Listener Feedback #237

Description: Leo and I catch up with a fun and interesting week of security happenings including Facebook Messenger's end-to-end encryption, Russia's President Putin, the fate of Russian-based VPN endpoints, Russian hackers compromising iOS devices, my promised follow-up on that Lenovo SMM hack which suddenly looked a lot more worrisome, the apparent illegality of password sharing, post-quantum crypto testing in Chrome, reconsidering antivirus add-ons, Pokemon Go woes, a possible defense against cryptomalware, news from the "of course someone had to try this" department, miscellany including the return of "Mr. Robot," Leo moves to FreeBSD, a recent pfSense facelift, Apollo assembly language source, even more - and, time permitting, five questions from Twitter.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-568.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-568-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here. Boy, there is a lot of security news. We have a topless Vladimir Putin. Yes, we have really a shocking flaw in the BIOS of many computers, including Lenovos and Dells. We'll talk about that. And Steve will answer - I think we get to one question, but it's still - it's a great question. And we'll talk about FreeBSD, so what could possibly go wrong? It's all ahead. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 568, recorded July 12th, 2016: Your questions, Steve's answers, #237.

It's time for Security Now!, the show where we cover the latest security information and how to protect yourself and your privacy online with this guy right here, our Explainer in Chief, Steve Gibson from the Gibson Research Corporation. Hi, Steve.

Steve Gibson: I just have to comment that our listeners are going to hear the difference, and we need to explain...

Leo: Really, is it that apparent?

Steve: It's remarkably more highs that I'm hearing. And, now, maybe we'll lose those, like in compression. Although I'm hearing a compressed result coming from Skype. So I

don't know. But, yeah, we should tell people that you're beginning to move to the new facility, and you've lost your curtains, which were clearly absorbing some of the high frequency.

Leo: So that my studio office, which we're in right now - and the only shows we do here are the radio shows, Security Now!, Windows Weekly, I think that's it. And so it doubles as my office, my office office. And we built it, when we built this studio five years ago, with windows all the way around, so it's a fishbowl, which is fine with me, except that I also like having some privacy. And because it's a studio we wanted some sound damping. So we got very thick, heavy, red velvet drapes which go all the way around, and they have been all the way around all this time. We're starting to take them - we took them down. And John then, after he took them down, said "Uh-oh." I said, "What?" He said, "You know, they really made a difference in terms of sound absorption in there."

Steve: The acoustics of that little room, yeah.

Leo: Because what you don't want in a studio is parallel reflective surfaces. Nothing's more reflective than glass.

Steve: For the sound to bounce back and forth; right.

Leo: Right. Now, fortunately this wall's got a bookshelf and hats on it, so it's not - there aren't any facing reflective surfaces. But it is much live-er, I can tell. You know what it reminds me of, there's a sound processing device that was all the rage about 30 years ago called the Aphex Aural Exciter. Linda Ronstadt...

Steve: Now, that really could go several different ways.

Leo: I know, I know. A-U-R-A-L.

Steve: Yeah, okay.

Leo: But the Aphex was used on a lot of albums. It was kind of the magic ingredient in some famous albums like some Linda Ronstadt albums and stuff. I remember it was just really popular.

Steve: Was it a compander? Was that what they called those things, or...

Leo: Well, they still make them, actually. I'm looking at it right now. They call it an "exciter."

Steve: An exciter. That's right. The aural exciter.

Leo: Which has an optical big bottom.

Steve: Oh, if it has that many knobs on it, it must be good.

Leo: It must be good. It's kind of a secret sauce. And but what I learned in those days was what it really does is some interesting phasing stuff. And you know what, I bet you anything that we are getting the effect of the Aphex Aural Exciter...

Steve: For free.

Leo: For free, by eliminating the curtains. It's exactly that sound, which is a kind of an odd, almost a chorusing of the high end. And it pops. And I think that's what we're getting.

Steve: Well, we've now explained the audio and awakened all [crosstalk].

Leo: For free.

Steve: That's right. So this is nominally a Q&A week, although, boy, is there a lot to talk about. Facebook Messenger gets end-to-end encryption. We've got to talk about Russia's President Putin; the fate of Russian-based VPN endpoints; Russian hackers compromising iOS devices; my promised follow-up on that Lenovo system management mode hack, which suddenly looked like it was going to be a lot more worrisome, and it is; the apparent illegality of password sharing, although this was kind of weirdly reported in the press; post-quantum crypto testing that started for the Google Chrome browser; reconsidering the value of antivirus add-ons. We have some Pokemon Go woes; a possible defense against cryptomalware; news from the "of course someone had to try this" department; miscellany, including the return tomorrow night, everyone, of "Mr. Robot"; Leo moving to FreeBSD.

Leo: Oh.

Steve: A recent pfSense facelift. Of course the Apollo assembly language source was the most...

Leo: Was that awesome.

Steve: ...tweeted to me thing all week. And even a little bit more. And, time permitting, we do have some questions from our fabulous listeners.

Leo: You are an optimist.

Steve: So we'll see. And I love the Picture of the Week, only because Putin figures in the top three mentions.

Leo: Oh, lord.

Steve: And I was looking at him bareback - wait, no.

Leo: There's a lot of pictures of him topless, I've got to tell you.

Steve: Bu that's like a pony, isn't it? It's not a horse. If he was riding a horse, he would be like a little pawn.

Leo: You're actually right. He looks kind of big on it, doesn't he.

Steve: It's kind of a little Shetland or something.

Leo: Yeah, it might be an Arabian. They're kind of small. That is funny.

Steve: Probably fancy, whatever it is. But I don't think - I think he's not as big as he wants to look on that horse.

Leo: If you google "topless Putin," you'll find many images of him.

Steve: No, actually, this was enough. I don't know how I found this one. But it's like, okay, I just - of course he made himself famous for taking his shirt - oh, my god, there it is, yes.

Leo: So I think it has something to do with his desire to be seen as a strong man and a hunky - and it may be something about the Russian culture. I just - I don't understand it. But there are endless images of him topless.

Steve: Weird. Weird.

Leo: Yeah, I don't quite get it. And there's the one that...

Steve: And I think Chelsea Handler did a spoof on him, too. Of course, she was topless with a whole different sort of effect.

Leo: Easy to spoof, that's for sure.

Steve: Yeah. And I guess also our ever-changing North Korean leaders always seem to sort of be a little strange this way. Like trying to create - like having a marketing arm for themselves to create an impression in the mind of their populace.

Leo: Yeah, yeah.

Steve: So anyway. I don't know. But, yeah, lots of Russian news and good stuff to talk about this week.

Leo: All right.

Steve: So, Facebook Messenger. We talked about WhatsApp not long ago, a few months ago. And of course we're always talking about WhatsApp because they're getting - they're in trouble in Brazil all the time. But Facebook has moved the Signal protocol into Messenger. So they call it "Secret Conversations." And it's not the default. It is something you can engage optionally on a per-conversation basis. Which to me I think that's exactly the right tradeoff because, as we know, the way they've implemented it, they're unable - because it is encrypted from end to end, things like their chatbot, which requires sniffing the conversation as it goes through Facebook's servers, that all gets excluded when you have end-to-end encryption.

So there will be some loss of extra fancy functionality that goes along with turning Secret Conversations on. They used the now-available open source Signal protocol libraries. There's one for Java and also one for C. And they make a point that they have an entirely different backend structure. They use a different transport protocol, a specialized on-device storage, and separate backend infrastructure. Next week I'm going to go more in-depth into two other features - one they call "abuse reporting," and the other is this implementation of secure storage - because as I began to look at it, it was like, okay, this is too big for a bullet point. And it looks interesting. Looks like there actually is maybe some new technology there that I want to talk about. And of course Messenger is a major messaging platform for the Internet, given that it's the default in Facebook.

So they have a whitepaper, 11 pages, that is available. And mostly it is sort of just a reprinting of the Signal protocol. And of course Signal, as we know, Moxie and his team absolutely did it right at Open Whisper Systems. As our listeners will remember, when I first started looking at it, I was thinking, whoa, is this thing over-engineered and over-complicated. Because, I mean, you just have stuff going in every direction at once and ratcheting protocols and key exchanges, and a lot of it seemed like overkill.

But when you look, and as we did when we covered this in detail a few months back, there's a reason for it. And you get all kinds of extra neat things. Like, for example, you have a non-real-time messaging protocol. That's where, for example, OTP falls because that has to be real-time end-to-end. With Signal they solved the problem of sending a message to somebody who isn't available at that instant in order to have a real-time interchange. So, and a lot of the extra machinery in the Signal protocol supports that, I would argue, very valuable feature. It's the kind of thing where somebody, if they turned on Secret Conversations, and it suddenly broke the way they're used to using Messenger, which is asynchronously, then that would seem like wrong to them. It's like, wait, I want to have a secret conversation, not a broken conversation.

So anyway, bravo to Facebook. And of course this ups the ante yet again on this whole

controversy we're steeped in at the moment, like this whole question of encryption on the Internet. Which takes us to Putin. Whether his shirt is on or off, and I'm sure it was on during his press conference last Thursday, he ordered, so five days ago, the Federal Security Service Bureau - the FSB, which as I understand it, that's the renamed KGB; right? So that's like the Russian security people. He ordered them to produce encryption keys, is the way it's phrased, capable of decrypting all data on the Internet. Okay. But no one's really sure exactly what that means because of course it's impossible. The FSB can't just suddenly do that.

So this was part of a new plan that the Russian government is implementing effective July 20th. So this is where they have two weeks to do this. And it's signed under law under the anti-terrorist bill. So, for example, some highlights from this are that telecom providers and - this is broadly defined, unfortunately - "organizers of information distribution," so everyone assumes that means websites because websites are organizers of information distribution, get this, must store copies of the content of all information they transmit, including phone calls and text messages, for six months, and store the metadata for three years so that they can give the Kremlin whatever it wants, whenever it wants it. Now, this is not just - they're not storing it in encrypted form. It has to be in plaintext form somehow.

