in their browser page that allows Bill's company to fill the frame with the data that they have collected. Normally what I would say, because the way the frame works, the frame is a URL provided on the web page that refers to a third-party server. And so the frame has a URL that goes and gets the content being requested. The nice way to do this would be for the URL to be customized so that, for example, the entity displaying the web page knows who this user is, the end user, looking at the web page. So they use their token for that user and add that to the URL which they send off to Bill's data-gathering company to identify the user whose information they want to populate.

Unfortunately, this doesn't work in this particular case because Bill has an identity for the end-user which is unique to his company, different as a consequence of cookies, different from what the company displaying the page shows. So in this instance I have to agree with Bill's web programmers, there is no other way to do this. You absolutely need the cookie that would be normally used in the first party as data's being collected and gathered, to then be used in the third party to display this data in a frame. And so this particular case I can't see how you could solve it without third-party cookies. It's what you would need them for. And so enabling them selectively is the only solution I could suggest. So Bill, if your job is support for telling people how to turn on third-party cookies selectively, I think you have a good, secure job.

Leo: [Laughing]

Steve: You're going to be doing that more.

Leo: You'll be explaining that to people for some time to come.

Steve: You'll be explaining that.

Leo: So there is a case for third-party cookies occasionally being...

Steve: Well, there's an instance where someone came up with a way to do it, I mean, it's...

Leo: Could they do it without an iFrame or in another way that - well, anyway.

Steve: No, I can't see how they could because the browser will send that domain's cookie...

Leo: Right.

Steve: That domain's cookie to the third party. No, it's just it's not...

Leo: If two websites want to interoperate in a way that keeps track of the session, you're just going to have to do that.

Steve: Well, no. See, that's just it. There you could definitely provide, the first-party server could provide URLs to the third-party containing unique tokens for the user.

Leo: Ah, saying hey, this guy is authenticated, and give him the information.

Steve: Yeah, and here's who he is. So that could definitely work. The trick in this instance is they're wanting to use data collected elsewhere to show in this first-party site. That's where the third-party-ness absolutely has to be present. So, yeah. In this particular case I can't see a way around that. The browser...

Leo: The right way to do this, by the way, would be for the third party to send the information, not to the client, but to the server of the first party, which would then serve it to the client. In other words, instead of having this transaction, this triangular transaction, have a transaction server to server that then delivers the information.

Steve: And the problem is, if the browser is blocking third-party cookies, it won't identify its user to that third-party server in the first place.

Leo: No, no, that transaction would have to be handled by the first-party server. So in other words, you could go as a client, as a browser, to the first-party server, say I want to see my information, instead of doing - the iFrame is frankly a cheap...

Steve: It really is a cheap solution.

Leo: ...way to do this. Better to have the first-party server query the second-party server, get the information, then display it. It's all first-party transaction at that point. They're just saving programming, server-side programming, by doing an iFrame.

Steve: Yup.

Leo: IFrame's cheap.

Steve: Yup. And not well regarded because it's a serious...

Leo: That's why. You've basically opened a window in the browser to a third-party server.

Steve: Yup. Yup.

Leo: I wonder, with new technologies like REST and so forth, there are ways to do this. Anyway, moving on, my friends. Jesse in San Francisco says that "The Newsroom" predicted PRISM in Season One.

Steve: Oh, Leo.

Leo: I remember this conversation, actually.

Steve: Oh, gosh.

Leo: He says like - go ahead. Want me to read the letter, or...

Steve: Yeah, read. I'm sorry. I just get too excited.

Leo: You want to talk about this. He says: Like you, Steve, I'm a fan of "The Newsroom." I was rewatching one of the episodes from the first season. It struck me how Sorkin essentially predicted the NSA surveillance story. His whistleblower/leaker, Solomon Hancock, was an NSA IT employee who revealed a secret program called Global Clarity which intercepts billions and billions of phone calls, emails and texts each day. This aired in August 2012. I'll play a clip from YouTube in a second [youtube.com/watch?v=r0AgBecuFdU]. He says: I know Sorkin took some heat for basing storylines on events from the recent past, making his characters seem extra smart with the benefit of hindsight. But maybe he should be given some credit because he's based his news story on events from the future. P.S.: Love the podcast.

Steve: No, and it is creepy. I want everyone to listen to this. It is just - it's spooky.

Leo: Yeah. Here we go. Let me just play a little bit of this. You can listen or, if you're on video, you can watch. This is a clip from "The Newsroom."

Steve: "The Newsroom" last year, well before all of this Snowden business.

Leo: Just so they don't get mad at us, a wonderful show that airs on HBO. Actually, I don't like it, but many do like it.

Steve: I love it.

Leo: Steve loves it.

