Listener Feedback #166

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

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-401.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-401-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here. But there's another Java exploit? How could this be? How could this be? We'll also talk about his favorite new sci-fi for the year - so far - and a little Bitcoin conversation. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 401, recorded April 24, 2013: Your questions, Steve's answers, #166.

It's time for Security Now! the show that protects you - that's how the song goes, isn't it? [Singing] Security Now!, the show that...

Steve Gibson: It's always sort of a long fadeout, and sort of a chorus-y sort of effect, too.

Leo: You know, it's funny - Steve Gibson's here, the Explainer in Chief, the host of our show, man at GRC.com.

Steve: I just happen to be present for this one.

Leo: It's amazing. I turn on the mic, and there he is. Every Wednesday just you're there. But we've been using that same theme song now for 401 episodes.

Steve: Why change it? It's just fantastic.

Leo: Yeah. I mean, it's identified with the show. I mean, I suppose we could update it. It is six, seven years old now.

Steve: No.

Leo: But why change it? Why change it? Steve, today's a Q&A episode, yes?

Steve: It is. We've got a typical weekly roundup of interesting events that have occurred, a little bit of follow-up from our listeners about their experiences with proXPN, and somebody's 85-year-old mother had her laptop saved by you know what. And then a bunch of questions. So a great podcast.

Leo: I set up my 80-year-old mother this morning. You know she's visiting this month.

Steve: It's funny, I was thinking about your 85-year-old mother when this guy was talking about what a super techie his was. And I thought, oh, just like Leo.

Leo: Yeah. Mom's really quite good at this. I set her up with Skype on her new Galaxy Note II and her iPad, and we're going to put it on her laptop. And I have it on my phone. And she said, wait a minute, you mean we - she says, why do people have telephones? I said, that's a good question, Mom. You notice I don't have a phone. Oh.

Steve: And you know, it's true. Landlines really are disappearing. Those days are...

Leo: The only reason I said she should probably have a landline is for 911. Especially as an elder. You know, you want to make sure that, if you can't talk, you can pick up 911 and go [distressed groan], and they know where you are.

Steve: Well, I still have a fax machine. And I've got...

Leo: Oh, that's true. If you have a heart attack, you're going to fax them.

[Laughter, Steve and Leo making machine noises]

Leo: Wait a minute, a fax is coming in. It looks like there's an emergency. Well, there was an emergency.

Steve: It's funny because I've kept my line because I really want the higher quality. But when you're talking to somebody on the other end who's always on a cell phone, well,

there's the problem.

Leo: Cell phones sound terrible. But Steve, notice how high the quality is on Skype. I mean, it's better than phone.

Steve: Oh. It is. It's...

Leo: And you know, all of the carriers are now introducing - some of them call it HD Voice. They're going to be using LTE to do higher bitrate voice on cell phones.

Steve: Ahh, yes.

Leo: I think T-Mobile's the first to launch this, to roll this out.

Steve: And you know that's all being funded by what they charge for text messages, which is the most ridiculous profit, I mean, zero bandwidth required for a text message.

Leo: If you pay 20 cents a text message, which is the going rate...

Steve: Oh, you went over your - you went over your limit this month. Oh, my god.

Leo: It's $1,500 a megabyte. A megabyte. But most people now have unlimited text. And that's what's happening is with Apple Messages and Facebook Messenger, people are using their data now for messaging. And I think that business is almost gone, I really do, for the phone companies. So, question and answer. We've got news to talk about.

Steve: Yup. I put Java at the top again, but go ahead.

Leo: Oh, come on. Really?

Steve: Oh, I know. Yeah, Adam Gowdiak's at it again.

Leo: My mom said, "Somebody sent me some Flash in my - something called a Flash, says I need a Flash video in my email, and I want to watch it." And I said, "Mom, there's a reason Apple does not put Flash on that computer. I would probably forego it if you can possibly live without that video, which is probably spyware anyway." Steve Gibson's our hero, the king of security and privacy. Let's get some Java news? Oh, no.

Steve: Yeah.

Leo: Oh, no.

Steve: Okay. So we have good news, which is the first use of the non-autorun features in the latest version of Java, which it's good that they put in because we've already found a need for them, unfortunately. It's been a week. And our intrepid security pioneer, Adam Gowdiak, whom we've spoken of many times, is the CEO and founder in Poland of Security Explorations. And that's certainly what he does. He made a post on Monday to the Full Disclosure mailing list, which is where he puts his stuff, saying, "It can be used to achieve a complete Java security sandbox bypass on a target system."

Leo: Oh, criminently.

Steve: "Successful exploitation in a web browser scenario requires proper user interaction. A user needs to accept the risk of executing a potentially malicious Java application when a security warning window is displayed." So it's good news. I mean, first of all, yes, there are more problems with Java. No one expected that there weren't going to be. Even Oracle said two weeks ago, or one week ago, that there were still unpatched problems, but as far as they knew they were not being exploited. So Adam found yet another new problem, sent proof-of-concept code to Oracle in order for them to be able to duplicate it and ultimately fix it. So it's a problem that there's this bypass.

I wanted to take this moment, though, to talk about sandboxing because remember that the fundamental problem with sandboxing is that we are - we're trying to constrain something powerful inside an artificial barrier. So the challenge is not to let this too powerful thing outside. So we're seeing now the problems with Java are ways to penetrate the sandbox. Which we might be tempted to say, well, okay, so what's the point of having it? Except one of the things that has happened that is something you don't notice until it's been a while is all PDF exploits instantly ended when Adobe added the sandbox to the PDF format.

So there's an example of a very, I mean, a truly successful change which I want to acknowledge because it's important for security theory, and also we've beaten up on Adobe so much over the years. This made a difference. We were talking about PDF exploit after PDF exploit. I mean, it was what Java has become a year ago, and it was the instant that they announced their sandboxing technology, PDF exploits just vanished. We haven't spoken of one for quite a while. And it was that event. So tip of the hat to Adobe for doing it. It certainly took them a long time, and they resisted, probably just natural hubris, believing that, oh, well, we'll just get these last few bugs fixed, and then we'll be okay.

Leo: Of course.

Steve: Uh-huh, yeah. But yay for the sandbox in Reader and Acrobat because it has made all the difference. And I would just say that Java is dramatically more complex, dramatically bigger. I mean, it is a full-strength, full-function language. And the idea of hosting that on a browser is insane. And although I don't have it in my notes here, I have picked up on some little blurbs that, for example, the Scandinavian countries that have been strong users of Java, for example, we had a lot of feedback from listeners who say, well, my bank requires me to use Java. The banks are dropping it. They are saying, okay.

Leo: Good, good, good, good.

Steve: Browsers are becoming Java hostile. The security community is Java hostile. We need to re-implement this in some other platform.

Leo: It strikes me that Java feels old-fashioned when you see it in a bank. I mean, it just feels like an old-fashioned thing.

Steve: Well, it's got a great place for multiplatform desktop applications.

Leo: Minecraft. It's great, yeah.

Steve: Yes. There it makes sense. But not on a web browser. That's just the wrong place. And this really annoyed me. I picked up the news from the Commissioner of Data Protection and Freedom of Information in Hamburg, Germany, did you see this little blurb about Germany slapping Google?

Leo: Oh, I did, yeah. They slap them all the time.

Steve: Well, this was, of course, and the reason I'm bringing this up is we've covered it so extensively. This was the inadvertent collection of unencrypted WiFi data by Google's Street View cars as they roamed around Germany, well, all of Europe and the U.S., I mean, everywhere. And we know, we absolutely know that this was inadvertent. The forensic studies were done. We talked to the guy who, well, I mean, people talked to the guy who grabbed the code out of the open source community, dropped it in because it did more than what he needed, but also what he needed, and it happened to also be logging all of the WiFi packets. And some of them happened to be encrypted when people were broadcasting, I mean, they were broadcasting their data in the clear.

Leo: Right, right.

Steve: So it's like, okay, well, we know that Google - this wasn't some scheme. This was just inadvertent. So the good news is German law prohibited a fine of more than 145,000 euros, which is currently $189,000 U.S. And what annoyed me was that this Johannes Caspar said that the fine was far too small to act as a deterrent.

Leo: Oh, yeah. It's cigarette money for Larry Page. It's nothing.

Steve: Well, yeah, it's 0.002 percent of Google's...

Leo: They make that in an hour.

Steve: Google's $10.7 billion net profit for 2012.

Leo: Maybe 10 minutes, even. I don't know.

Steve: But the notion that a fine would be a deterrent suggests that Google wanted to do this, and now, ooh, it was too expensive for us to do that. What?

Leo: No. It's ridiculous. Europe doesn't - the Europeans, in particular the Germans, do not like Google. And they're very privacy, you know - and this is where sometimes you can go too far on the privacy thing.

Steve: Well, I'm glad that Europe is as privacy concerned as they are because I wish...

Leo: But let's be realistic.