And then, secondly, not only do "organizers of information distribution" have to store all transmitted information, they have to turn over, quote, "any information necessary to decrypt those messages." And so additional coding, as it says in the law, must be added to electronic messages which will function as instructions for the FSB to decode them. So reading between the lines, this sounds like someone who was a politico, who doesn't understand crypto at all, doesn't want to use the word "backdoor," but absolutely wants the equivalent, is saying that, I mean, this, quote, this "additional coding" is code for a second key or something.

Leo: It sounds so much like Feinstein-Burr, which said we're not going to tell you to do a backdoor, you just have to be able to give us the information.

Steve: Exactly.

Leo: Whatever that takes.

Steve: Exactly. Exactly. So in pronouncing Mr. Putin's decision to sign the amendments into law Thursday, his spokesman, Dmitry Peskov, told reporters that the president instructed the government to make adjustments if the measures indeed do pose any, quote, "financial risks," unquote. There again, it's like, okay, what does that mean? Dmitri said, quote, "The government will keep a close eye on how this law is implemented. And if some unpleasant consequences are discovered, the president will ask the government to take steps." Again, murk added to more murk. So again, I'm glad I'm in the United States of America; although, as you said, Leo, Feinstein-Burr tried to do the same thing.

Leo: Not so very different, yeah.

Steve: Yeah.

Leo: I think every government - but the real problem is this means, well, they're going to have to outlaw WhatsApp. They're going to have to outlaw Facebook. They're going to have, I mean, because no backdoor is possible.

Steve: Yes. And that's what, when I say this is going to be really interesting, it's the reporting now downstream of this, what's going to happen. Now, what has already happened, several of our listeners who were users of a VPN service called Privacy Internet Access sent me snapshots of a message that they received on their devices yesterday, saying: "We Are Removing Our Russian Presence." And so this letter reads: "To Our Beloved Users: The Russian government has passed a new law that mandates that every provider must log all Russian Internet traffic for up to one year. We believe that, due to the enforcement regime surrounding this new law, some of our Russian servers were recently seized by Russian authorities without notice or any type of due process. We think it's because we are the most outspoken and only verified no-log VPN provider."

Now, okay. So we can see that they're spinning this into a little bit of a PR bump for themselves. But still, they continue: "Luckily, since we do not log any traffic or session data, period, no data has been compromised. Our users are, and will always be, private and secure. Upon learning of the above, we immediately discontinued our Russian gateways and will no longer be doing business in that region. To make it clear, the privacy and security of our users is our number one priority. For preventative reasons, we are rotating all of our certificates."

And of course if Russians or some aspect of the Russian government seized their servers, then they obtained what you want to protect most in your server, which is the private key, so that only the public key is exposed. The private key is explicitly kept secret. But if Russian authorities come and raid your datacenter and take your servers, you've lost control of your keys. So they absolutely had to immediately cease all use of keys that could have been compromised.

So they said: "We're rotating all of our certificates. Furthermore, we're updating our client applications with improved security measures to mitigate circumstances like this in the future, on top of what is already in place. In addition, our manual configurations..." and then they go on in this more marketing spiel. But so the point is here is the first of, as you were saying, Leo, many probable pullouts from the Russian Federation because it may come down to essentially what Brazil has been trying to do with WhatsApp, which is either give us the content of conversations, or we're going to shut you down. And in this case, if you do encrypted communications that we cannot decrypt, you are breaking Russian law. And so the consequence is pull out because, I mean, now...

Leo: That would be the economic consequence, I would think, that they're referring to, is like, if this makes us a Third World nation, maybe we won't do it.

Steve: Exactly. And again, so I'm glad I'm not there. Oh, and Snowden's not happy. He grumbled about it's a dark day...

Leo: It's a dark day for Russia.

Steve: Exactly.

Leo: He forgot that he was living in a totalitarian state, apparently.

Steve: They're the only one that would have him.

Leo: Yeah.

Steve: So anyway, fascinating to see what's going to happen.

Leo: Oh, yeah.

Steve: And, I mean, so here we have real, like, immovable forces coming into collision, Putin saying no encryption that FSB cannot decrypt. So what happens? Do the services remain, but go decrypted? I mean, you can't do usernames and passwords, I mean, even if we rolled back 10 years to when most things were HTTP, but at least logging in was secure. Now, of course, we know that that was never actually even secure because the browser was given a cookie which, if that cookie is not marked as secure, and it can't be marked as secure, if you're then going to fall back and maintain session state over an HTTP non-encrypted connection. As we know, that allows session hijacking, a la Firesheep, trivially. So do services drop crypto and remain? Or do they think, oh, wait, we can't do that because then we're going to confuse people? Are we encrypted or not? Where do we get encrypted? Really, really fascinating to see what happens when a strong man says no, no Internet encryption that we can't get.

Leo: Russia's not such a big market that these companies couldn't walk away. Now, if China does it, hmm. That would be interesting.

Steve: Well, and this may - China may be watching, too. It's like, let's see how this goes. Like what do companies do? I think you're right, Leo, I think companies have to pull up stakes. They have to say, okay, fine. And what does that turn Russia into on the Internet? Imagine then all of the valuable services that they have now, that they've gotten accustomed to using, that will go away. I mean, here we've got one VPN provider saying, okay, see ya. And it has to be everybody else.

Leo: Right.

Steve: Yeah, so, wow.

Leo: Really interesting, yeah.

Steve: An interesting next few weeks.

Leo: Yeah.

Steve: There was also some weird things going on with iOS devices, people stating that their iOS devices were becoming locked in so-called "lost mode," and with a Russian extortion demand appearing on the screen. And those who have dug into it believe that what's going on is that this may be another downstream consequence of these recent mega breaches that we've talked about, the LinkedIn, for example, breach that caught Mark Zuckerberg when he wasn't paying attention to his Twitter account, where through password reuse, and then probably some phishing attacks in order to get people's Apple IDs, if you have the Apple ID and matching password, then you can put a device into lost mode, where it essentially locks it up, displays a message on the screen.

Now, typically, this is you left your phone at the airport, so you want to tell whomever finds it, "Hi there, this is my phone, you can't use it because I've locked it now, but here's how to find me, and I'd like to get it back," and so forth. And I've never messed with this myself. But as I understand it, it can make a sound. You can tell it you want the sound to make noises...

Leo: Right, right.

Steve: ...so that it gets seen or found, and display a message. So these people, these scammers are asking anywhere between 30 and $50. And so some people are paying. And apparently Google has been finding people typing this weird Russian extortion in and asking for translations because it's like, okay, my phone is speaking Russian, and I don't know what it says. And I guess it's a problem if it's just gibberish. And then of course other people are just doing a factory reset because as long as you have a backup, or as recent as your backup is, a factory reset and a restore from the most recent backup will recover from lost mode. But there isn't anything else that anyone can do. You can't unloose it, as I understand it. That is, if a third party has maliciously put it into lost mode, all you can do is do a full factory reset and restore.

Leo: It's kind of weird because - hmm.

Steve: Yeah. And it's not massive. It's not widespread.

Leo: Yeah. I wonder how they're doing that?

Steve: It's people, yeah, and again, they have to have both the userID and password. So that's where the presumption has come...

Leo: Yeah, so they match you somehow; right?

Steve: Right. Or phished you. It may have been...

Leo: Phished you; right.

Steve: ...like a fake message from Apple. It's like, oh, it's time for you to reassert your identity. Please enter your Apple ID and password. And a lot of people will.

Leo: I was, for a while - Henry had lost his phone, so it was very credible to me. For a while I was getting text messages saying this is Apple, and we've found your lost phone. Click this link, which of course is a phishing link, to your account and claim it. We have it, or we know where it is, but you have to log in obviously to prove that you're you. And it was very credible because the timing was right when Henry lost his phone. That was just, I think, coincidental.

Steve: Yes. Well, and remember, I think we talked about it on this podcast years ago, there was that weird scam where a friend who was traveling abroad would apparently send email saying that they got in trouble, and they need help.

Leo: Yeah, that was a Yahoo! Mail hack, yeah.

Steve: Right. And it was so believable that a lot of money got transferred.

Leo: So, so silly. Just I hope people are getting just, like, really skeptical now.

Steve: Well, and we'll be talking about this and Pokemon Go here in a minute because that's caused...

Leo: I'm not going to stop playing this game. I don't care what you say.

Steve: Okay. Just be careful about the cameras that you buy on sale from China during Amazon Prime Day because, you know, wow.

Leo: That's another thing, yeah.

Steve: Yeah. So Lenovo. This is not good. So what exists in many ThinkPads, some Yo- is that Yoda or Yoga?

Leo: Yoga.

Steve: Yoga, yeah, thought so.

Leo: I would buy a Yoda laptop.

Steve: Also some other devices. And I put a link in the show notes because there's an extensive list of, I mean, it just scrolls and scrolls, with every single model. And, for example, even my brand new Carbon fourth-generation X1, vulnerable.

Leo: Oh, no. And it's a BIOS vulnerability.

Steve: Well, it's worse, actually.

Leo: They say system management mode; right?

Steve: Right. So it's an SMM, system management mode vulnerability. So here's what it means. From a malicious app running locally, so it's only local, but the app has to have admin privilege. So if something is running on that machine and obtains or is given admin privilege, this bug allows the right protection to be removed from the firmware, safe boot mode to be bypassed, and the firmware to be altered to install a permanent malicious preboot rootkit. So, okay. So I got a kick out of Lenovo. Lenovo's disclosure is a little bit butt-covering, but okay, because they're not happy about how this came down.