[Clip]

SOLOMON HANCOCK: The project title is Global Clarity. It intercepts 1.7 billion phone calls, emails, and texts every day.

CHARLIE SKINNER: Legally?

SOLOMON HANCOCK: By what standard?

CHARLIE SKINNER: The law.

SOLOMON HANCOCK: No. It involves a significant amount of illegal warrantless wiretapping of American citizens.

CHARLIE SKINNER: Just to be clear, when you say "warrantless," are you saying unnecessary?

SOLOMON HANCOCK: Without a warrant. Warrantless. We could hunt for terrorists legally, but due to our bosses' devotion to Global Clarity, the NSA has been happily violating the Fourth Amendment, USSID 18, and about a dozen of the NSA's own regulations about spying on Americans. You've got guys listening in on ex-wives, dropping in on calls from soldiers overseas, checking out what movie stars are up to.

CHARLIE SKINNER: Why are you whistleblowing?

SOLOMON HANCOCK: I fought the Soviets. The way that government made their people live their lives was a very good reason to fight them. After 9/11, we started doing the exact same thing.

[End clip]

Leo: Now, I just want to say he doesn't look at all like Edward Snowden. The point, and I think a lot of people have made this point, is that this isn't something we didn't really know about. This warrantless wiretapping started under George Bush in 2001. We knew this. And Sorkin's not prescient. We just didn't know the scope of it until Snowden came along.

Steve: Yes. And it's good that this is getting fleshed out, I mean, that we have - this is going to - this allows our lawmakers and the public to say, oh, is that what we asked for?

Maybe it is. But the question has to be asked.

Leo: If you just search for "warrantless wiretaps," you'll see all the stories from 2001 about this.

Steve: Yeah.

Leo: Andy in Michigan, a man of few words - actually none. All he did was send us a link, a free and open source (FOSS) Skype replacement called Toxim, or T-o-x dot i-m. Coming soon. It's not here.

Steve: Correct. So many people have brought this to my attention. I just wanted to let people know I'm aware of it. It is not yet released. It looks very pretty. They've got some nice screenshots. Tox.im. So it's "talks" as in t-a-l-k-s. But in this case Tox.im. And presumably super secure and everything that we want. Don't know anything about it yet.

Leo: Open source, as well, so you can validate it.

Steve: So at one point, when it happens, and if it looks like it's a useful thing, and it's multiplatform and does what we want, I will certainly tear into it and evaluate its security for all of our listeners.

Leo: Who is doing this? Do they say? They don't. They don't say who they are.

Steve: That'll be important, too.

Leo: Yeah. But it is open source, so one hopes that it will be validated, the source will be validated before we use it.

Ben in Australia wondering about PGP and encrypted SMTP: Love the show. Just caught up on Episode 413, heard you mention that Gmail has SMTP encryption. Is this an "always on" feature, or is there something we need to do? And how can we tell our mail is being encrypted? I assume this is still not a 100% covered solution for keeping your mail private and that other steps should be taken as well. As such, when Leo was talking about PGP, he mentioned there might be a plugin for Gmail. Yeah, Mailvelope, it's called. Are you aware of any such plugins to enable PGP in Gmail, short of installing the desktop app and copy-pasting? I've been looking for such a thing for a long time. Thanks, and keep up the excellent work.

Steve: Okay. So we need to be a little bit clear about email and the protocols and as regards Gmail. I'm talking about SMTP, the Simple Mail Transfer Protocol, which is the way the servers forward mail to each other and the way our clients forward mail to the server. But getting mail uses the typically POP or - and I'm drawing a blank on the other one.

Leo: IMAP.

Steve: IMAP. Thank you. POP or IMAP. So that's used for connecting to the server's repository for obtaining mail. So a setting, a user-settable choice in Gmail's configuration is to require Gmail's use of SSL for your POP or your IMAP connections. And all contemporary email clients will allow an SSL connection to the server. So that gives you encryption to and from the server. Also SMTP encryption can be requested. So your client can receive encrypted email over SSL, send encrypted email over SMTP in both directions with Gmail's configuration. You have control of that.

The glitch is, when it leaves Google, it's almost never going to be encrypted, nor as it's coming in is it going to be encrypted, which is why the NSA sitting upstream makes so much sense from their standpoint. They can get it all anyway. And I'm going to be taking a very close look at Mailvelope because Leo's exactly right, that's the one. It's www.mailvelope.com.

Leo: It's a Chrome extension.