Steve: I wish the U.S. were more. But so if any of that leaks over here, that would be good. But this is just ridiculous. I mean, I'm sure he's a bureaucrat. He has no idea about the technology, and he assumes that it was some plot on Google's part to collect this data, which they have no interest in whatsoever. We know that.

Leo: The German Bundestag voted to prevent Google from linking to newspapers. The newspaper publishers were complaining that Google was stealing their content by putting them in its search results.

Steve: After they put it up on the web.

Leo: Yeah. So there's a certain amount of unclearness about this whole thing, I think.

Steve: Yeah. Would you like anyone to find your articles?

Leo: Well, that's the problem.

Steve: And see your ads on your website?

Leo: Yeah. Rupert Murdoch said the same thing, and he blocked Google from searching his properties, I think, in the U.K. And after about a year he said, you know, never mind.

Steve: That didn't work out so well.

Leo: Please index our sites. Please. We beg of you.

Steve: Yeah. So speaking of Google, some very clever malware authors managed to sneak some bad stuff into the Google Play app store. This came to light late last week. Apparently, no one's exactly sure what the count is, somewhere between two and nine million malicious apps were downloaded. And the way this was done was clever. This was in 32 apps, spread across four different developers.

Leo: Oh, I didn't realize this. Oh.

Steve: Yes. They were always intended to be malicious. But they weren't when they submitted them.

Leo: So individually they weren't? Or did they update them?

Steve: Exactly. They updated them. They waited months. So they submitted them to the store, 32 different apps, all submitted to do random, presumably useful things. I mean, apparently nine million people thought so, up to nine million. And then they bided their time for several months...

[Homer Simpson's voice in background]

Leo: Never mind. That was my yabba-dabba do.

Steve: ...and said - was that Homer?

Leo: It was. I'm so sorry.

Steve: That's all right. And then after a few months they slipped in malicious updates that were causing those apps to contact remote servers every four hours to send back harvested data, including the device's phone numbers and the IMEI numbers, which we were talking about last week. You peeled the label off the back of that phone because also it's built in. And in some cases they were also causing the devices to then download the AlphaSMS trojan, which sends text messages on behalf of the user to numbers that incur charges, heavy charges. So anyway, I just thought that was interesting. So here - so basically what's happening is the bad guys are smart. We know the bad guys are essentially the same people as the good guys, they're just bad. So they're as smart.

Leo: [Laughing] There's the same intellectual capacity.

Steve: Exactly.

Leo: Just a moral compass that is lacking.

Steve: They took the other branch in the road.

Leo: Yes, yes, the fork in the road, yes.

Steve: And so we have the Spy vs. Spy sort of scenario, the white spy and the bad spy. And so the bad guys look at the security models, they look at the protections and the barriers, and their whole mission is, hmm, how can we sneak past this? And so, oh, let's put out a bunch of good apps, and then they'll go bad after a while, after we've built the trust of users and acquired a reputation and no one's had a problem with them. And so this subverts things, like the how long has this been published, because we tend to mistrust brand new things. So let it age for a while. So we trust it. And, ooh, look how many people have downloaded it. It must be okay.

So they used all of that sort of natural reputation that apps get over time, just by waiting, and then they slipped the bad stuff in. Of course Google immediately yanked them, as soon as this malicious behavior was detected. But they had their day; they had their 15 minutes. So I thought that was interesting. I mean, it's like, where there's a will, there's a way.

Now, really, really good news. Not only just granularly good news, but industry-wide. And so we're tempted to use the acronym OTPMFA, which is actually two acronyms. OTP is One-Time Password, and MFA is Multifactor Authentication. Because we had last week Microsoft announcing that they were adding two-factor authentication to their stuff, Microsoft Account, whatever that is. And then, just in the news, I think it was yesterday, or maybe today, this morning, Twitter has said - I guess they posted a job listing in February specifically saying we want somebody with expertise in multifactor authentication.

Now, what's really encouraging is that Microsoft's multifactor authenticator - they of course have one for Windows Phone which is called Microsoft Authenticator. It is standards compliant. There's an RFC 6238 which is the specification for a time-varying one-time password. And we talked about this years ago. I mean, here I'm holding up my still-going-strong little gray football that we talked about, which is a time-based multifactor authenticator. And right now I just pushed a button, it says 901668, which I can tell everybody because it expires in 30 seconds, and then it's going to change to something else.

So the good news is we are, I mean, this is really beginning to happen. We've got Google. There are Bitcoin exchanges. Facebook, Yahoo!, Amazon Web Services, Dropbox, DreamHost, Blizzard's Battle.Net, Valve's Steam, and LastPass. Not only are they time-based one-time tokens, one-time passwords, but they are all based on the same standard. So what I'm excited about...

Leo: Oh, I didn't know that.

Steve: Yes. They are all cross-compatible. You can use Google's Authenticator to log into Microsoft.

Leo: Yeah, I do that. And I use Authenticator for LastPass, for Google, obviously. That's really handy.

Steve: Yes. And so we talked a long time ago about the problem, we called it the key ring problem, of needing to have a whole bunch of different key rings, or a key ring full of individual tokens, one for each service. And we were praying that that was not going to happen. The model that VeriSign worked on was their proprietary model, where only they would know what the serial number was of your token, and they would provide the authentication service. What I remember hearing was they were extremely expensive to use. I mean, yeah, you've got VeriSign's name and everything branded all over your stuff, but ouch. Pricey. So here we finally have moved to, I mean, this is exactly what we want, which is an open platform. It's device-based. In Microsoft's case, they will send you a one-time password via text message, or you can use the Authenticator.

Leo: That's great.

Steve: And there are also some very nice-looking iOS apps. I can't speak for the Android. I haven't gone over and looked. But, for example, I just was poking around to see what was out there. There's something called HDE OTP for iPhone and iPad. What I like about it is it shows you a screen of all of your different one-time passwords, all changing at the same time. So you can sort of scroll through the various accounts that you have established, and it shows some sort of a little meter with the one-time password expiring, how much longer it will be valid.

Leo: Yeah. That's what Google Authenticator does, too.

Steve: Yeah.

Leo: So I have my LastPass and my Google in there, and there's a little clock running out, and then there'll be a new one in a few seconds.

Steve: Right. Really, but what's so nice is that these things are...

Leo: So this is an open standard. I didn't realize that.

Steve: That's what's so cool.

Leo: So everybody should use this.

Steve: Yes. In fact, I looked around for any announcement about what Twitter was doing, and I couldn't find anything. It's probably a little premature. But they'd be crazy - and that's my point is with this much inertia now, why would anybody create their own nonstandard one-time password solution?

Leo: Right.

Steve: They're just - there's no need for it.

Leo: Good, I hope not, yeah.

Steve: Yeah.

Leo: Well, it's also good for us because I don't want to carry multiple dongles or have multiple apps. I can have one app that has all my one-time passwords. That's beautiful.

Steve: Right. Right. Anyway, I'm just - I'm delighted because this is a great development. Now, it's worth mentioning that it's not a perfect solution. That is, you still have the problem of real-time interception. In fact, that's why I deliberately read that number out, was I'm sure people are going, wait a minute, Steve, you just gave us your number for the next 30 seconds.

Leo: And I just gave out my LastPass and Google numbers, too, onscreen.

Steve: So that's an example of the remaining vulnerability in this system. We've seen instances where a CAPTCHA can be cracked in real-time by sending it off somewhere to a CAPTCHA cracking farm or people who are needing to solve CAPTCHAs for some other purpose, and so they're - and that's an instance where a bot is essentially able to use a human as its worker in order to solve a problem that it can't solve. It is possible to do, I mean, in theory to do a real-time man-in-the-middle crack where you would intercept somebody's submission of their currently authentic and correct one-time password and block their submission, log on as them, and grab their session.

So it's not absolutely perfect, but it is a huge step forward because, I mean, for example, it completely, as long as there aren't other problems, if people's passwords get loose, well, that's no longer enough. If you have an email account, which is typically your username and account identifier, and your password, historically that's all that's been needed to break in. So we understand that this raises the bar in a very useful fashion. And, yay, we've got a standard, which is...

Leo: Yeah, god, I hope Twitter does this. I hope they're sincere about - or this isn't just a rumor.

Steve: They have to. No, no, Twitter's definitely doing it. But the question is will they be compliant. And I can't imagine...

Leo: They'd better be.

Steve: ...that they would, like, make people go out and get their own app. That would be just crazy at this point.

Leo: Crazy talk.

Steve: And I think, my point is we have so much inertia now that it's a fait accompli, essentially. It's going to happen. This is the way we do this.

Leo: Right.

Steve: Also there was some concern, and I think it was already out by last podcast, but I didn't have a chance to get to it, I wanted to address it, and that's the concern about a design flaw in 1Password, which is a very, very popular...

Leo: Very popular, yeah.

Steve: ...password manager. It's interesting to discuss here because of what the problem was. The guy who is developing the HashCat system, we've talked about him in the past, it's oclHashCat-plus. This is the GPU-based, massively fast, password-cracking, hashing system which supports an incredible variety of hashes and crypto standards. He decided to add support for TrueCrypt cracking in his HashCat system.