They said in their support article: "Execution of code in SMM by an attacker with local administrative access." They say: "Lenovo's Product Security Incident Response Team is fully aware of the uncoordinated disclosure," is the way they put it, "by an independent researcher of a BIOS vulnerability located in the System Management Mode code that impacts certain Lenovo PC devices. Shortly after the researcher stated over social media that he would disclose a BIOS-level vulnerability in Lenovo products, Lenovo PSIRT," which is their Product Security Incident Response Team, "made several unsuccessful attempts to collaborate with the researcher in advance of his publication of this information.

So we can all read between the lines. "Since that time, Lenovo has actively undertaken its own investigation, which remains ongoing. At this point, Lenovo knows that vulnerable SMM code was provided to Lenovo by at least one of our independent BIOS vendors." So we have a new acronym, the IBV, the Independent BIOS Vendor. "Independent BIOS Vendors (IBVs) are software development firms that specialize in developing the customized BIOS firmware that is loaded into the PCs of original equipment manufacturers, including Lenovo." But not only. We'll get to that in a second.

"Following industry standard practice, IBVs start with the common code base created by chip vendors such as Intel or AMD" - and in this case Intel, it's the Series 8 reference code - "and add additional layers of code that are specifically designed to work with a particular computer. Lenovo currently works with the industry's three largest IBVs.

"The package of code with the SMM vulnerability was developed on top of a common code base provided to the IBV by Intel. Importantly, because Lenovo did not develop the vulnerable SMM code and is still in the process of determining the identity of the original author, it does not know its originally intended purpose." It's like, what? Okay. "But as part of the ongoing investigation, Lenovo is engaging all of its IBVs, as well as Intel, to identify or rule out any additional instances of the vulnerability's presence in the BIOS

provided to Lenovo by other IBVs, as well as the original purpose of the vulnerable code." So again...

Leo: How many IBVs are there? I mean, there's Phoenix.

Steve: Yeah, those are the guys. And so they talked about...

Leo: I don't think there's that many. There are three, right.

Steve: So, yeah, and remember - and Award. But there's also been some acquisitions.

Leo: Award, AMI.

Steve: Yeah. So there has been some coalescing in that industry. But it's like probably the three are the three. And there may be some small guys, for example, that specialize in BIOS code for specific, like low-volume subassembly stuff that not everyone's putting in all these.

Okay. So the guy's posting is beautiful reverse-engineering. I mean, it's - and unfortunately, as Lenovo grumbles, this was not done in the modern model of responsible disclosure. This guy wanted the glory of just putting it out there. And unfortunately, until firmware updates are available, a huge number of laptops are vulnerable to this. He's got proof of concept exploit code, instructions for compiling it, including Visual Studio project files to make the whole thing just script kiddie compatible.

So there's a little bit of chronology in his posting. On July 2nd he wrote, he added, that one of his followers confirmed that vulnerable code is present in his HP Pavilion laptop. Alex James found vulnerable code on motherboards from Gigabyte. And we've got one, two, three, four different model numbers listed, and they're Z68, Z77, Z87, and Z97 family motherboards. That was on the 5th. On the 6th, a Japanese researcher found vulnerable code in Fujitsu Lifebooks, and other Fujitsu computers probably affected. We don't know that for sure, but certainly that one particular Lifebook model. And Dell Latitude, the E6430, is also vulnerable.

So what's happened here is that, unfortunately, it looks like this - it's not clear that it came from Intel or that it was added by the IBV. But what happened is there's sort of relatively universal BIOS firmware, which either Intel or the IBVs are supplying, which across the industry contain this vulnerability, which essentially was released as a zero day. I mean, just bang, here it is, have fun.

Leo: How do you get, I mean, how do you make it happen, though? I mean, you have to have physical access?

Steve: Yes. So it's a local vulnerability.

Leo: Right, so it's not so bad.

Steve: Something malicious. Yes, correct. Something running locally on your laptop with admin privileges can then essentially install itself. So you have to have malware first. It has to be malicious. And it's able to install itself into the BIOS in a way that you would never be able to remove it.

Leo: So any virus could do this.

Steve: Yes.

Leo: As long as it can get administrative access.

Steve: Right. And of course there's lots of ways to get that these days. That doesn't seem to slow things down very much.

Leo: Well, that's pretty nasty.

Steve: So it turns out, looking at mitigations, they had a mitigation section. And I was all, oh, great, something I can tell our listeners [buzzer sound]. It's like, don't run with admin, and don't turn your laptop on. And it's like, okay, well. So the good news is the industry is scrambling to figure this out. I mean, that's the only good side of there being a high window of criticality is that it's got everybody's high-power attention to immediately patch this, rather than the stories we've heard of people waiting nine months for a response from the vendor and then finally saying, okay, fine. So just be careful, everybody. I mean, it's...

Leo: Let's be careful out there, yeah.

Steve: The good news is they know what the vulnerability is. The flipside of the full disclosure is it provides full documentation for fixing it also. So there's no excuse for this taking long. And unfortunately, what, we've got HP, we've got Fujitsu, we've got Dell, I mean, it looks like it's across the industry. So think in terms of a firmware update coming to your machine soon.

Leo: The problem is that they don't come to your machine. You have to seek them out.

Steve: Yes, yes, yes. And the other problem is, for example, if you're a Lenovo user, and you're smart, you turned off all of that horrible crapware that they add to do things like go check to see if there's new firmware because that's worse than the firmware problem.

Leo: Right.

Steve: So anyway, that's why last week I said, okay, this thing exploded, so I need to understand what it is. That's what it is. It's worth checking. And, now, I've only been talking about ThinkPads, but it's Lenovo computers. And I don't know, the HP, well, there's a laptop. Maybe it's only laptop chipsets. But don't take my word for it. These all look like Lifebooks and the 6430.

Leo: They make servers, too.

Steve: Yeah. And Lenovo does have on that page that is linked here a complete list. A lot of it is some they know are not vulnerable. And it's funny, too, because for the first several pages of this, as I was scrolling down, it was either "not vulnerable" or "we're still checking." And I'm thinking, is that what you're going to say for all of the problems, "still checking"? But I got way down...

Leo: They say "researching."

Steve: That's what it was, right, researching.

Leo: Researching.

Steve: It's like, okay. But way down, when I got into the ThinkPad section, which is down deeper, most of the ThinkPads are vulnerable. And all the ones I have are. I mean, even the old X430 and the 220, the brand new X1 Carbon. So it's like, yeah, it'll be nice to flash some firmware. Haven't had [crosstalk].

Leo: Terrible. This is really bad.

Steve: Yeah, it's not good. Yeah, well, because, I mean, it's the worst nightmare. It potentially installs a hidden rootkit backdoor-y thing.

Leo: That you'll never know. You'll never know.

Steve: You can't...

Leo: And you can't eradicate it.

Steve: Right, you can't format away, yup.

Leo: Oh, my god. That's as bad - I guess this is as bad as you can get.

Steve: Yeah. It would be a little - the only thing worse would be if it were in the thing that's now monitoring our network interface adapters all the time, and you could do it remotely. Then there'd just be, okay, Code Red, Nimda, MS Blast, game over.

Leo: Right. The mitigation is disconnect.

Steve: The mitigation is, yeah, maybe, you know, keep checking for firmware update news from your various vendors.

So the press had a field day with this. And it's like, okay, it's a little overheated. Although we did hear some sanity from our friend Judge Reinhardt with the Ninth Circuit Court of Appeals. We've talked about him in the past in a favorable light, as I recall. So this is a 2012 trial where the plaintiff was found guilty. And of course, again, in sort of clickbait mode, what we were seeing in the headlines was "Share your password, go to jail." And it's like, what?

So, okay. So here's the whole story: "A recent federal court ruling from the Ninth Circuit Court of Appeals" - which is ours out here on the West Coast - "could make sharing your passwords for subscription services" - now, this is sort of the extension, and this is what Reinhardt was concerned about. But sort of the lead-in to this says that "sharing your passwords for subscription services, covering everything from Netflix to HBO Go, a federal crime punishable by prison time, wrote a judge who opposed the decision." And I quote him in a second.

"The ruling, pertained to a trade-secrets case, found that certain instances of sharing passwords are prosecutable under the Computer Fraud and Abuse Act (CFAA), predominantly concerned with hacking. The case involved David Nosal, a headhunter who left his former company, Korn/Ferry, and later used the password [provided to him by a still-employed assistant] to access the company's database and use that information [for competitive purposes] at his new competing firm. According to Fusion, the defendant was convicted of hacking charges in 2013" - the case began in 2012 - "and sentenced to one year and a day in prison. The appeals court" - and so this is the news is that, just recently, the appeals court upheld the conviction 21. So it wasn't unanimous.

"One of the two judges upholding the lower court decision, Margaret McKeown, wrote: 'This access' - so she's the one who was for upholding the guilty verdict - says: 'This access falls squarely within the CFAA's [Computer Fraud & Abuse Act] prohibition on access "without authorization," and thus we affirm the conviction for violations under the CFAA.'

"However, in his minority dissenting opinion, Judge Stephen Reinhardt argued that the case was not about hacking, but password sharing. Consequently, he argued, the ruling jeopardizes password sharing for the general public. He wrote: '[The ruling] loses sight of the anti-hacking purpose of the CFAA and, despite our warning, threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens. The majority [that is making this decision] does not provide, nor do I see,' writes Reinhardt, 'a workable line which separates the consensual password sharing in this case from the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners. There simply is no limiting principle in the majority's world

of lawful and unlawful password sharing.'" So the concern, if Reinhardt is right, it could place users of popular streaming sites like HBO Go and Netflix who share their passwords in breach of the CFAA and open to federal prosecution.