Steve: And Firefox, available for both Chrome and Firefox. It comes preconfigured for Gmail, Yahoo!, Outlook.com, and GMX. Open source, based upon the OpenPGP.js JavaScript library, and is very nice. So the idea would be essentially it creates a minimal enhancement to those email services giving you PGP encryption. And we'll know more about what that means in the next few weeks because I'm going to be spending the next few weeks plowing into, deeply, into that. Oh, and also S/MIME, S-slash-M-I-M-E, actually predates PGP. And that's been part of the RFCs for quite a while, and that's secure MIME. It's sort of built into the email standard as opposed to being a separate add-on to it. But highly recommended. Mailvelope is beautiful.

Leo: Yeah. It's a little ungainly. I mean, it's a lot easier to do this in your desktop email client. But it works. It works. And what I did is create keys with open - actually GNU Privacy Guard and then imported them into Mailvelope. So I can now in Gmail, as long as I'm using a browser with a Mailvelope plugin, I can encrypt and unencrypted, by the way, email.

Steve: Yeah, what I think we're going to be seeing is I think we'll have, because encrypted email is always going to be sort of the stepchild, there will be people with whom you are exchanging data that you want to remain confidential. And it'll make sense for you to go through the trouble of getting your keys exchanged and using PGP where you really want encryption. The upshot of all of what we've been talking about, Gmail and encryption and mail encrypted on the server versus encrypted in flight, blah blah blah, absolutely the only solution is Pre-Internet Encryption, PIE, where your data is encrypted before it leaves your computer. Then it doesn't matter whether it's encrypted in flight or in storage along the way or anything. It absolutely doesn't matter. You encrypt it before it leaves. It isn't decrypted until after it arrives. That's the way to do it, and that's why we'll be talking about it for the next few weeks, all the ins and outs of how to achieve that. Because I think there's probably an increased interest in true email encryption, and we're going to go into how it's all done.

Leo: It's easy.

Steve: Yeah.

Leo: I mean, not for - anybody who listens to this show it's easy.

Steve: Yes. Glenn Greenwald put up a fuss because Edward wanted him to do that. Finally he did, and then they were able to talk.

Leo: Yeah. Once you set it up, it's kind of straightforward.

Steve: Yeah.

Leo: And then anytime somebody...

Steve: It's just ugly.

Leo: ...contacts you - well, I'll show you. When I use Apple Mail it's not ugly. It's Mailvelope's a little ugly. It's really ugly. But when you use a desktop mail client that has PGP or OpenPGP implemented, it's pretty straightforward. You could also use S/MIME certificate-based encryption. That's maybe even easier. But it's very straightforward. It's very straightforward.

Anyway, here's Kevin Graham, our last question of the day. He's in Colorado Springs. He worries about PGP email address harvesting: I'd like to try PGP, but I'm under the impression it's not much good without a way to distribute your public PGP key. It seems to me if you publish your PGP key to any public site like pgp.mit.edu - that's the MIT key server - then you're asking for spammers and other organizations who collect information to harvest your email address. Should folks avoid the public PGP key directories and only exchange PGP public keys in person?

Steve: My intention was to use this as our segue to our detailed coverage of PGP next week, where we'll go into all this. If you have an opinion, Leo, I'd love to hear it. But...

Leo: It does. You could harvest the email addresses from that if you wanted to. So that would be certainly a solution.

Steve: Yeah.

Leo: But I put - but really the value of PGP is putting it on the key servers. In my opinion.

Steve: Or putting it somewhere where people - putting it somewhere you control, where people are able to obtain it from, like, from something you control. For example, I could put my PGP key on GRC.com, and people who went there, GRC only allows secure connections. The NSA does not have my web server certificates. And so people could get the PGP key absolutely knowing that it was the key I was intending to distribute under my own name on servers I control, and they could get it and then, as you had mentioned at the top of the show, Leo, you're beginning to have some test messages back and forth to see that it works.

Leo: Yeah. I do both. I of course publish my keys on the key servers. That's the easiest way for all of us to kind of share our keys. And it does have an additional feature. People can then sign the key. If it's not on a key server, a public key server, then you can't really sign somebody else's key. And this is the one flaw in PGP is that you can generate your own keys. So I could generate a key that says I'm Steve Gibson. And there's nothing to prevent that.

So the key is to see if this key is signed by others who have taken steps to verify it. For instance, people have key signing parties where I show you my driver's license, and I say, here's my key, would you verify this? And you say yes, I checked his license, he really is Leo Laporte, and I signed the key. So my key is signed by a lot of people because I have my key ID on my website, so you can be pretty sure that it's my key. And that's something you need to do on a public server.

On the other hand, just go to my website. You can download the key, install it in your PGP key ring, and then you'll be able to send encrypted mail to me and validate when you get email back that it is from me because only I have the private key. So it's easy if you're a public person. Steve and I can just say, go to our website, there's our key. But for the rest of us I think it's really probably a good idea to...