Now, what that means for us is that there will be an open source brute-forcing technology specifically designed for TrueCrypt. But TrueCrypt is only as strong as the password. We've spoken of that often. There was the famous case of somebody in Brazil, the Brazilian authorities were unable to crack the drive because it was protected with TrueCrypt, so they sent it up to the FBI here in the states, and the FBI couldn't make any more of it because the person had used a really, really strong password. So the fact that we're going to get cracking for TrueCrypt is interesting, and it advances HashCat's breadth of coverage, but it doesn't - it's not a concern unless you've got a too-short TrueCrypt password that would make it vulnerable.

Leo: This is true in general, isn't it. I mean...

Steve: Yes, exactly.

Leo: ...there are rainbow tables and other systems that will crack bad passwords. But a long random secure password, the kind generated by 1Password or by LastPass or KeePass, you'll be fine.

Steve: Right. And so I wanted to make sure, though, because when I talk about TrueCrypt cracking, there will be people who will, like, oh, my god, TrueCrypt has been cracked. It's like, no, no, no. It's just making more available the technology for doing that, but that's been around already. So one of the TrueCrypt algorithms which famously protects TrueCrypt is AES, the Rijndael cipher. And this developer did not have support

for AES in his GPU technology. So he said, okay, I've got to add GPS cipher handling. Which means, for example, the key setup for AES, where you take a small key, the AES 128-bit key, and expand it to much more data because each round of the AES cipher uses a different chunk of key-derived material.

So he had to write a bunch of GPU accelerator code specifically to support that, which he had never done before. So he said, okay, if I'm going to do that, what's around that uses AES that would be simpler to do before I tackle the whole TrueCrypt problem? And he said, oh, 1Password. 1Password is a pretty simple, straightforward encryption system. It uses PBKDF2, the password-based key derivation function, in, like, many thousands of iterations. So it's been well designed by guys who know crypto. And what that produces is an AES key. So he already - oh, and it uses SHA-1, the hash, in its PBKDF2 algorithm. He already had SHA-1 programmed on his GPU. So this was beautiful because to do TrueCrypt he needed all kinds of more stuff.

And he thought, okay, I'm going to get the AES code all working just using 1Password. That caused him to look deeply into the algorithms that 1Password was applying, and he found kind of a mistake. The idea was that 1Password would verify a password was correct by running the submitted, the user-submitted password thousands of times through the PBKDF2 algorithm to so-called "password strengthening," basically to slow down any brute-force attack. But they needed a 128-bit key for AES and another 128-bit initialization vector for the cipher block chaining that they use. Well, that meant they needed 256 bits. But SHA-1 produces 20 bytes, which is only 160 bits. So you needed to use the SHA-1 hash twice.

Well, what it turned out was that it actually wasn't necessary to, in order to check whether a password was correct, to do the entire setup for decrypting the password. And so essentially what this news was of a design flaw amounts to maybe one or two bits of entropy lost. Meaning maybe it's half or a quarter as hard to brute-force crack the password. And in practice, that means that it probably won't take you 376 years to crack it. It might only take you 192, or maybe 96. People vary in their estimations.

The point is it hasn't dramatically hurt 1Password. There was in fact a discovery that, due to the way they were authenticating passwords, it wasn't as hard from a brute-force cracking standpoint as it was believed to be, but only by a factor of maybe either two or four, depending upon some optimizations that may be available. So it's like, okay, a tempest in a teapot, I think. I mean, they're going to fix it. Mostly it was users being worried that this meant 1Password was cracked now and dramatically less safe than before. That's not the case. Absolutely not the case. So just a bit or two worth of strength weakening, and nothing more than that. So 1Password users should not worry.

Leo: Good. That's a relief.

Steve: And same, yes, same advice applies, as always, which is use a good, strong password, and you'll be as safe as you can be.

Leo: Let the password programs generate the passwords. Although the issue with 1Pass and KeePass and LastPass is, that's the one password you want to memorize. So you don't want to make it too cuckoo.

Steve: Yes, yes. Or...

Leo: By the way, it's working great with the experiment with my 80-year-old mom using LastPass. It's working great.

Steve: And you helped her to come up with a neat way to remember a cuckoo password.

Leo: I gave her a mnemonic.

Steve: Yup.

Leo: And it's not easy, but she can reconstruct the password in her head.

Steve: Every time she needs it.

Leo: Every time. She actually memorized it. And I think it's 16 or 20 - it's long. That's the nice thing about a good mnemonic, you can make it long. And as we know, I think we know from your password padding exploits, that longer is better.

Steve: Yes.

Leo: Yes.

Steve: Yes. Okay, now, I have to apologize to the people who were confused, and there were some last week, by my discussion of the point-to-point tunneling protocol, which proXPN supports in addition to OpenVPN in the paid-for model. And I should mention that a lot of the other VPN providers do also. And that's the sort of the de facto protocol that all the mobile devices use.

Leo: Yeah.

Steve: But it's not nearly as secure as SSL, which is what OpenVPN uses. And I just, you know, I know that. We've talked about it often. But I didn't say it again last week. And so that's my apology is I should have explained that when I was talking about, for example, using it to protect yourself at Starbucks, whereas in an open WiFi environment, if you had no protection, everything you're doing is in the clear. Well, so any encryption is way better than none. And PPTP is natively available as the VPN protocol in iOS and Android and other mobile devices. So you don't have to install anything in order to get it.

But we also talked last summer about Moxie Marlinspike's announcement, and it was in early August, I think, of his Cloud Cracker. And what Cloud Cracker does is you can capture point-to-point tunneling protocol traffic and submit that to - you run it through a little open source app first to extract some of the handshake details that it needs. You submit that to Cloud Cracker along with $200, and a couple days later it will give you back the result of essentially cracking what is a 56-bit DES key.

So the problem with PPTP, the point-to-point tunneling protocol, is that it's normal encryption technology. And mutual authentication is based on, I mean, it's old. It's NT4 and Windows 98 era. So, I mean, it's not surprising that it's a little creaky. But that's also why it's so ubiquitous. It's available everywhere. But you do need to use it with caution. And so that's the point I wanted to make that I should have made last week. And so I apologize to our listeners who said, wait, I mean, I got a lot of mail saying, wait a minute, you said it wasn't safe to use it. Uh, okay, so, right. It's old. And 56-bits is no longer enough protection. And Moxie now demonstrates that for $200 he'll crack it in about a day.

Leo: Wow.

Steve: So if the model, if the attack model was that the entire communication session, at least starting at the beginning, because you have to have the initial handshake, and then you of course would want to keep capturing the traffic in order to be able to decrypt what had happened, if you captured all of that and then ran it through the pre-processor and submitted it to a DES cracking system, and there's one online that you can rent for 200 bucks, then a couple days later you can decrypt that traffic. So that's the downside of point-to-point tunneling protocol.

But the other thing that came to light that I was not aware of last week, and many people made me aware of it, is that there is an official OpenVPN client from the OpenVPN Project on iTunes. And so you can use OpenVPN on your iOS devices, and presumably Android, although I haven't looked, just as easily as you do use OpenVPN client on your laptops. So there is no need to use point-to-point tunneling protocol. And anyone who is put off by the fact that all their traffic could be captured and could be decrypted in a couple days, by all means, definitely I'm glad that people held me to account for this because we've discussed all this before, and I sort of assume that this is...

Leo: Some people don't listen to every single episode, Steve.

Steve: Yeah. I assume it's in our knowledge base. But anyway, so I should have said it last week, and I apologize for not doing so.

We've had a mixture of feedback. I got a lot, there was a lot of Twitter activity. Someone, Ryan Jones, whose description calls himself an IT professional from New York City metropolitan area, co-host and producer of the Fifth Down podcast, which I guess that's a football reference? He said, "Loving #proxpn," and that's all he said. And then Erik Chavez, who tweets as @homesicktxan, he tweeted to the proXPN people, who by the way do answer their Twitter feed, I've been seeing a lot of back and forth chatter with them, said "Signed up for one year of @proXPN thanks to @leolaporte and @sggrc. So the promo code is good for subsequent renewals?"

Leo: Right.

Steve: And they responded, "Yes, it's for subsequent renewals, too."

Leo: It was a lifetime promo code, lifetime...

Steve: Ah, and then he said, "Great speeds so far."

Leo: Good.

Steve: Now, I've also heard people say not so great speeds. I've heard - I saw somebody else say that his YouTube seems to be playing much faster through proXPN.

Leo: That does not seem right. But okay.

Steve: So your mileage will vary. And I did see some people complaining that the free use was just driving them crazy with dunning them to upgrade to the paid model. That's the one complaint that I did mention last week which I did see online in a forum somewhere. I have still not had a chance to play with it myself.