So, now, I think it's clear that there was badness done in this case where the appellate court said, nah, this is really wrong. An assistant still employed gave someone she knew was no longer employed the password to - which may well have been changed since this guy left, I mean, it had to have been, otherwise he could have used it, in order to remotely gain entry to their privileged, confidential data and database. That seems clearly hacking.

Now, but also there seems to be plenty of guilt here to be spread around because I would argue that her employer certainly has grounds for being upset with her as well, I mean, if she still has a job there. I don't know any of that background. But anyway, so what the press has done, and you'll see this in the headlines, is oh, my god, now sharing your password...

Leo: That's quite a jump. I mean...

Steve: Yes, exactly.

Leo: "Could" is the operative; you know?

Steve: Right. But Reinhardt's position is, well, this provides post-appellate case law to affirm this concept of sharing a password is a crime under the CFAA. And as you said, there's no way to draw a line. There's no clear delineation that the law would like to somehow make between somebody sharing their Netflix password, I mean, that's against the law. The license agreement says you can't.

Leo: Yeah, but I don't think that that - judges have quite a bit of leeway. They don't have to do - just because it could be applied in that case doesn't mean they have to do that. There's a lot of stuff that is technically illegal, but that a court would say, well, come on, that's de minimis.

Steve: Well, and the whole question, too, is what will the punishment be? Because it could just be a slap on the hand, or we're going to make you watch reruns of something horrible for the rest of your life.

So an interesting piece of news. A lot of our listeners sent it to me because they thought this would be interesting to talk about on the podcast, and that is that, in some Chrome browsers, and because it's experimental, and it's not widely distributed yet, there's something called Chrome Canary.

Leo: Canary's their beta. Or actually the gamma. So there's - or alpha, I guess it would be. So what's even more cutting-edge than beta? Alpha; right?

Steve: Right.

Leo: It's the alpha. Because there's Canary Developer, and then there's - I mean, Chrome Developer and then Chrome Canary. But you can install it. I mean, it's on the - yeah.

Steve: Yeah. And users who do can dig down into some configuration dialogue somewhere and see whether this is present in their Canary build and turn it on or off. Google is experimenting with what they're calling "post-quantum crypto." And certainly a topic that never really leaves my Twitter feed is, oh, my god, quantum computers are coming. Crypto is going to all just melt down. And I actually, in the paper that is written, or maybe it was on the website, this has a website, cecpq1.com. I'm not sure what this first "C" is for. But the "EC" is elliptic curve. And then the "PQ1" is post-quantum.

So what they've done is they've merged elliptic curve, and actually they're using my favorite Bernstein 25519 curve, which was the genesis of SQRL, it's because of the properties of this amazing elliptic curve that that's what made SQRL possible and when it suddenly clicked in my brain. They're connecting that with something called "New Hope Key Agreement," which always makes me think of a Star Wars episode for some reason. So that's this thing.

Anyway, on the site they talk about, they refer to this as "quantum nervousness," which is the general sort of background nervousness over, okay, yes, classic computing architectures are growing at a rate that we've been tracking for two decades now, and we have a sense for it. And so we know that SHA-128 is kind of okay. MD5 not. SHA-256, that gives us lots of security margin. And we're ready to go bigger as we need to, sort of scaling the existing crypto technology with processing power.

But then, of course, we've got coming out of left field is the specter of a computer that works in an entirely different way, the so-called "quantum computing," which, if everything works the way they say it would in such a computer, it completely short-circuits the fundamental nature of one type of crypto. And this is worth pointing out. It's only the public key crypto that is in danger. Quantum cryptography does not endanger private key, that is, secret key, or symmetric key crypto.

So like the AES-256, the quantum computing has nothing to say about that. And again, that's also easily scalable. But no one expects that to collapse. It's the so-called one-way functions which inherently exist in the public key crypto, which is a concern. That is, we know, for example, we've talked about it through the years, it's very easy to raise an integer to an integer power in a modulus field, that is, a so-called "finite field." That's trivial. But we know of no way to, in a reasonable time, reverse that operation. That is, to get a discrete logarithm of that, the reverse of exponentiation. Similarly, we can multiply two really big primes trivially; but given that product, we have still discovered, despite lots of work, no good way to examine what we know is a product of two primes and discern what those two primes are.

So again, multiply easy, factoring hard. Exponentiation easy, discrete logarithm hard. And so it's that, it's the asymmetric crypto, these one-way functions. That's where the nervousness comes from, the idea that, if you had a sufficiently capable quantum computer that as far as we know doesn't even begin to exist with the level of complexity that it needs because quantum computers, the size of problem they can handle is a function of their complexity. And what's spooky about them is that they sort of - they change this whole concept from brute-force to checking all possible solutions at once, as unnerving as that sounds.

Anyway, so being on the leading edge, there already is a proposed spec for a key agreement protocol; that is, again, once we have the symmetric key, we're not worried about any kind of computing, quantum or not. It's the problem that a huge leap forward in computing technology might kill asymmetric crypto. And so it turns out there is a different way of operating, a different kind of one-way function involving lattices. And I've not looked into it at all. But they've named it the New Hope. It probably actually is after Star Wars.

But so what this does is this concatenates two different technologies. And a paper exists. Code exists. And it's actually running in Canary browsers. And again, no one needs it. But this is Google. This is one of the advantages Google has, having a widely distributed browser of their own. They can experiment with things, for example, as they have in the past, like the HTTP 2.0 spec, where they're experimenting with compression and header compression and tweakings of the protocols. They're able to bring it up on their servers, and then to optionally move it out into the browsers, and then instrument this and see how it performs in the real world.

One of the problems with this technology until very recently was performance because it was agonizingly slower than what we have today. And this technology, this New Hope key agreement approach says maybe about 1.6 times slower. So in a world where you actually do have quantum computing, fine, I'll take it, because we really do need the technology of public key agreement to remain standing. And so the good news is Google's playing with it. And I imagine that, by the time we need it, we'll have it.

There was an interesting article, and it was the fact that it was in Yahoo! News that sort of came to my attention because it's just - that's sort of a more pop lay news outlet, and this article in Yahoo! News was supporting the idea that antivirus software is becoming increasingly useless and may make your computer less safe. Now, it was a series of interviews of security people following from the rather catastrophic Symantec kernel flaw that we talked about last week where virtually the entire Symantec product line was found to have a bad vulnerability because it was filtering Internet traffic in the kernel. It was remotely exploitable by something that - just by sending a message. No user had to take any action because the act of this flowing through the connection could allow a system compromise.

So, and this sort of - that's an instance of what we've also, sort of the broader topic of the general attack surface problem, which is the more stuff you add - and of course Lenovo is infamous for this. The more stuff you add, the more opportunities there are for something to break because, as we know, security is hard. So anyway, that was just sort of the gist of this story. There were, among the quotes there from various security experts that the author of the story quoted, someone said, yeah, antivirus software used to be 80 to 90% effective, but now it was really about 10% effective, mostly because the nature - and Leo, I've heard you talking about this a lot on The Tech Guy show. The nature of the problem has changed. We have polymorphic viruses. The viruses are not static. They're staying ahead of the virus signature updates.

But also, and you guys were talking about this on MacBreak Weekly, I think Rene was talking about the fact that the human factor has now become the weakest link in the chain, the so-called phishing problem. Just get somebody to click on this link somewhere within Sony, and you can establish a foothold and hide yourself and then go from there. And I did hear somebody, one of our listeners saying that he'd spent some time at his father's recently and removed whatever AV they had and just installed the Microsoft package. It's like, okay, fine, Pops, this is all you need.

Leo: Yeah.

Steve: Pokemon Go.

Leo: By the way, they fixed this issue in iOS, anyway.

Steve: So, and I added "home" to the end, Pokemon Go Home.

Leo: Oh, come on. You're just a cranky person.

Steve: I am.

Leo: You never leave your house. It wouldn't be any use. Actually, you go to the Starbucks.

Steve: Well, actually, yesterday at lunch was the first time I saw this in action. And I guess it was...

Leo: I guess there were a few people doing it; right?

Steve: Oh. Well, so the place I eat is out on a nice patio with sort of a center court. And there's a Verizon cellular right next door, which is really handy because they've got really good WiFi and no password, so I'm able to use the WiFi on there. Times out after two hours, but normally I'm not there and needing to refresh. Anyway, so I'm watching this Verizon guy in his Verizon shirt with his Verizon logo, and he's holding his phone up high. And that seems to be somehow the sign of Pokemon.

Leo: Yeah, and swiping up with it, yeah.

Steve: And so it's like up in front of his face, and he's completely transfixed and walks right into a tree.

Leo: Oh, no. Oh. Oh.

Steve: And so I thought, uh-huh, yeah. And then I was talking to my server, who takes care of me every early afternoon, or late - yeah, early afternoon, or late morning. And I was telling her about what was going on. And she came out, like an hour later, and she says, "Okay, I hate this whatever this is, this Pokemon thing." She says, "Everyone in the restaurant is doing it." And in fact I saw one - there was a party of eight that they were, like, shuffling along very slowly. Every single one of them had their phone up, and they were like completely transfixed by this and like sort of - so they weren't moving at a

regular pace. And then when they got to the front door, nobody wanted to be the one who, like, arranged the table and everything because some creature might run by.

Leo: We're busy, yes, we're busy.

Steve: I don't know what was going on. Oh, my lord. But there was in the news a concern which was that - and I guess this is what you're saying they fixed. And is that the Google App Permissions?

Leo: Yes, that's right.

Steve: Got fixed? Good.

Leo: They say they did that by - it was an error, and they fixed it as soon as they found out about it.

Steve: So for our listeners who don't know, the early installs, Pokemon - was it only Android? Or Android and iOS?

Leo: Android and iOS.