Steve: Or maybe Facebook page. Everybody has a Facebook page now.

Leo: Spam shouldn't be a problem anymore, to be honest. The spam filters are so good, I get very little spam. Gmail, if you use Gmail, pretty much kills spam dead.

Steve: Yeah.

Leo: There's lots of ways to do it. My email address - the problem is, now, you do a very smart thing. You change your email address regularly.

Steve: Yup.

Leo: But my email address has not changed in more than a dozen years. So I'm on every spam email list. It's not like you're going to get anything new by searching for my name.

Steve: The other thing it's possible to do, you could also bootstrap. You could use a distribution name like spammenot@gmail.com, set up PGP for that, and then over the

secure PGP email you could send someone you care about your actual PGP key.

Leo: Ah.

Steve: And so that way you have a public address used for distributing your private address PGP key.

Leo: Ah. That's clever. There's ways around that.

Steve: Yeah. We'll be talking about all kinds of neat things in the next couple weeks.

Leo: Excellent, excellent. That's going to be fun. I'm looking forward to that. And you can use me as a guinea pig.

Steve: And I will have finished the Void Trilogy, and I will be back at work on SpinRite, and I'll have a SpinRite progress report next Wednesday.

Leo: He will be sunburned next week. You doing another 17-mile walk today?

Steve: Well, not today because I did the first 10 miles was early in the morning because I had gotten myself sunburned Sunday and Monday. So I was avoiding the midday sun. And then I did the final...

Leo: You should be reading these at night.

Steve: Well, there's not enough time. I need all day, Leo. These things are huge. No, that's all I do. I wake up, and I start reading. I'm reading while I'm having breakfast. I'm reading all day long.

Leo: Wow. That's a great way to do it because you are then really in...

Steve: Oh, baby, am I in.

Leo: ...in the world, like, immersed.

Steve: Yup. Yup. I mean, I'm, like, exclaiming out loud, and people are looking at me when I'm walking. It's like, well, okay, it's a good book.

Leo: Yeah. You don't walk into trees, do you?

Steve: No. There are paths. I have paths. I have my own Silfen Paths.

Leo: Doesn't it make you wish there were Silfen Paths?

Steve: Oh, yeah.

Leo: Ah, yes. Steve Gibson, when he is not busy reading, is writing things like GRC's amazing SpinRite. You can get that at GRC.com, the world's best hard drive maintenance utility. Not free, that's his bread and butter, but he does have lots of freebies, too, at GRC.com. All sorts of information about security passwords and more.

Steve: And this podcast.

Leo: This podcast is there, and some specials on no-carb and low-carb eating, which has been really amazing for so many of our listeners. So many people come in here, almost every week, and say I lost 50 pounds.

Steve: I know. I know.

Leo: Somebody came in on Sunday and said, "I lost 50 pounds thanks to Steve." You're saving lives, dude. All of that's at GRC.com. But, yes, as Steve said, he also has 16Kb audio, the crappiest-sounding audio you ever heard [not true].

Steve: And Elaine loves it because her satellite is able to download it.

Leo: It's for the bandwidth-impaired. And then Elaine types it all in. A human being, Elaine Farris, actually writes a transcript. So that's probably the most compact way. But then you miss the nuance.

Steve: Yeah, you miss Leo's accents.

Leo: You miss my funny voices. That's at GRC.com. You can also ask him questions. We do Q&A episodes every other episode, usually. GRC.com/feedback. Do not email Steve. He does not do email. GRC.com/feedback is a form where you can fill that out. We have high-quality audio that you could listen to if you've got enough bandwidth. And even video, if you've got more bandwidth than God, you could just download beautiful, hi-def versions of this. Watch Steve's suntanned face express, emote. Every once in a while he hands come into the picture, and they get big. It's really fun. He's doing it right now. GRC.com.

TWiT.tv is our site, TWiT.tv/sn for the Security Now! show, all 415 episodes there. TWiT.tv/sn. Actually, a little hint. You could page back through all the episodes. But

if you just append the episode number, you'll get the episode you're looking for. So as an example, TWiT.tv/sn414 will give you the 414th episode. Goes all the way to - I think we have Episode 1. Somebody - I think maybe not. But we go back to, like, starting Episode 2 or 3. That works.

And what else? Oh, yeah, we are available for subscription at wherever you can subscribe to Internet broadcasts. And that's the best way to get it, so you don't miss an episode. I know a lot of schools are using this show for curricula. They're actually teaching kids about security and stuff from these shows. It's really great. We thank you for doing that, and we thank you, Steve, for doing it. And I will see you next week on Security Now!.

Steve: Okay, my friend. Thanks so much.

Leo: Happy reading.