So again, it is what it is, but that's the - and so we've had generally positive feedback except that people were saying, wait a minute, I didn't think PPTP was secure. And now people know exactly what the nature of its insecurity is. It's way better, if you don't have OpenVPN, than completely unsecure WiFi in an open WiFi mode. But if you're trading state secrets in a mode where your traffic might be captured, and Moxie Marlinspike is going to earn $200 from someone for cracking your traffic, then by all means it's not safe enough.

And I did get a nice follow-up from Shannon Coleman, who said, "Thanks for the Opera suggestion on Security Now!." And Shannon said, "Much better than Chrome! LastPass support with an add-on and native side tab support." Now, I did not know about native side tab support or LastPass. So I'm glad for both. I'm still sitting over here on Firefox and very happy. But, boy, Opera really did impress me, as I mentioned last week.

Leo: I'm going to have to try it now after all you've said about it. And this is big. Having LastPass is critical for me. I won't use a browser that can't support LastPass.

Steve: No, it's not possible to use, I mean, I don't know what any of my passwords are anymore.

Leo: Right, you're not supposed to, right.

Steve: I mean, yeah.

Leo: Yeah. Yeah.

Steve: Yeah. Okay. A little sci-fi break. Oh, my god, Leo, this summer, oh, it is just a

gala of science fiction. I'm just, like, a pig in you know what. I am so happy. I just look at these previews and just think, oh, yes, bring it on. So Friday "Oblivion" opened. I've already tweeted twice about it.

Leo: Is this the Tom Cruise one?

Steve: Yes.

Leo: Okay. Okay.

Steve: Yes, yes, yes. And no spoilers. You will never, ever hear a spoiler from me. Think about it. When I've been talking about science fiction books that I've loved, I've managed not to give anything away. So I loved the movie. I mean, it's not an incredible, ground-shaking, you know, like when we first saw "Star Wars" or "E.T." or something. But...

Leo: "The Matrix." That was the one that, when I saw that, I walked out of there, my jaw on the floor.

Steve: Dazed, yes.

Leo: Yeah, yeah.

Steve: So this isn't that.

Leo: And Morgan Freeman's in this one, too.

Steve: But it's great. I've seen it twice, in fact.

Leo: What? Now, is it based on a sci-fi novel or...

Steve: No. I asked Jen because she generally knows these things, and she said no. And I then spent the next - I guess I spent, what morning was it, maybe it was Saturday, reading the negative reviews of the critics. And some people just hated it. And it's like, okay, I mean, I understand, I mean, some people seemed to have something, a problem with Tom Cruise himself. I don't.

Leo: I don't like Tom Cruise, but I can - but, you know, "Minority Report" was good. He's done some great sci-fi movies.

Steve: Yeah. I wouldn't say this is great; but, oh, it's a visual feast. It is beautifully

visual, and the sound design is really exceptional, too. They've got a bunch of drones who just make really wonderful sounds when they're, you know, just sort of - sort of an advanced R2-D2 sort of thing. And anyway, I loved it. And about 30 minutes in I whispered to Jenny, I said, "I'm going to see this again immediately." Just because I wanted to experience it again. I mean, I'm that way. I own a lot of these movies on disk, and I'll own this, just because after it's been long enough I will watch it again, in the same way that I'll read a book, a sci-fi book that I've already read, I'll read it again just to bask in the suspension of disbelief.

Leo: The guy who directed "Tron Legacy," which was also beautiful, not a great movie, but beautiful looking, did this one. Rotten Tomatoes, 56 percent from critics, that's pretty poor, that's a splat; 68 percent of users. So I think you're not alone. I think people liked it better than the critics liked it.

Steve: Yeah, and it did dominate the box office. It did just shy of $40 million in its opening week, which is better than both of Tom's previous movies combined. So, I mean, it's like, if you don't want to see it, you won't have to wait long for something else really good because "Elysium" looks fantastic with Matt Damon. We of course have "Into Darkness," the next...

Leo: I'm glad sci-fi is back. I am glad it's back, yeah.

Steve: Oh, my god, yeah. Oh, and we've got that cool, what is it, the Earth one, "Back to Earth" or "Old Earth" or whatever it is ["After Earth"], and that's I think Will Smith and his son and, oh, anyway, it's going to be a summer of wonderful movies.

Leo: It's based on a graphic novel, apparently, that the director wrote. Oh, is he the guy who did "300"? He is, isn't he. He's the guy did "300." The Chicago Sun-Times says, "If nothing else, 'Oblivion' will go down in film history as the movie where Tom Cruise pilots a white, sperm-shaped craft into a giant space uterus."

Steve: Oh, I was afraid that that was the guy. I read that on Saturday morning.

Leo: Not good. Richard Roeper, though, said that this is "the sci-fi movie equivalent of a pretty damn good cover band." I don't know what that means. But he does give it - he does like it.

Steve: Yeah. So here's my point. And we went with some people who I think are not sci-fi people, and they were, like, eh. And I just thought afterwards, okay, well, they just don't like science fiction.

Leo: So you have to like sci-fi.

Steve: Just drape a phaser over anybody, and I'm happy.

Leo: Yeah. I love sci-fi.

Steve: Yeah, I do, too, obviously.

Leo: Yeah, yeah. All right.

Steve: So, but, you know, it was great. Maybe people could wait till it comes out in some other format, if they're really not avid. But...

Leo: But wait, though. Is this a big movie you want to see on a big screen with surround sound and thundering...

Steve: I think so. I saw it the second time in a smaller theater, and I missed the impact of the sound. And, I mean, because this was - there's a lot of sound in this. And I just think it was a fun - I think it was absolutely worthwhile.

Leo: Not worth waiting, then, till DVD or whatever they call it. Used to be wait for DVD. Now I guess it's wait for Netflix or I don't know, wait for on-demand. But not worth it, it sounds like. So go see it.

Steve: And by the way, did you see that Netflix has already recouped their entire two-season investment in "House of Cards"?

Leo: Yeah, yeah. So did the stock market.

Steve: Oh, wow.

Leo: Netflix, because they now have more subscribers than HBO, I think that they...

Steve: Yes.

Leo: You know, last summer when Netflix - people were really critical of Reed Hastings, the CEO of Netflix, said he made a stupid move by splitting the DVD by mail from the streaming and...

Steve: I remember that.

Leo: ...and charging people extra, and everybody said how stupid they were. I said, wait and see. Reed is not a dumb man. This is a very, very smart CEO, one of the

smartest out there.

Steve: Didn't they go back on that decision, though?

Leo: They changed it a little bit. But you know what, do you have DVD by mail with them?

Steve: No.

Leo: No, nobody does.

Steve: No.

Leo: Those 30 million subscribers, streaming. He was pushing, and I think people complained, but in the long run they won.

Steve: Oh, so he was trying to move his customer base over to online.

Leo: Yes. The reason is the Hollywood folks are squeezing him and won't let him have movies. They won't let him have - there's a 30-day delay after the movie comes out. They're giving it to on-demand services first, blah blah blah. They were squeezing him. And so the DVD by mail business was dying. And people said, well, the streaming stuff isn't as good as DVD by mail. So he really needed to - he's pivoted. The company's pivoted. And what they've done is they've become a content creation company, and - like HBO.

Steve: Yes.

Leo: And I'm a believer. I have never given up on them. I always thought their model was very good. Too bad I don't like [indiscernible].

Steve: "House of Cards" was great.

Leo: Wasn't it amazing? I can't wait to see Season 2. Is it out yet?

Steve: No. I was so happy that they had a second season. Already paid for. I mean, they've already produced it.

Leo: I know, it's done.

Steve: It's done.

Leo: Kevin Spacey will be on when Season 2 comes out. I've already extracted a promise from our friend the producer, Dana Brunetti. He said we'll get Kevin on. I tried to get him on when it first came out. He said, you know, "He's exhausted. He's on vacation. Do you want to do it when Season 2 comes out?" I said yes.

Steve: That would be cool. I remember when you had him on The Screen Savers.

Leo: Yes. Kevin's a geek. Big geek.

Steve: Yeah?

Leo: He loves this stuff.

Steve: Yeah. Okay. So energy storage update.

Leo: Okay, good.

Steve: Many people also tweeted.

Leo: I need to know about this.

Steve: Also tweeted. What happened was the publication "Nature Communications" came out with an article celebrating a breakthrough in chemical battery storage, so not supercapacitor, but chemical battery. And I have and I have read and studied the complete article. It's titled "High-Power Lithium-Ion Microbatteries from Interdigitated Three-Dimensional Bicontinuous Nanoporous Electrodes."

Leo: Oh, that.

Steve: Yeah. And it's cool.

Leo: Okay, good.

Steve: Now, what I love about this is - so the problem with traditional electrochemical batteries is that they are electrochemical. That is, in order for them to be charged and discharged, you have to have the migration of physical ions through the electrolyte between the battery's two electrodes. That is, physical migration, so it takes time. And that physical migration creates resistance. And so what this ends up meaning is that the battery can only be charged and discharged at a certain rate. And if you push it too far,

then it begins to get hot.