Steve: Would ask for full permissions at Google. So that is this week's bit.ly link. That is to say, the Google security permissions page. So you can get to it with bit.ly/sn-568. And so the point is, we've talked about this from time to time. These sorts of things, whether it's Twitter permissions or Facebook app permissions or Google, it's nice to just sort of audit them. And really nothing brings that to mind unless something brings it to mind.

So now, just think about it. I looked at mine, and sure enough, there were a number of apps that I no longer use. Yet they're still - they still had permissions. And interestingly, only Chrome had full permissions into Google. Every other one of maybe, like, 10 had much more modest permissions. So that sort of demonstrates that the original Pokemon probably didn't need full permissions. It was just, as they said, oops, sorry, we didn't mean to be so aggressive. But again, bit.ly/sn-568. Just check in. Again, this is attack surface minimization. Remove the things you no longer need. There's no reason to have them sitting around. They just represent an opportunity for exploitation.

Leo: And while you're doing it, I mean, really what these are is the Google Connect, Facebook does it, too, and Twitter does it. And you'll see these all over the web, where it's a quick login. It says you can create an account, or you can log in with your Google account or your Facebook account or Twitter account. And all three of those networks will have a page where you can go and see where you've done that, which apps you've connected. And it's an absolute must kind of quarterly thing to go through those and delete the old apps because they still have permissions until you revoke them.

Steve: Right.

Leo: And in this case, yeah, they say it was an error. It's typical for your browser to ask for that kind of access because that way they can access Gmail without asking for additional logins, things like that.

Steve: Right.

Leo: I look at mine, and it's all either a browser or an operating system that has that kind of permissions.

Steve: Well, and if you're not trusting Google's Chrome browser to have access to Google, then just go use Firefox.

Leo: Right, right. So the Pokemon Go used that quick login. You didn't have to use it. They also allowed you to create an account at the Pokemon Trainer site. But it did give you that. And normally what you'll do is you'll get a list of the requested permissions, and you can say "allow" or "deny." In this case it didn't give you that list. It just gave the Pokemon Go full access to everything. So if you update your Pokemon Go, and I guess what you'll need to do is remove access, it'll ask you to log in again. And then it will ask for those more limited permissions. It's pretty typical for games to - for instance, here's a game that says, "I just want access to Google Play to verify your account."

Steve: Right.

Leo: That's much more typical.

Steve: Right. And much more well behaved.

Leo: Yeah. I mean, I don't think Pokemon Go is going to send email on my behalf; but it's just, you know, good...

Steve: So a listener of ours who left himself anonymous, and the subject line caught my eye, his subject was "Pokemon Go app spreads DroidJack malware." So he wrote to me: "A bunch of news sites can be found talking about the subject simply by googling. I believe I have been a victim. After realizing that I was infected, I factory reset my phone. However, it seems that DroidJack remains in place after a factory reset," he says, "with an asterisk next to the item. Why?" And he said: "This is poor judgment on my part, installing an app from a third party. I should have known better. I hope this will help anyone who listens to Security Now! in the future."

So a couple points. DroidJack is a malicious RAT. We've talked about RATs before, Remote Access Trojan. Well known, and it's been talked about, you know, Symantec and Kaspersky and others have described it. This infected version of Pokemon Go was

uploaded to a malicious file repository - that is, a file repository. I don't know if the whole thing was malicious, but it was malicious - at 09:19 UTC on July 7th. So shortly after Pokemon was released, less than 72 hours after the game was officially released in New Zealand and Australia. So probably because the game had not yet been officially released globally, many people wishing to access the game before it was released in their region resorted to downloading the APK, the app file, from third parties.

And get this, Leo. Many large media outlets provided instructions on how to download the game from third-party sites. Some even went further, providing instructions and encouragement for installing the APK download from a third party. Quoting one of them: "To install an APK directly, you'll first have to tell your Android device to accept side-loaded apps. This can usually be done by visiting Settings, clicking into the Security area, and then enabling the 'unknown sources' checkbox."

And the idea of that being said on some random news program somewhere, you know, oh, if Pokemon's not available in your area, here's how you can get it from a third-party site. It's like, no, no, no, no, no. I mean, we were just the other day talking about making sure. I said that I had had to do that briefly to grab a copy of the Zeo app, or the Zeo Companion, before it was up on Google Play. But I knew who made it and who compiled it and understood the risks, and turned that back off. And didn't you say, Leo, that there's something about it snapping back off? Or am I confusing two different things?

Leo: Yeah, it does. But that's if you go somewhere, and you download an APK, and then you try to install it. It will say, oh, you have the setting disabled. Would you like to enable it for this one time only?

Steve: Perfect.

Leo: You can go into Settings, check that box, allow third-party downloads, side loads, and basically that's the same thing as jailbreaking on an iPhone. And it carries similar risks, which is instead of downloading it from the Google Store, you're downloading from a non-Google store. And so there's some risk. Although there's lots of legitimate reasons for doing this. You've got one. So you just use extreme caution, that's all.

Steve: Yeah. And I would also argue that, for the more sophisticated user who chafes at Apple's iOS curation model...

Leo: Right, it's an option.

Steve: ...this lets, you know, it's like, hey, I want to own my phone, and I want to put any software in it that I want to. So I think this is...

Leo: It's one of the reasons I like Android is because I can do this.

Steve: Yes, yes.

Leo: But with great power comes great responsibility.

Steve: Yeah. And thus my problem is that news organizations are irresponsibly telling people, go get this now, rather than waiting for the official release. And this on the back of stories that there have been infected instances of Pokemon Go. So, yikes.

I'm going to do deeper coverage of this also next week - I've already got it in next week's show notes - because I want to understand what they've done. The first reporting that I saw provided no details. When I dug into it this morning, I found the whitepaper. And it's like, oh, now I have too many details. So researchers from the University of Florida and Villanova University claim to have found an "obvious" solution to the encrypting malware problem, which they're dubbing "CryptoDrop." They said, quoting from their paper: "Our system is more of an early warning system. It doesn't prevent the ransomware from starting. It prevents the ransomware from completing its task, so you lose only a couple of pictures or a couple of documents, rather than everything that's on your hard drive; and it relieves you of the burden of having to pay the ransom."

So that's why I need to look at this closer because it's like, eh, this sounds a little soft and a little heuristic and a little, okay, how many files does is take before it notices? Is it planting canaries through the file system that it's monitoring for change? What's it doing? And it's certainly interesting. They gave a paper, a presentation last month at a security conference, so it seems to have some cred to it. Again, it's in the show notes for next week. I will have a full report. Oh, and there is something available for Windows that grew out of this, I also saw. So again, I'll know more next week. I'll have read the whitepaper.

And yes, Leo, the BBC described it as sounding like the Daleks, of course because they're the BBC.

Leo: Ah, you're talking - I know exactly what you're talking about. We talked about it...

Steve: The Dr. Who robots, yes.

Leo: Yeah.

Steve: But it turns out actually it was researchers from UC Berkeley and Georgetown. They'd never expected this to be actually used. They were just curious whether it was possible. And that was what I was - at the top of the show, I said, "from the of course someone had to try this department." So they asked the question, could we design some audio which we could sneak by people because it would just sound like something, but not what it is, which is audio commands a la the various voice command systems that we now have in the industry, which could, for example, convey an 'Okay, Google, call 911' sort of command. And I was put in mind of the famous work on the MP3 compression, which as we know, the secret of that MP3 audio compression is, and it actually works in a similar way to JPEG, motion JPEG compression, is that you can...

[Indiscernible robot speak]

Leo: It's working. So if you didn't know what you were listening - they point out that you know what you're listening for, so you understand what it is.

Steve: Yes.

[Indiscernible robot speak]

Leo: But if you just heard that kind of coming out of something like a toy...

Steve: Yeah, you would think something was broken, or can you hear me now, and I can walk somewhere.

Leo: Right, right. But it works.

Steve: Yeah. So what these guys did - yeah, and they made it work. And so our listeners can have a sense for what it sounds like.

Leo: And it worked. What it was saying was "Open xkcd," which is harmless, obviously. And it did, it opened it. If you add background noise, even less distinctive. You're in a caf. And then the second command: "Turn on airplane mode." Turn on airplane mode. But you really, if you didn't know that that was what was going on, you probably wouldn't detect it.

Steve: You're right, you're right. And so bottom line is they wanted to see whether they could do audio that was obfuscated, essentially, to people, but which the nature of the speech recognition algorithms that are in use would hear through. And the reason this is cool, to me, is that understanding someone saying commands in a noisy caf, we humans take for granted our ability to, to an amazing degree, find the signal in the noise. But that is incredibly difficult for software technology. Again, we just - our brains are phenomenally complicated.

So, yeah, our brains can do it. So in order to make speech recognition work in a practical way, it had to first ignore noise. It had to do what we take - it had to be able to do what we take for granted, which is separate the speech from the background. And so these guys realized that, or maybe were involved in solving that problem, and they said, okay, what if we add noise to the command?

And so for the phone, that's what it's hearing all the time. It's hearing something that awful and managing to - because we take it for granted, but that's what the phone's hearing. And we take it for granted. And so when something does that, the phone, it's like, oh, yeah, I've had to be trained up, says the phone, in the ability to separate the voice from that background. These guys put background in on purpose, added noise to it. And the phone does its job, what it was designed to do. Something it had to be able to do.

Leo: Moving on.

Steve: So miscellany time. I got a bunch of stuff to cover quickly. I just wanted to make sure everyone knows that "Mr. Robot," the Golden Globe winner for Best Drama after its first season last year, returns tomorrow, July 13th. And remember that there is the "Hacking Robot" post-show, which will premiere immediately afterwards on USA Network.

Leo: Is that good? Is that worth watching?

Steve: I don't know. It's hosted by Andy Greenwald.

Leo: Oh, yeah, he's good.

Steve: Yeah. I know that the - I think they were doing the same thing with "Breaking Bad" because it had such a...