And of course we've famously seen all kinds of battery explosion problems over the years. That's what happens is these batteries end up being pushed too hard. That's what supercapacitors don't have. Supercapacitors are just two electrodes super close together with as much surface area as possible, and then you just pile on the electrons. So there, there is no, by definition, there is no resistance at all. But you're not storing the charge electrochemically. You're storing it electrostatically, so just in an electrostatic charge.

The problem with supercapacitors is, in order to store a lot of power in the capacitor, you need to have a lot of voltage. That is, you pour the electrons onto one of these plates, pulling them off of the other, which creates a tremendous need for there to be essentially like a spark between them. So there's a dielectric which insulates them. And that's the challenge is to have a supercapacitor with a large plate area where the plates are incredibly close together, yet the dielectric strength insulates them against the incredible voltage difference. And that allows them to store power.

But when they store that power, it's available virtually instantly. That is, I mean, that's one of the dangers is, like when you're driving a car around with supercapacitors, you definitely want to make sure you've got fuses all over the place so that it just doesn't suddenly unload all at once.

Leo: You know, this is - people say, oh, gosh, well, I'm never going to use it because of that. But all of these systems are, if you think about it, you can't push a car around without a lot of energy stored somewhere. And the sudden release of the energy, whether from gasoline explosion or from sudden discharge of a supercapacitive battery, is going to be disruptive to the space-time continuum.

Steve: Yeah [laughing]. There was a car project that Ben Rosen, a famous venture capital guy, invested huge amounts of money in, where their energy storage was a spinning flywheel.

Leo: Right, right.

Steve: He had a flywheel spinning in a vacuum chamber, and he electromagnetically coupled the spin so that he would pour power in and spin this thing up and then actually run the car on the mechanically stored energy of the spinning flywheel. And the great problem was, if it ever got loose, it was like a whirling dervish from hell. I mean, it would just chew anything to pieces.

Leo: Right.

Steve: And so there again...

Leo: It's going to always - I don't care what you use. It's always going to have - because you don't move a car around for a few hundred miles without storing a lot of power, a lot of energy somewhere.

Steve: Huge, a huge amount. Okay. So get a load of this. What these guys did was they dramatically improved on existing, all existing electrochemical battery technology. So this is significant. They created electrodes. One of the things you need is you need electrodes with high surface area. That is, you want, like, well, they call it "nanoporous." You want to think of it sort of like an incredibly porous sponge, so that the electrode itself has a very, very high surface area, so that it's in contact with a large volume of electrolyte. What that means is, first of all, it lowers the resistance because you've just got so much electrode surface in contact with the electrolyte. And it also means that, if you're able to get these electrodes close to each other, that the total electrode distance, the separation is low. That lowers the ion transit time. Remember, that's the problem with electrochemical cells is they have to physically move ions through this goop. So having large surface areas and closely spaced electrodes solves those problems.

So the way they made these is so cool because we can all visualize this. They started with microspheres, polystyrene, like a volume of microspheres held in a colloidal suspension. So just like mixed in a goop, or like these microspheres. And they came up with a way of making them self-organize. Everyone's sort of familiar with, like, when you put billiard balls in a rack, how all the balls are able to pack. And if you think about it, you can pack another layer of spheres exactly on top of that layer and so on. So it's possible to create a solid array, almost sort of like a crystalline lattice, of spheres.

So what these guys invented was a way of evaporating the suspending fluid, which contains all these spheres, so that, as the fluid evaporates, the surface tension meniscus at the boundary of the fluid automatically organizes the spheres into a solid array.

Leo: Whoa.

Steve: I know. It's so cool. So it works. So now they have...

Leo: That's surface tension at work.

Steve: Yes, exactly. Surface tension is your friend.

Leo: Yeah.

Steve: So now they have an array of spheres that are densely packed, touching each other on 12 sides. So it's intimately arranged. They then electrochemically plate this spherical array so that - and when you think about it, if you think of spheres, they're touching, but there's also spaces in between; right? There's also - there's, like, the nonspherical areas, the sort of funky triangular curvy-shaped areas, if you can visualize that, that is all the air, all the air spaces that exist where the spheres are not in this array.

So they electrochemically plate this array so that all of the areas that are essentially the air get plated. Then they have an agent which is able to dissolve the polystyrene spheres. So after they create and after they plate all of the exposed surface area of the spherical matrix, they then essentially remove the spheres from the middle of it. They dissolve the spheres out of it, leaving this amazing - oh, oh, I should say one thing, I forgot one step is when they've got the spherical array, they heat it up, and the spheres

soften a little bit. And so the spheres deform and come into greater contact with each other, and that changes the overall shape in a way that is beneficial to them.

Then they dissolve the spheres out of this so they end up with what they called a "scaffold." If you can picture this, this is a scaffolding of essentially the spherical, but now a little bit deformed, outlines of the spheres, all interconnected in a solid piece. So it is a nanoporous mesh. And that is the basis for their electrodes. They then plate one of them with a negative electrode substance, and the other one with a positive electrode substance. They've come up with a production methodology that allows them to do this in a production mode. And they end up with, and this is what's amazing, is electrochemical cells which can charge and discharge at the rate of a supercapacitor and store on the same order of energy, hundreds of times more energy per volume than traditional lithium-ion batteries. And so it is a breakthrough. Now, the one glitch, Leo...

Leo: There always is, isn't there.

Steve: There's always a glitch, is it doesn't cycle very well. If you charge it and discharge it and charge it and discharge it, when I was - I was all excited as I'm reading the paper. And then it's like, whoa. I mean, it loses, like, 16 percent of its capacity after the first cycle, and it goes downhill from there.

Leo: So this is nice, but it works once, is what you're saying.

Steve: Well, today. I mean, this is also, you know, they're publishing their research. This is a really interesting, possible-to-fabricate technology that outperforms every other, I mean, there have been people who've tried to do nanoporous electrodes of various sorts. This just blows past them all. So this is a huge step forward. What it does represent today, it is not only more rapid charging, but also much greater total energy density. And so there are applications, for example, think a pacemaker, where you want - and that's really how they're selling this now. Remember it's called "high-power lithium-ion microbatteries."

So they're not suggesting that this is going to replace the high-end lithium-ion cells we have in our electric cars today. But they're saying today it is vastly superior to existing battery technology for, like, implantable medical devices, where you're not having to charge and discharge on a daily basis. So the cycle life of the battery is not a problem. And this allows whole - basically it changes the terrain for medical implantable devices and also long-term remote sensors, or maybe, for example, satellites, where they've got exotic power supplies now that are arguably maybe not safe because they typically use radiation sources. You could probably replace them with these kinds of batteries and be vastly less expensive, lower technology, and also long-term sustainable. So very cool.

Leo: Someday.

Steve: Yes. So this is just a step forward. And we still don't know whether supercapacitors are going to get there before nanoporous, multidimensional, continuous, spherical-derived, electrode-based batteries. But this is a nice step forward.

Leo: I'm just really glad that they're working on this stuff. That's the key. They must be, of course. This is huge. Because we've essentially created, and smartphones are the perfect example, but cars are another really good example, highly sophisticated mobile technology that has outpaced battery technology by a century.

Steve: Yes. And in fact the article starts, in its abstract at the beginning, talking about how, despite the fact that microelectronics has enjoyed incredible scaling factors in capability and size, batteries have not changed all that much. But imagine if they could just solve the cycle life problem, and there's no reason to believe they won't be able to, imagine that our smartphone batteries still, well, they charge in a few minutes, and they last a week. I mean, and they're no bigger.

Leo: Okay. Thank you. I'll take two.

Steve: Yeah, I know.

Leo: Yeah. I mean, I have this phone; I love this phone. But especially because I'm using it so much, it goes half a day. That's no good.

Steve: No. We need to fix that.

Leo: Yeah.

Steve: Speaking of fixing that, I got a nice note, dated April 10th, so, what, two days ago...

Leo: Well, except that this is the 24th of April, but other than that, yes.

Steve: Two weeks ago.

Leo: Welcome to [inaudible].

Steve: And I just saw it in my mailbag. He [John Moehrke] said, "SpinRite saved my 85-year-old mother's laptop."

Leo: Oh, this is like my story, yeah.

Steve: He said, "My mother is a true geek grandma. She's been an early adopter of the Internet back in the '90s, so I'm not surprised that I, too, am a geek. I have provided Security Now! some feedback on the topic" - and he gives a URL. He has a blog, healthcaresecprivacy.blogspot.com. So I guess healthcare security and privacy. He says,

"It never is good when a security geek has a family member hit by a security or privacy failure."

Leo: Yeah.

Steve: Many of our listeners know about that. He says, "Well, it happened. My mom's laptop stopped and would not reboot. Absolutely dead. Being the good geek grandma that she is, off she went to buy a new computer. She was perfectly happy dumping the old computer. She wanted a faster, sleeker, and less noisy computer. She had no backup and actually was okay with the loss of information. Well, I was not satisfied with the lost data, so I got myself a SpinRite license and set it running on her laptop. It found the hard drive and got stuck at 0.032 percent." So clearly right at the front of the drive. He said, "I left it run, and it was still running days later. I moved the laptop out to the cooler temperatures of the garage in Wisconsin. Not cold, but floating above freezing." He says, "Yes, I shut it down to move it." He says, "There I left it running, and running, and running. Four weeks later it finished."

Leo: She bought a new computer by this time and has forgotten this other computer for a long time. But okay.

Steve: He says, yeah, he says, "FOUR," all caps, "weeks later it finished. It recovered ALL," all caps, "of the photos and documents on her old machine. I delivered them to her last weekend, a full CD-ROM full. Thanks for a fantastic and persistent product."

Leo: Isn't that awesome. Yup, it is persistent. And sometimes a month is not - is like, that's nothing. It could go for - what's the longest you've ever heard of a SpinRite running for before it completed?

Steve: Well, the problem Leo, is that if people drop it out of a four-story building, and it hits cement, that is, drops the drive, and so now it shakes when it powers up, and you can hear the rattly bits inside, well, SpinRite will try. But, you know - and it'll try till you say, okay, I don't know, but this is not going anywhere.

Leo: But there are cases where it's just a lot of really unreliable sectors, and it could recover them.

Steve: SpinRite tackles them one after another, and it will work on it until it gets it. And if you want your data back, SpinRite will not give up before you do.

Leo: Amazing. Amazing, amazing, amazing.

Steve: We're just now getting to...

Leo: Oh, we got time.

Steve: ...listener questions.

Leo: We've got time.

Steve: No, no, no, Leo, I mean, we've had a wonderful podcast so far. We're an hour and 13 minutes in. So let's just go until 1:00 o'clock, and that'll still give us an hour and a half of podcast.

Leo: We just had a lot to talk about.

Steve: There is. There was a lot to discuss this week. And I'm sure everyone's had a good time so far.

Leo: Yeah. Well, we'll get as many as we can in here.

Steve: Yeah.

Leo: We love our questions. You can go to GRC.com/feedback, by the way, to get your questions answered from Mr. Steve. And he picks usually around 10. We'll get to as many as we can today, to answer in our Listener-Driven Potpourri #168.

Vince Reimer, Vancouver - and this is interesting because I have one of these. He wants to know about his Nest hacking his nest: Steve and Leo, enjoy the show very much. Been listening since Episode 1. Have had success with SpinRite and haven't had one cold since I started on Vitamin D. So thank you. That reminds me, I've got to get my Vitamin D for the day here.

I recently bought the super-cool Nest thermostat. I have one, too, and I bought one for Lisa. I'm buying one for everybody I know. I love these things. I hooked it up, and it wanted to know if it should go online and check for updates. How cool is that, I thought, and readily gave it my WiFi password, assuming it was an innocent cul-de-sac on my home network. Then I got to thinking about the new smart electricity meter that had been installed by the power company with at least the incipient ability to talk to my future Internet-savvy fridge and air conditioner via my existing house wiring. I then wondered if it could talk to my smart appliances. And since my Nest knows my WiFi password, have I not created a hole in my home network security? What do you think? I know this is just a curiosity. But you have touched on interestingly edgy topics before, so I thought I'd ask. Sincerely, Vince.

I hadn't really thought about that. I have a smart meter on my - well, I think there's a lot of paranoia about these smart meters that the utilities are installing. Or is there?

Steve: Well, okay. So I think the right attitude to take is that everyone is probably trying to do the right thing. There have already been articles about the lack of security of the smart meters. And you could have predicted this. I mean, I'm sure our listeners who've been with us from the beginning, when they heard about smart meters, they rolled their eyes and thought, oh, this is not going to turn out well. And sure enough, they have, at least first-generation, really crappy security, easy to crack, I mean, I don't know what moron in this day and age could design something like that, that wouldn't be right initially, because again, a lot of these problems we know how to solve.

For example, we were talking about the one-time passwords. It's like, no one should invent a new algorithm for that. We've got that. That's done. Just use the one that everyone else is using, and you get all kinds of economies of scale. So don't go and reinvent that.

Similarly, we know how to do security for something like a smart meter. But apparently, for whatever reason, that's not what happened. Similarly, the Nest is, I'm sure, designed to be secure. The question is, did they get it right? Because, for example, routers were designed to be secure. And we know how many millions of them are exposing the Universal Plug & Play protocol to the public interface, which is totally insane. So there was a mistake.

So giving the Nest access to your network is probably okay, but it's arguably creating an opportunity for a problem to be exploited. So I know that you're able to access the Nest from the Internet. You can get pictures of it. You can change your settings. You can do things. Presumably it connects to Nest Central, and then you log into their website, and there's some communication. But that's creating a connection out of your internal network, where the Nest exists. And we know that it's microprocessor based, and it's smart. And we have seen instances where people are downloading trojans into people's routers. So you've got the same potential. Again, I don't want to upset anybody or scare anybody. I would say, if you hooked it to the Internet to update its firmware, then...

Leo: It's always online. It's always online. So it's getting the weather for my locale. In fact, I'm just - I just turned the heat down.

Steve: Ohhhh.

Leo: You think of it as a little computer; right? It's getting on your WiFi. I just turned the heat down. I can turn it up. My mom's at home. If she's cold, she can call me. I can say, yeah, I'll turn up the heat. And I can just turn it right like that. She's probably wondering why the furnace keeps coming on.

Steve: Leo's at work playing with his new toy.

Leo: I'm playing with my toy. So that's why it's online. And, yes, of course getting updates. But, I mean...

Steve: So what I was going to say was...

Leo: ...lots of devices get on the network; right?

Steve: Yeah. What I was going to say was, if you don't use the online features, then take it offline. Just standard security precaution. You close the ports you don't need rather than leaving them all open. If it doesn't need to be on the 'Net, if you're not using those network-enabled features, then tell it, like change your network password so it no longer knows what it is, or erase it from it, if you can do that. So, I mean, that's just what I would do. Presumably they did everything right. But now you're depending upon them to have done everything right. And we know that hackers apparently have a lot of spare time on their hands.

Leo: Right. Right.

Steve: And it represents another, yet another target.

Leo: Most of the features, I mean, there's a lot of features of the Nest. A great many of them want to be online.

Steve: Yeah.

Leo: I mean, it really...

Steve: Well, and you know, Leo, that was on purpose. I mean, that was - how are you going to sell, what is it, $300 or something?

Leo: Yeah, 250, yeah.

Steve: I've got one, too.

Leo: Oh, you do.

Steve: It's still in its box.

Leo: Oh, okay.

Steve: Oh, yeah.

Leo: I can lock it with a numeric locking PIN in an allowable temperature range.

Steve: Oh, that keeps the hackers from turning your heat up. That's good.

Leo: Yeah, I mean, I'm not sure what they're going to do with a Nest, to be honest. All they can do is turn the furnace on or not.

Steve: No, clearly when they were trying to leverage a $250 thermostat, they sat around thinking, okay, how can we justify this price? We've got to give this thing features that, you know, just coming out of its ears.

Leo: Well, and it does. It has some really, really great - it learns. It's got a motion sensor, so it knows when there's somebody in the house. It learns your settings.

Steve: I just like to look at it.

Leo: It's beautiful.

Steve: It's just gorgeous. Oh.

Leo: And really, seriously, if they get into my Nest, all they can do is turn the heat on or off. And you can block that. But I can see...

Steve: No, no. No, no, no. If it knows how to - if it's on your network, and they get into it...

Leo: Oh, they can get the password from it, I guess, yeah.

Steve: Well, then they have access to your network.

Leo: Right, right, right.

Steve: So, I mean, I'm not saying that's a likely...

Leo: How about putting it on a guest network or a separate access point or something like that? Would that...

Steve: That would work, for example, if you had arranged your home so that you had two WiFi systems, a trusted and a visitor WiFi, and the visitor WiFi was strictly - had no other access to the other systems in your home, then absolutely put the Nest on the visitor channel, yup.

Leo: Okay. Okay. That's easy enough. Question #2 - we're trucking along here. Trey Dismukes in Houston wonders about faked website fingerprints: If someone's running an HTTPS proxy on me, what's to stop them from altering the fingerprints you display on the fly? It seems like this tool would be more useful out of band. Perhaps an iOS app that will return the fingerprint when I enter the URL. He's talking about your fingerprinting app at GRC.com.

Steve: Right.

Leo: Or even an SMS short code I can text to a URL that will respond with the fingerprint.

Steve: So that's certainly a good point. I do talk about it and address it at the bottom of the page [grc.com/fingerprints.htm]. Everyone should know I'm hard at work on a next-generation solution for this. It's been a big hit. People really like the idea of being able to check for anyone intercepting their secure traffic. However, there have been problems with just sort of confusion. Some people wonder, they worry if the fingerprint is case sensitive, whether the hex being uppercase ABCD and F - wait, ABCDE and F - whether it matters that it's upper or lowercase. It doesn't. And so on. So I've got something that's very cool coming out soon. But I've been thinking about this problem of we're relying on a potentially intercepted connection to report on connection interceptions, which is obviously a Catch-22.