Leo: Right. Oh, a lot of shows do it. "The Walking Dead" has "The Talking Dead."

Steve: Oh, my lord.

Leo: It's just, yeah, it's kind of the - well, you know what was happening is blogs and magazines were stealing all of this. So they said, wait a minute, we've got to put this on the show, on the network right after the show. We don't want to lose these viewers who want to talk obsessively.

Steve: Well, and "Game of Thrones" has it, too; right?

Leo: Right, yup. They all do.

Steve: "After the Throne" or "Behind the Throne."

Leo: Yeah, exactly.

Steve: "Under the Throne."

Leo: And you know, they're not that, I mean, they're not great. But, you know, there you go.

Steve: So if you can't wait till tomorrow night, the first episode is floating around. It was

teased and released a few days ago. Someone shot me the news, and I tweeted out the reminder that the series was officially starting tomorrow. And I have heard good things about the first episode. But I can wait till Thursday. It'll record after I'm asleep on Wednesday night, and then I'll watch it on Thursday, time-shifting as I do. And that's fine. But I heard, like, apparently it's off to a great second season start. So the first episode apparently has, like, immediately reengaged people. So that sounds great. And I picked up the news, I think it was Saturday...

Leo: Yeah, The New Screen Savers, yeah.

Steve: The New Screen Savers pre-show. You mentioned you were moving to my non-Windows operating system, FreeBSD.

Leo: Now, do you want - now, so there's the one that's focused on security, which is OpenBSD; right? And then FreeBSD is kind of the base that Open and NetBSD and PC-BSD are based on.

Steve: So FreeBSD is faster than all of the others.

Leo: Right, right. It's the original, too, kind of.

Steve: Oh, it is. And so what happens is, and it's not surprising, with any community of developers, especially, you're going to have a community of egos.

Leo: Right.

Steve: And someone says, "Well, you know, I want to do this." And the rest say, "Uh, no, we're going to do that later." "I want to do it now." And so "I want to do something with networking." And they're like, no. Well, that creates a fork. And so then you get NetBSD, and OpenBSD, and so forth. So, yeah. So FreeBSD...

Leo: But you like FreeBSD.

Steve: It was recommended to me 15 years ago, maybe, by Brett Glass.

Leo: Well, there you go, yeah.

Steve: And I've never, never regretted it. I've been running...

Leo: What do you use it on, though? I didn't realize you were using it.

Steve: Oh, yes. I have three FreeBSD servers.

Leo: Ah.

Steve: Our DNS is running real BIND.

Leo: Oh, BIND, yeah.

Steve: BIND 9. And my good old GRC newsgroups, the NNTP server, that's INN. And so that's one server. And then I just brought up another server for GRC's forthcoming forums, you know, standard web forums, because with the release of SQRL I have to have a readily accessible, high-visibility public place for users and testers and developers to be able to collaborate. The NNTP newsgroup is valuable for what it is, but it's just not accessible enough. And so that's where I was talking to you a couple weeks ago of having brought up, not quite a LAMP stack, but a FAMP stack.

Leo: Right, right. That's right.

Steve: Because I use FreeBSD, Apache, and MariaDB, which is from the originators of MySQL, but they forked it back from Oracle because they don't trust Oracle in the long run, or Larry. And then PHP 7. And so that one's running FreeBSD 10.7, which is the current latest. And then the third one is also hosted on FreeBSD, and that's FreeNAS, is a FreeBSD-based...

Leo: Yes, FreeNAS, right.

Steve: ...network attached storage system. And of course I've got it, you can't see it on the shelf up there, there's something called NanoBSD. There's also TinyBSD and PicoBSD. NanoBSD is the host for the pfSense router/firewall that I've been talking about.

Leo: Right, right, right. I'd forgotten you were doing all that. Yeah.

Steve: Yeah.

Leo: Now, where do you get your hardware for your FreeBSD? The reason I'm thinking of it, I mean, and you know what, use Linux is fine, use Windows, OS X, that's fine. But what I want is a rock solid - what I found by using Linux is I don't need Windows or OS X. All the stuff I want to do, with the exception of Lightroom, and there are solutions around that, can be done on an open source operating system. And then I started looking at stability, reliability, and the difference between Linux and BSD, which is kind of that BSD is a base unit that's all created at the same time, as opposed to Linux, which is a kernel, and then stuff is added on top of it.

Which makes BSD more reliable, I think.

Steve: Well, and what I like is it is Unix. It is not...

Leo: It is true Unix. It's not Unix-like.

Steve: It is true - there is a UC Berkeley Regents of State of California, because they had the source at one point, I mean, there is that license in there. It is actual, evolved Unix, as opposed to what Linus did, which was to create a Unix-like OS, you know, [crosstalk].

Leo: Aiming toward POSIX compliance, as he says.

Steve: Right. Right. And so I have, in what, 15 years, it's never crashed.

Leo: Never rebooted. Never rebooted.

Steve: It's never hung. Yeah, you don't have to reboot.

Leo: [Crosstalk] 15-year uptime, yeah.

Steve: It just comes up and runs. Now, I did hear you, and I sort of smiled at this, mentioning the difference between packages and ports.

Leo: Right.

Steve: And I was a ports user. I am now gleefully a packages user.

Leo: It's so much faster, of course.

Steve: That's my point. And when you bring a system up, you will get email from it at 3:00 a.m. every morning. And so what you see in the security report is, oh, these three packages, which are installed, have security vulnerabilities.

Leo: Right.

Steve: So you want to be able to go "PKG Upgrade," Enter.

Leo: Right. This is very much like the Linux experience, where you use apt-get or pacman, and it updates, because you've downloaded binaries, precompiled, ready-to-run binaries, much like you do on OS X and Windows. Very rarely do you download source code and build the application. And that's the port system. But the port system's so beautiful. I love the port system.

Steve: Well, and as I've said to you in the past, when you see this gibberish scrolling, like, endlessly...

Leo: Makes you feel like you're doing something.

Steve: Where one character out of place, and it wouldn't work. You would think, okay, this can't possibly work. And I used to build the kernel. I rebuilt the kernel on our original server a couple times, just tweaking it here and there, just because I wanted to play with that, and that's fun. But it's like, okay, I've done that. Now I don't really need to. But so, for example, I have this older piece of hardware. It's an Intel system, multi-SCSI. It's the SCSI 320 drives. An Adaptec 2120, I think it is, or 2021 RAID controller. I mean, it's just like this random machine. Dual Xeon processors, so it's nice.

Leo: That's what I was thinking of doing, yeah.

Steve: Yeah. And...

Leo: Lots of RAM. BSD likes RAM. FreeBSD likes RAM.

Steve: Yeah. And in fact I'm still running 4GB on two of them; but for the FreeNAS, especially ZFS, it really wants more RAM.

Leo: That's what I'm really excited about is ZFS.

Steve: And so I just got 12 because this motherboard has six slots that can take 2GB per for RAM. So I just - I install FreeBSD from a CD, and it sees and recognizes everything in the system. The older one, which is like 5.something, it chokes a little bit when it's booting up on the RAID controller because it's like not happy with it. Well, they fixed that. And so 10 just cruises right through, recognizes everything. Everything came up and ran perfectly. And it's like, oh.

Leo: That was easy.

Steve: This is really nice.

Leo: I know. It's amazing, isn't it.

Steve: Yeah. And so then I have, you know, I established asymmetric keys so I'm able to SSH into it and just instantly get a command prompt with crypto keys, and it just makes administration and use a joy. So anyway, I [crosstalk].

Leo: And I agree with you, because I've been building from ports. I built Xorg, and I built Gnome 3. It took all day.

Steve: And I was thinking, Leo...

Leo: Even on a fast machine it takes all day.

Steve: It's fun to do it a few times. But then it's like, eh, no, thank you.

Leo: And there are some arguments for building from source because it's a little more customized to what you have [crosstalk] binary.

Steve: Well, actually, GRC's INN is customized.

Leo: Right.

Steve: There's all kinds of things I did. For example, for a while we were having leakage from the newsgroup out to Google or out to universities. It turns out they were reaching in and pulling news from us. And the people in the group said, you know, that seems wrong. We want to keep this here. And the other problem was people might be responding to posts that somebody had exfiltrated from our server, and no one was ever going to see their response.

Leo: Right.

Steve: So it would be frustrating for them, too. So, for example, one of the modifications I make tags the IP of the person who pulls the article in the article headers. It adds the article on the fly on the way out. So what's cool about that is that there's no information disclosure because everybody then is, if they look at their headers, they see their own IP. So, okay, that - no information was disclosed. But if an article appears out in the wild, we look at its headers, and we get the IP of the entity that pulled it originally from us.

And I think it's called X-Original-Reader is the header that I created. And so it allows us to backtrack and find out how things are escaping. And then I just go block them so that they can't have any more newsfeed. And there's a bunch of other things. Only people who post are able to delete their own posting. Nobody can delete anybody else's. So there's a whole curation system that I added to it. And this was all in C. But I was able to

do it thanks to the open source, that I was able to bring the source down, figure out how it all worked, and then add some of my own code and recompile [crosstalk].

Leo: That's why I love open source, yeah.

Steve: Yeah.

Leo: You know...

Steve: And you're right, Leo. It's where I will end up.

Leo: You will end up. But you're already there. I keep forgetting that you're running all these FreeBSD boxes. Do you buy - do you build and just put them together yourself? Or do you have a...

Steve: Yeah.

Leo: Yeah. That's my real concern. What I want to do is replace my computer at home, my iMac at home. But I want a three-monitor solution. And, you know, there's some - so I want to make sure it's all going to work. And so that's the challenge. And of course...