Leo: Hmm, yeah.

Steve: And then I thought, wait a minute. What about the EV certificates, the extended validation certs? Because I'm all EV, and my site shows up as green on all the browsers now that support EV, and in fact they all do. And so I did some exploring. And it looks like, and I still have to verify this, Firefox and Opera and Chrome on Windows all - and probably Chrome on Mac - still adhere to the fundamental principle of extended validation certificates, which is that they are special. They build into the browser an awareness of which certificate authorities' root EV certificates are valid for signing, and that can't be changed.

Unfortunately, Microsoft somehow didn't get the memo. They completely screwed up extended validation. There are even links that Microsoft has in their Knowledge Base about how you can make your corporate server come up green. And it's like, oh, no, that's, I mean, now it means nothing. If certificates not issued by EV certificate authorities can be made to show green on Internet Explorer, then IE is broken for extended validation completely, meaning that it's spoofable.

But the point is that the good browsers that have adhered to this cannot be fooled. So what this means is, if you go to GRC, and you're seeing green, there's no way that a proxy can intercept that for Firefox, Opera, and Chrome because they understand extended validation means what it's supposed to. And so that's one thing, the extended validation is something that no proxy which is intercepting SSL can spoof. It is unspoofable when it's implemented properly.

So that's, I mean, what that also means, if you know that your bank is extended

validation, all you have to do is see that it's green on one of the good browsers that correctly handles extended validation certificates, and you know you're safe. So I'm going to be adding, among other things, a display for extended validation so that you know if your bank is supposed to be EV, so that when you go there you can see if that's what you're getting. Which is a good thing because that will push the use of EV certificates, which are substantially more secure for exactly this reason, than non-EV certs.

Leo: Leo Laporte, Steve Gibson. We can be a little late for This Week in Google. Let's do a few more, what do you say?

Steve: Okay, sure.

Leo: You up for it? Kris Ackermans in Kortenberg, Belgium shares a wonderful tip for running 16-bit code on Windows 7 64-bit: Just heard you mention your concerns about running - you use Brief, which is not only 16-bit, it's DOS.

Steve: It's real 16-bit.

Leo: It's real.

Steve: It's actually maybe 14 or 15-bit.

Leo: Plus a parity bit - 16-bit programs in Windows 7 on Security Now! 399. Best way to do this is to use the XP compatibility mode infrastructure. Now, to do this, by the way, Steve, you have to have Windows 7 Professional, the business version. But install Windows 7 32-bit in the VM instead of XP.

Steve: Is it Pro or Ultimate? Isn't there an Ultimate also?

Leo: There's Ultimate will do. Yeah, I think Ultimate will have it. Ultimate must have it. It has everything. But the Pro will also have it, Professional. It was deemed, this XP emulation was deemed a business feature. So you're going to get the high-end business version of Windows 7. But he's saying don't use - so what you're going to get is, what is it, Virtual Drive, Microsoft's VM solution [Microsoft Virtual Machine], and a copy of Windows XP. But he's saying install Windows 7 in the VM. You could actually do both if you wanted to. The advantage to any other VM solution is the programs installed in the VM appear on the Start Menu of the host as all other programs do. And you only see the program's window. You don't get this big Guest OS window.

He says, I've been using a 16-bit accounting program like this since the IT department moved us to Windows 7 64-bit some years ago. So he's saying you can run Windows 7 64 as the main OS, use the VM - you could run XP, or you can run, if you prefer a more modern, you could run Windows 7 32-bit in the VM. And

essentially that gives you a 32-bit window.

Steve: That's really interesting, too. What I love is that they did it right, the way - I think it was Parallels who first showed us this. I know that we talked about Parallels years ago...

Leo: On the Mac, yeah.

Steve: ...on the Mac, where it just looks like you have Windows sort of like cohabitating with your Mac. So all you're seeing is the hosted application window sitting there without the whole - for example, I'm still using VMware as my go-to VM manager. And it's an environment that encapsulates everything, and then you work within it. But I love the idea that you could just launch an app and sort of behind the scenes it's actually firing up a 32-bit OS that supports 16-bit apps and then runs the app in that. So thank you very much, Kris. I'm glad to know that's possible. I'm sure that's what I'll be doing - for my DOS apps, of course.

Leo: Yeah.

Steve: Yeah.

Leo: You can have a command line. It's okay. Jehan Procaccia, or Jehan Procaccia - I have no idea how you pronounce this.

Steve: You did a good job of that.

Leo: I made it up. But that's - okay. No one knows except Jehan how much I'm butchering his name, Jehan Procaccia.

Steve: And his mother knows.

Leo: His mom. Mom's going, Jehan...

Steve: But she's probably not listening.

Leo: Why he say your name so bad? He's in Paris, France, and he wonders about bitcoin losses. Leo talked recently about backing up his bitcoin wallet. What would happen to the overall amount of bitcoin on the planet if one loses one's wallet? As creation of Bitcoin is limited in volume and time, will those lost bitcoins be allowed to be recreated, or are we going to have this kind of coin drain? Thanks for the good job, and blah blah blah. I wonder that myself. What do they do about that?

Steve: Yeah, and, you know, this whole recent bitcoin frenzy that we've been going through the last few weeks has spawned everybody with an opinion about what bitcoin means.

Leo: Even Paul Krugman is writing about it in The New York Times.

Steve: Yeah. I tweeted about a neat article, and I did get a piece back from a listener who said, oh, Steve, you've got it all wrong. Here's a link to somebody who really knows what they're talking about. Read this. And so I've emailed the link to my iPad, so I will probably read it tomorrow. I didn't have time while I was doing the podcast prep. Because I'm interested in what people think about this. But there is this notion, like a concern, which is valid, which this listener asks about, which is sort of like the evaporation of bitcoins, because there is no way to ever recapture bitcoins which are in wallets that are lost.

Leo: Lost or hoarded, for that matter. I mean, if there's somebody sitting on them...

Steve: Well, if they're hoarded they're - well, okay, out of circulation.

Leo: Out of circulation for whatever reason.

Steve: Out of circulation is different than destroyed. Because, if it's destroyed, it is gone forever. There is absolutely no way, because your entire evidence of your ownership is the signed crypto chain in your wallet, I mean, that's what you have that you're trading.

Leo: That's why I use Carbonite. Now we're really talking some value on the hard drive, literally.

Steve: Well, and I think that's exactly the point, is when people understand that there is no one you can go to to recover your bitcoins if you lose them, they're just gone. I mean, it's like burning paper money. If you throw paper money into the fireplace, you can't go to your bank or Uncle Sam and say, oh, gee, I burned a stack of money. And they're going to go, uh-huh, sure you did.

Leo: But the difference is the money supply can be fixed because the bank can print more.

Steve: True.

Leo: You know there's a huge - there's god knows how many billions of pennies are out of circulation. But the government just makes - don't worry, we'll make more. You can't make more with bitcoin.

Steve: Well, and so the countervailing aspect to that is that you can divide bitcoin down to microscopic size. I really ought to know how many zeroes there is. It's like 12 zeroes, you know, 0.000000000000 of a bitcoin you're able to transact with. So I just think this is going to end up regulating itself. People who lose them, oh, well, that's too bad. But the market will set the value based on the active trading. So if people are hoarding them, they'll just be out of circulation, and the market won't account for those.

Leo: This is the complexity of macroeconomics.

Steve: Oh, yes.

Leo: And unless you're a...

Steve: It's no wonder everyone has their own opinion and a different...

Leo: Yeah, if you're not a trained economist, it's kind of hard to understand how all of this fiat currency works and everything.

Steve: And actually, Leo, I don't think they know, either.

Leo: No, they're making it up.

Steve: I think they get degrees - yeah.

Leo: They're making it up. I'm just trying to look through...

Steve: They're wrong as often as they're right.

Leo: Yeah. Oh, yeah, we know that. In fact, did you see, there was a Paul Krugman article about some economists, I think they were at Harvard, who published a paper that was taken as gospel forever after that said that the federal deficit cannot exceed 90 percent or some disastrous crisis will happen. And so that Congress and everybody have been saying, you know, blah blah blah. It turns out they made an error in the Excel spreadsheet. They finally - they didn't want to publish the spreadsheet. They didn't want to publish it. Finally they gave it away, and people said, wait, you've got a - there's a mistake in here. It's like...

Steve: I love that peer review.

Leo: A literal error. And it's become gospel. And it's a typo.

Steve: Wow.

Leo: I just love this stuff. It was a great article.

Steve: And their common sense didn't lead them to the correct result. They believed their formulas over what their gut told them.

Leo: Well, exactly. Not only their gut, but evidence. Because in fact - I think it was the other way around. I think their gut told them, and they wanted the model to match what they thought was the case. And in fact they were wrong, and history has proven them wrong, but...