Steve: Yeah. The coolest thing is that people are used to having, like with Windows, where we keep chasing Microsoft's eternal quest for more power, we chase it up, to the point now where we've had water-cooled chips in order to display a Pokemon running around a screen. It's like, what has happened? So what I wanted to tell our listeners is anyone listening to this podcast has a machine in the closet that's like, I mean, an old machine. They couldn't, they didn't want to part with it.

Leo: Older is better, frankly.

Steve: That's my point is that FreeBSD allows a machine like that to have an entire next life, essentially. If you want to play with pfSense, put a couple of cheap network adapters in, or get a quad NIC. Stick it in, FreeBSD will see it, recognize it, know what it is. And then you just download the free pfSense, and you have a world-class firewall router for zero cost that you can play with.

Leo: Yeah. I'm looking forward to it.

Steve: Neat, neat. I think it's the right [crosstalk].

Leo: That's definitely the right thing. And it's, you know, for a lot of the stuff I do at home, the one thing is photography, is the only one, Lightroom and photography. And there are easy ways around that, including I still have a lot of Macs.

Steve: It's funny, I heard you mention that also before. And I was put in mind of the beginning of Windows, when I was still in DOS. DOS worked. Brief worked. WordStar worked. Everything was fine. But then there was this Micrografx Designer. It was like, ooh, gosh, look at those. Look at that. And so I would fire Windows up only to run that one program which was one of the early graphics design tools under Windows. And I would do something and then come back to DOS.

Leo: That's one of the solutions is running Wine, and just for Lightroom. And it works fine. Works fine. And for the kinds of stuff, my hobby stuff, the programming stuff I do, this is the way to go.

Steve: Oh, Leo. It's, I mean, just - you just look through the...

Leo: All the tools, the tooling is so much better, yeah.

Steve: I mean, it really is a - what's Paul's word? An enthusiast's - a computing enthusiast's platform.

Leo: For Python, for instance, you want to learn Python or use Python in your future life as a retired, reformed Windows user, there's some really interesting Python - there's, like, bpython, which lets you use a command, a REPL to type in stuff. And if you like it, save it to Pastebin so that you can kind of code in this interesting way where you're trying stuff, seeing what happens, and it's saying, yeah, keep that. And it's very interactive. It's very interesting. And all of these tools are just - they're free, widely available and, best yet, very well supported. I mean, lot of enthusiasts out there. That's why I like Linux, too. And Arch Linux has an amazing wiki.

Steve: Oh, and, I mean, I'm not an expert in Unix. So as I'm putting together this new system, I would hit a little roadblock, and I'd go, hmm.

Leo: Somewhere online.

Steve: Just google a phrase, and okay, fine, now just press that button, and off I go. Speaking of pfSense, for those who may be running it, it just received a very nice facelift. I went, I didn't otherwise know about it. And I went to the main system page, and I got a little flashing notice there saying upgrade available. And I thought, oh. And I had time. And it upgrades itself in place. So I just clicked a button, and it downloaded into its other image bank an update. It's supposed to restart itself, and it didn't. It may have been because it was a major change. Once I got that, then there was a .1 update to that one. And that one did restart and come back up.

For the major jump, it went down, and I expected it to. But then I kind of like, okay, how long should this be taking? And I waited for a while, and then I pulled the power and plugged it back in again, and then it came up. So it just had a little bit of a catch. But the new UI is way more mature. Little flatter look, like it's modern now. And they spent a lot of time on it. So I just want to let people know because you wouldn't maybe otherwise know that there was a new version. I'm on all kinds of mailing lists and things, but no one told me. So it did.

Leo: Yeah.

Steve: And I wanted to acknowledge everybody who sent me the link to the Apollo assembly language source code.

Leo: That's fun.

Steve: Fun to look through. And as you said when you were talking about it over the weekend, Leo, and you were right, well, it's for some random homegrown obscure computer. So it's not like you can run this on anything.

Leo: You can't assemble it and run it.

Steve: Although there is an emulator.

Leo: Oh, I'm sure there is, yeah, yeah.

Steve: I mean, if you, like, really want to burn your engines, then you can...

Leo: Be fun, wouldn't it?

Steve: Or stir the gas or stir the hydrogen or whatever it was.

Leo: And there's the fireworks display, which is fun. It's really fun just to look at it and just feel the history just pour through it. It's amazing, yeah.

Steve: And I'm tempted to rename Peter Hamilton's novel, which he called "The Great North Road," "The Endless North Road."

Leo: Yeah, it's kind of long, I know. I know. I know.

Steve: Oh. However, I'm at the end.

Leo: Did you finish it?

Steve: I think I'm - it feels like I'm at the - oh. I think I finished the penultimate chapter.

Leo: Right, yes, yes. There you go.

Steve: Yes. I concluded...

Leo: You can tell it's kind of wrapping up. They've solved the mystery.

Steve: Yes. And so for anyone...

Leo: By the way, not the best solution, either. I mean, it's kind of a little bit of a...

Steve: I love his work. There was lots of clever stuff. I don't think this is his best work. I really...

Leo: No, I agree.

Steve: I think "Pandora's Star" and "Judas Unchained," that pair. I like the Ozzie world and all that. But I was tweeting a little bit with someone who just finished the Rho Agenda prequel trilogy about Jack and Janet, the CIA assassin people, and he really enjoyed those. And so we were talking a little bit about - because here I was not quite where I am now. I feel a sense of relief now, it's like, okay, that's over. And his point was - and remember when I was sort of a little snarky towards Richard Phillips' work, that is, the Rho Agenda guy. And then I backed off on that. I apologized because it was wrong. It's that Richard's stuff doesn't have fluff. And Peter's adds decoration and sparkles to the fluff.

Leo: Baroque, yes.

Steve: I mean, oh, my lord. I know what color socks the various people are wearing and whether they like stripes or checks. And it's like, okay. Is this really important? But on the other hand, you end up really knowing these people rather deeply at quite some expense. So it was great. I'm glad I read it. But it was a long read. But again, some interesting new concepts. But I don't know. Seemed a little bit lighter than usual for him. And the one that we're now waiting for, due in September, the sequel to the whatever it is, "Abyss of Dreams" or "Beyond Dreams" or whatever.

Leo: Yeah, oh, the Faller Chronicle, yeah.

Steve: That's probably going to be great fun again.

Leo: Ah, yeah. I finished that one. That's awesome.

Steve: So, and I did get a nice note from a listener who asked me to please share this. His name is Dave Jones. This actually came as a DM, a rather lengthy DM. He said: "Hi, Steve. I wanted to drop you a quick message to add yet another success story to your ever-growing pile of SpinRite testimonials. I'm a software engineer living in Edinburgh, Scotland, though I'm originally from England, where my folks still live. As I suspect will be the case for many of your listeners, I provide tech support for my friends and family.

"On my latest visit to my parents, my dad asked me to look at his Windows 7 laptop that, over the previous months, had slowly ground to a crashing, unresponsive halt. Over the course of a few hours I followed your advice" - oh, this is the guy I was talking about earlier, I knew I'd heard it recently - "I followed your advice to upgrade Windows Update, install Never10, and replace third-party AV with Microsoft Windows Defender, all of this knowledge accumulated over many years listening to Security Now!, a valuable resource, not only for security, but also for staying abreast of Windows issues - not easy when you develop exclusively in OS X.

"After auditing the laptop's software, I pulled out my copy of SpinRite and set it running at Level 4" - which is the deep one - "on the laptop's hard drive." So he wanted to give it a good scrubbing. "SpinRite ran for almost exactly 24 hours; and, though the status screen reported no faulty sectors" - as we know, it often will - "I rebooted the system feeling quietly optimistic. Sure enough, SpinRite had forced the hard drive to take a long, hard look at itself, and the laptop is now running like a dream. Thank you for your brilliant suite of tools, library of podcasts, and methodical approach to problem solving. Give my regards to Leo and his wonderful podcast network. I'll visit that studio someday. Kind regards, Dave Jones."

Leo: Thank you, Dave.

Steve: And he said: "P.S.: Please feel free to share this on a future SN podcast. In fact, I'd love it if you did."

Leo: Well, there you go. You got your wish. Now, let me go and see what questions I have for you, Steve. You said these mostly came from - yeah, I see them, I see them - mostly came from Twitter. We start off with Hans Dekker, who asks: If I keep an Internet-exposed web server, for instance, or a Minecraft server - that's what I'm doing - on a WiFi guest network with limited access, am I safe? Hans Dekker.

Steve: So I'm a little confused, I guess, by "WiFi guest network." So the server maybe has a wireless access point, and then it links to a wireless router? I guess I'm more used to seeing a machine like that, an Internet-exposed web server, would be plugged into a router. So I wasn't exactly sure what Hans meant.

Leo: I think that's what he means. He says what he wants to do - I understand what

he wants to do because my server, which is running on a Mac Pro, my Minecraft server, SSH server, wiki web server is plugged in. But it has WiFi. And what he wants to do is isolate it; right?

Steve: Right. And so...

Leo: Because you have to DMZ it, or you have to port-forward. Somehow you have to indicate that traffic coming in on 35565 is going to go to that server. Well, what if you put it on a guest WiFi? Would that protect the rest of the network from it?

Steve: The problem is there are too many unknowns in order to suggest that that would actually provide protection. What I was put in mind of was what I did when I brought up this forthcoming forum server because, as we know, we've covered it for years, traditionally forum software...

Leo: Oh, it's so buggy.

Steve: ...especially with a SQL backend, is like one of the worst places from a security standpoint. So there was no way I would even consider bringing up a system where anonymous people could post their own content into a server unless I could absolutely isolate it from the rest of GRC.

Leo: That's what he's asking.

Steve: Yes. And so this brings up two things. What I did was - oh, and what I needed was to know that, no matter what could possibly happen on that server, no matter what could crawl inside it from the outside through an unknown problem in the forum software or, for example, if it was a Minecraft server, some...

Leo: Bug in the server, yeah.

Steve: ...buffer overflow that might exist there, no matter what could happen, no meltdown or compromise of that machine could in any way affect the rest of GRC's network. Again, I'd just rather not have it than to have something that is a source of that kind of vulnerability. So I used to have, essentially the hub that links all these different machines together was a very nice gigabit switch. It is now a managed switch. And that's not something we've ever spoken about before. A managed switch is very much like a multiport appliance that you plug things into. And if you don't explicitly configure it, it acts just like an unmanaged switch. That is to say, the hub/switches that we're used to talking about, they are implicitly unmanaged, meaning there's nothing to manage. There's nothing to do.

But managed switches give you a console interface or, more recently, a web interface. And what I chose was a product from Cisco. I liked that it had my initials. It was the SG300-10, which is a cute little 10-port - thus the -10 - 10-port managed switch.

Basically it is sort of the OS side of Cisco's IOS, the Internet Operating System, and you're able to define access control lists, ACLs. So essentially, it is an inexpensive hardware firewall. And again, when I say "hardware," we talked about this question last week. What's the difference between a hardware and a software firewall? It's like, well, yes, it's running an operating system. There's software in there. But by hardware I mean that's all it is.

So now, rather than having all of the servers at GRC converge on this switch, where they're able to share traffic among themselves, on a port-by-port basis I'm able to impose rules on which packet traffic is allowed to ingress and egress from each port individually. So, for example, the port that this forum's server is already running on, it is able to send email, because I have to be able to do that from the forum software. It can access GRC's SMTP server, which is on a different piece of machine, and that's it. It is blacked out from the rest of the network. I make it go get DNS from outside. It talks to the rest of FreeBSD land from outside. So it is in my network, but it is absolutely bolted down so that, no matter what happens in there, it can't get up to any other kind of mischief.

So one option is to add to an existing network a managed switch. And you'll want to make sure if this is the kind of thing you want to do because there are sort of - there are grades of management. You probably want what's known as a Layer 3, as opposed to a Layer 2, managed switch because Layer 2 can do things like quality of service and traffic prioritization, but not packet filtering. You want to make sure that the one you get can do access control lists, packet filtering. Dell makes them. Amazon has a bunch of them. And they're not super cheap. They're a few hundred dollars.

But the alternative, and this is the second part of this, is, for example, this little pfSense box I have, it's got four network interface adapters, so any little machine with multiple NICs. The concept here is that you want port isolation so that the computer is plugged into a physical port, and there are then firewall rules. And we call them firewall just because it's looking at the packet and deciding what to permit or to drop. There are rules that say only this traffic is able to come in or out.

And so, for example, in the case of this forum server, it has full access to the Internet for all the things it wants to do, only to GRC's SMTP server that feels unlikely that it's able to get up to any kind of mischief. If I weren't so careful, then I might put firewall rules in that machine. But of course we can't trust firewall rules in that machine because it's the machine that might be compromised. So the solution has to be outboard. And we never really talked much about actually bringing up packet filtering to our audience. But I have a feeling we're going to be heading in that direction in the future because this Internet of Things, and doing more sophisticated things like running a publicly facing server in your home, where you want to make sure that there isn't a crossover between any mischief it gets up to and the rest of your home network. The way to do that is isolating the traffic.

And I know people will talk about VLANs, and that's sort of a mistake. Virtual LAN technology is an organizational tool, not a security tool. It can be used for security, but you have to be very careful that the switches that you use honor the VLAN tagging and that that's all done really right. I regard it as a fragile solution. So I think physical port isolation is the way to go. And so it's either a multiport router where you have control over individual traffic coming in and out of the switch on an interface by interface basis - and, for example, pfSense gives you all that. It's a full firewall also.

Or another solution is - and I expect we're going to see some downward pressure on pricing because I would like them to be cheaper for our listeners - is a managed switch that can do Layer 3 management. They are just so fun to play with. Oh, and you can do

other cool things like port mirroring. You're able to, for example, tell a managed switch that you want all of the traffic on the following ports to also be forwarded out of that port. And of course that's where you put your monitor in order to, like, watch what's going on on your network. So it's able to see all of the traffic coming and going.

Leo: I don't know if it's horribly expensive. Here's one from HP that's 160 bucks.

Steve: Wow, that looks nice. How many ports does that have? That has, like...

Leo: Twenty-four ports. I mean, you don't need that many.

Steve: You won't run out.

Leo: You won't run out. So effectively you could think of this...

Steve: Yeah, you're right, that's a good price.

Leo: Yeah, I should just buy this and put my server - now, the way I've done it is it turns out I have two Comcast networks, so I use one for the server and just my office stuff, and then the house, the whole house network is on the Comcast business class and is separate. No, it's vice versa, exactly. I'm on the Comcast business class because that way I have a static IP address.

Steve: Well, Leo, as I expected, we have filled our time.

Leo: Oh, that's right. And we haven't filled our question quota.

Steve: No. But let's punt those to next week. We already have some topics to discuss, following up in more depth on some of the stuff from this week. And so, to be continued.

Leo: Good. HP has an 8-port Level 3 switch for only $83. That's probably enough for me.

Steve: Wow. I've got to - okay. Where is that?

Leo: It's on Amazon right now. It's a prime, baby, prime. You buy one, and I'll buy one.

Steve: HP 8-port managed...

Leo: Yeah, 8-port, and it's Level 3, L3; right? That's what you need.

Steve: Yeah, Layer 3. $83.77.

Leo: Yeah. And eight ports is enough. I'm not running more than eight servers. So what you would do is you could still put this on your network and use it as a buffer, as an isolator. Is that the idea?

Steve: Okay, now, I'm not seeing - this is, well, it says Layer 3. So it says single IP management. So that's for managing. Traffic prioritization, rate limiting, broadcast control, secure web GUI, session logging, flash images, port mirroring. It has all that, but I'm not seeing packet filtering. So that's the one thing...

Leo: Oh, okay.

Steve: That's the thing we absolutely want to make sure we're getting. And the way I was solving this question was just going and finding - go to HP, pull down the PDF docs, and see if it's got packet filtering as an option in there.

Leo: Because essentially that's what you're using to isolate it.

Steve: Correct, correct. And, I mean, our listeners will have so much fun with this because you're creating rules that say "traffic bound for this range of IPs on this protocol at this port allow," and then otherwise, if it's - and so it's sort of like a stepwise, very much like a little computer program where each rule is examined for allow or deny until it matches the characteristics of the packet. And then normally by default there's a "deny any any," meaning if it didn't match, if there wasn't an explicit "allow any any" at the last rule, then when it falls off the end it drops the packet. So this gives you absolute control over managing who's able to do what on your system. And if we can find one that's inexpensive and we know does packet filtering, then that would be a win because it would give our listeners something, really, it's just so fun to play with.

Leo: Well, those rules sound familiar. They sound like firewall rules. So it sounds like it's very similar to that kind of.

Steve: Yeah, yeah. That's exactly what it is, yeah. I guess I would call - when you say, okay, what is a firewall, well, it's something that restricts some traffic. And so that's what this is. Technically it's called an "access control list," meaning an ACL. It is a list that specifies the families or classes or types of traffic that is allowed in and out of a port, on a port-by-port basis.

Leo: I would bet this doesn't do that packet filtering.

Steve: I think it probably doesn't.

Leo: And that you'd have to get the enterprise version to do that, would be my guess.

Steve: Oh, but here's the one that does. In the little chart down below, the SG300-10, the one I got.

Leo: Oh.

Steve: That's $175. So, okay.

Leo: That's not terribly expensive.

Steve: It's not. It's less expensive than I remembered. So, yeah, that one, it's running a version of IOS, the famous Cisco Internet Operating System that the routers run. Very nice web interfaces, 10 ports. And again, it's not 24, but come on, 10. And so, I mean, most of your stuff is all going to be on one switch, feeding into that, for management in the aggregate. But that's the one I bought, this little SG300-10. It comes with little wings, so you can 19-inch rackmount it. It's sitting at Level 3 in the datacenter, rackmounted, right now. That's the one I'm using.

Leo: I'm going to cancel that other one, and I'm going to get the SG.

Steve: The SG, the Steve Gibson 300.

Leo: Steve Gibson-approved model. Nice. Folks, that concludes this edition of Security Now!. We're getting ready for TNT, so we'd better wrap it up here. I see Jason Howell has arrived. Don't forget you can get this show on Steve's website, along with SpinRite, the world's best hard drive maintenance and recovery utility, and all the great free stuff he does. GRC.com. We have also the show in audio and video at our website, TWiT.tv/sn. And the best way to do it is subscribe.

Somebody asked me in Twitter, well, I've missed a few episodes, and your feed only has 10. What do I do? Well, feeds, that's the nature of feeds. Ten is, like, generous. It's the most recent shows. But you go to the website, TWiT.tv/sn. Every show ever is there. And then I also pointed him to my blog, LeoLaporte.com, where we have user-submitted scripts for downloading any range.

Steve: And doesn't subscribing prevent you from missing them? You don't have to go get them one by one.

Leo: Right. You subscribe.

Steve: You just subscribe, and then they're there.

Leo: And that way you'll get everything going forward. You'll always have it. Exactly.

Steve: Right.

Leo: Unless you have some rule. Sometimes some of the podcatchers have rules like, if I don't listen to it in a month, delete it and stuff like that. Cool. We'll be back here every Tuesday, 1:30 p.m. Pacific, 4:30 p.m. Eastern, 20:30 UTC. So stop by, say hi. Join us in the chatroom. And we'll see you next time on Security Now!.

Steve: And we already have a great show lined up for next week.

Leo: We're planned. We're all ready. We're ready to go.

Steve: Just pause your life for however many hours that is.

Leo: We'll be back soon. Take care.

Steve: Bye.