Steve: That's what we call bad science, Leo.

Leo: Yeah. Yeah. It's really interesting. The article was published April 19th in the Opinion section of The New York Times. It's Paul Krugman, who is a Nobel winning economist. He talks about two Harvard economists, Carmen Reinhart and Kenneth Rogoff. Their paper was called "Growth in a Time of Debt," and it said there's a tipping point for governmental indebtedness. Once it exceeds 90 percent of GDP, economic growth just ends. So you can't owe too much because then it will just kill it. And then it turns out, well, um, well, uh, there was a typo.

Steve: We meant, in our formula we had, we had M4, and we meant M5, so...

Leo: And then they said, but we really never said this 90 percent threshold. And of course, you know, they have admitted there was a little - you know, math is hard.

Steve: Yeah, well, economic science is an oxymoron.

Leo: Fascinating stuff. Fascinating stuff. Just amazing. Gosh, you know, it's amazing we survive as a species. Joe Rodricks - one more. We'll do one more. How about it?

Steve: Okay.

Leo: Do you want to pick one? There's six remaining.

Steve: Oh, there is one, yeah. There's something that I had intended to get to, where is it, No. 8.

Leo: All right. Brandon Brimberry. You just like his name. Brandon Brimberry in Indianapolis.

Steve: I am a fan of alliteration, yes.

Leo: Leo Laporte and Brandon Brimberry - wonders about the Butterfly Labs scam: What's the story on Butterfly Labs? I only know about it because I heard it on the podcast. Are they really going to ship their hardware on their website? This is the company that was making bitcoin mining hardware; right?

Steve: Okay. So let's get the question done, and then we'll...

Leo: Yeah, then we'll explain. The price and the specs seem too good to be true. Currently, if someone bought the 5 gigahash model on their website, with the current bitcoin valuation at $274 [coughing extravagantly] - that's not quite the right - not now.

Steve: Oh, that was last week.

Leo: Yeah, that was last week before the crash. At the current difficulty level and coin minting rate...

Steve: That was an hour ago.

Leo: Yeah, it was an hour ago - that miner would make around $900 a month. What's your opinion? Are these boxes going to ship? Is the whole company a scam? I ordered one, so your opinion is very important to me. I think they're shipping, I think they started shipping this week. I thought I read that. Also I noticed on their site they take PayPal and bitcoin. That's like the snake eating its own tail. I like the bitcoin idea, but it just dawned on me, if they never plan to ship any hardware, and they take bitcoin, hey, there's no governing power to give bitcoin buyers their bitcoin back, says Brandon Brimberry, bitcoin miner. What do you think?

Steve: Okay. So here's the deal. I have no information about, like, what the future holds. What we do know is, in the past, they have been real. They have shipped FPGA-based, high-performance bit-mining boxes. Lots of people are using them and very happy. That's why their credibility for their announcement of a super-galactically, screamingly fast, ASIC-based bit-mining box held so much sway. So what they've done is they've gone from FPGA, field programmable gate arrays, where you basically take a generic software-configurable hardware, an FPGA. They were using that to outperform the GPU, the graphics processing unit-based bitcoin mining hashing systems. Then they said okay, we've pushed FPGAs as far as we can. The way to really make screaming mining machines is an application-specific IC, meaning we're going to design our own integrated circuit from scratch. Now...

Leo: Is that hard to do?

Steve: Well, it's another - yes. It's another scale of difficulty. All kinds of things can go

wrong. So it may have been too great a stretch for them. Apparently, because I did do some poking around when I saw Brandon's question - because I should also mention this is representative of many of our listeners who are wondering if Butterfly Labs is a scam.

Leo: Well, I even see on the bitcoin forums considerable chatter about that.

Steve: Oh, huge amount, yes. And I have to say I was in a position once, I was going to ship SpinRite 3. SpinRite 2 existed; I announced SpinRite 3; we sent out the upgrade announcements. And just as I was getting ready, Microsoft released DOS 6, which incorporated compression in the OS, which SpinRite was completely incompatible with. And I thought, well, I can't ship it.

Leo: That was a nightmare. I remember that compression, OS-based compression.

Steve: Oh, Leo.

Leo: Oh, what a nightmare that was.

Steve: It was a disaster. But for me it meant...

Leo: Thanks, Microsoft.

Steve: ...that I had all this money from people who desperately wanted SpinRite 3, and I never shipped it. I shipped SpinRite 3.1, but I was six or seven months late. We kept offering people their money back, and they said, I don't want my damn money back. I want SpinRite.

Leo: Just give me the program, yeah.

Steve: And but I couldn't ship it if it was going to be incompatible with DOS. So anyway, I will never again, I mean, I learned my lesson. My column in InfoWorld was suspended because people were saying, how can Steve be writing a weekly column if he hasn't shipped SpinRite?

Leo: Yeah, get to work, Steve.

Steve: Like, yeah, that's a good point. So my gut says that these guys just got in over their head. Apparently they have this backlog.

Leo: It is delayed. It's delayed; right?

Steve: Oh, seven months.

Leo: Oh, okay.

Steve: Apparently seven months.

Leo: It's not shipping. I was mistaken. Something else was shipping, some other bitcoin...

Steve: So seven, yeah, well, there is. There's, like, is it Avalon?

Leo: That's the one that shipped, yeah. Yeah, yeah, yeah.

Steve: And it's a nice-looking unit. But this thing outperforms Avalon's. So if these guys can get it out the door - and, I mean, I'm sure somebody - I'm surprised they're not communicating better. They ought to be better communicators. I saw somewhere that they had 35,000 units on backorder.

Leo: Ohhh. Now, were they taking the money?

Steve: Yes.

Leo: Oh, see. The thing on a preorder to do is to say, we'll get your order, but we won't charge you.

Steve: Yeah, well, they probably needed the money.

Leo: Yeah, they were financing the research.

Steve: To finance the development of this. So my sense is...

Leo: That's what Kickstarter is for.

Steve: Yeah. My sense is these guys are probably real. But they are probably in trouble. I have a feeling that they're not sleeping. I wasn't sleeping either when I was really under the gun.

Leo: Well, that's because you're honest. Who knows whether they're sleeping.

Steve: Yeah, I just - I guess I want to believe that they're okay. I don't have any specific knowledge. But there must - it must be that there have been journalists who have interviewed the executives to get the whole story. So the whole story must be available somewhere, but I don't have it. I just know that, when they get this thing out, if they do, the ASIC approach raises it to the entirely next level of hashing performance.

Leo: But somebody has to design this integrated circuit, and it's nontrivial because it's application specific. I mean, you're building it into the silicon.

Steve: Yeah. It's way, way, way easier today than it was 10 years ago. There's all kinds of engineering support. They can take their designs, and there's automation to create it. And the problem is, when you get your first builds, maybe there's some bugs in the chip. There may be some mistakes that all of the simulations you ran didn't reveal until you actually had it. So I just think they're probably really behind the eight-ball and doing everything that they can to get this thing done.

Leo: Just ask Jeri Ellsworth. She knows how hard it can be. Hey, Steve, the leaf blower brigade has arrived, so I think this would be a good time to wrap things up. Steve Gibson is at GRC.com. That's his website. And that's where you'll find, oh, my gosh, so much stuff. First of all, SpinRite, the world's finest hard drive maintenance and recovery utility, now at Version 6.0. So those Version 3.0 days, they're long gone. And by the way, so is operating system-based hard drive compression, thank god. What Microsoft didn't realize is hard drive capacities were going to increase vastly. You didn't need to compress the hard drive. It was because - they were doing it because there was a commercial program, I'm trying to remember the name of it, that did it. Remember that?

Steve: Theirs was DoubleSpace.

Leo: DoubleSpace.

Steve: And Stac.

Leo: Stac was the big one. And so Stac started doing it, and Microsoft said, oh, we'd better do it. DoubleSpace and Stacker. Stacker.

Steve: Stacker, yup.

Leo: Stacker. Oh, boy. Remember those days. Bad old days. They made drives so unreliable. Anyway, when you get to GRC.com, there's all sorts of free stuff you could check out, including, of course, this show, 16Kb audio and transcriptions available there. We have full bandwidth audio, video as well, at TWiT.tv/sn for Security Now!. And of course if you subscribe you can get those on demand, every time there's a new episode. iTunes and all the other places have it. When you have a question for Steve, don't ask him in email. Send it to - just go to GRC.com/feedback

and fill out the form there. That's the only way you'll get him to respond. And he does it by answering these questions. We have others. Maybe we'll just use it next time. Do you know what you're going to do next week?

Steve: I don't yet. But I'm sure, I mean, there's so much going on...

Leo: No lack.

Steve: ...that I have a whole backlog of things to talk about. But something may come up in the meantime. So we'll just play it by ear. I'm sure we'll have a good podcast.

Leo: We'll talk next week. Every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1800 UTC for GRC and Steve. Thanks, Steve.

Steve: Thanks, Leo.