Listener Feedback #219

Description: Leo and I discuss the week's major security events and discuss questions and comments from listeners of previous episodes. We 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-527.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-527-lq.mp3

SHOW TEASE: Time for Security Now!. Steve Gibson is here. We've got a Q&A episode. We'll talk about the latest security news, including what Lenovo's up to with the ThinkPads now? Oh, no. It's all next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 527, recorded Tuesday, September 29th, 2015: Your questions, Steve's answers, #219.

It's time for Security Now!, the show where we talk about security and privacy and protecting yourself. And although Steve and I might be on different ends of the security spectrum, we both agree, you've got to do it. Steve Gibson's here from GRC.com. I actually have some questions. I know this is a Q&A episode, but I have a question of my own.

Steve Gibson: I know. I've already - you previewed it over on MacBreak Weekly, so that'll be great. We will come to that. So it's a Q&A today. I found a bunch of interesting questions. Few of them, for a change, are about adblocking. There are a couple things have come up that we'll talk about, but this is no longer the adblocking podcast. Everyone can breathe a sigh of relief. And I've got some really cool deep technology stuff lined up for the upcoming weeks. I've had some feedback from people saying, come on, Steve, let's wind up our propellers. It's like, okay. I think it's time.

The news is it is probably time to migrate away from TrueCrypt. We will....

Leo: Ohhh.

Steve: Yeah, we had 16 months since last May of 2015, I'm sorry, 2014, when as was famously reported, something happened. But some problems were found in all of the TrueCrypt forks because they existed in the old code. But of course, since the original TrueCrypt is not being maintained anymore, so they're only being fixed in the forks of TrueCrypt. We will cover what that means. Of course, you know, the press is breathlessly going overboard again, talking about, you know, full system compromise. It's like, well, okay, what does that mean? Well, anyway, we'll describe what that means.

And I have a quick adblocker update. The ThinkPad, sadly, is no longer clean. It no longer stands among Lenovo's products as not having been molested.

Leo: Yeah, I wanted to ask you about that, too, because it didn't strike me as being a horrible...

Steve: No.

Leo: ...privacy violation.

Steve: No, no, no. No, I don't think it is. But it is certainly the case that it's not - we can no longer consider it the exception to the Lenovo rule. They're doing this to, you know, across the board. And some interesting concerns. There was a story about Tavis Ormandy, who we've talked about before. He's with Google's Zero-Day Project to find bugs in software, theirs and others. That AV utilities are often means for malware to get into people's machines. And if you think about it in terms of attack surface, it makes so much sense because the AV utility is trying to be at the gate. It's trying to examine and filter everything coming in and out. Well, that means that it is the attack surface. It is the Internet-facing code that everything has to pass through. Well, if it's not written perfectly, essentially, then it can end up reducing the security of your system rather than, as you would hope, increasing it. So an interesting podcast full of stuff. And then great Q&A from our listeners.

This week's Picture of the Week, it cracks me up every time I look at it. I just - it is - I own both of those books. Those are real O'Reilly texts. And for those who are seeing this...

Leo: I also own them both, by the way.

Steve: Yeah. I just love it. Okay, so on the left is the "JavaScript: The Definitive Guide." And it's about two inches tall. I mean, it's just - it's huge and thick, and it's got little thumb tabs down the side you can see to help you find the right sections because there's just so much there. And then sitting next to it is sort of a companion book that is maybe a quarter-inch thick. I mean, it's just diminutive. But what works so well is the interplay because this book is titled "JavaScript: The Good Parts." And it's like a pamphlet next to the bible. So I just ran into - someone tweeted this to me. Thank you, whoever you were. I just - this just - every time I look at it, it's just - it's just my perfect form of humor. It's just my funny bone.

Leo: I love it. And you will want both, actually.

Steve: Yes. And...

Leo: As Steve and I both own, yeah.

Steve: Yeah. And "JavaScript: The Good Parts" is a really good read.

Leo: It is, it's excellent.

Steve: Yeah. And of course you need the bible for all the syntax details and, okay, how do I do this, you know.

Leo: And to be fair, there's the Good Parts books, that's a whole series for other languages, as well. Many languages can be boiled down to a few good parts. That's why I like LISP. They're all the good parts. Okay, Steve, let's take a look at the tech news here before the questions.

Steve: So, yes. The bad news is, well, I don't know if it's bad news. First of all, it's not an emergency. But my feeling is, after 16 months, it's probably time to gradually migrate away from TrueCrypt. That's how I would put it. I will...

Leo: So there's no incident that makes you feel that way, it's just the length of time.

Steve: Correct. What has happened is that James Forshaw, who is another member of Google's Project Zero team - and of course, as we know, Project Zero is routinely finding vulnerabilities in widely used software. I was just talking about Tavis and how he took a look at AV stuff and immediately found problems that, for example, in this case Kaspersky is in the middle of, like, has already addressed a bunch and is working on more. So he found two vulnerabilities in the kernel driver that was in TrueCrypt, still is in TrueCrypt, and is in both of the two forks of TrueCrypt, VeraCrypt and I can't - the other one's not coming to mind. But VeraCrypt is the one that I'm recommending based on everything I've seen of the French company that has picked it up. These guys are all about security. They've got a public-facing, good-looking persona. There's other stuff they're doing. They look like, you know, good carriers of the torch.

So what's been found is a privilege elevation or escalation defect such that software running in a machine where TrueCrypt is installed, even if there are no drives currently mounted, that is, the TrueCrypt kernel driver is present, software is able to leverage a mistake in the driver code to elevate its privileges. So if that software were in a limited account, it could get admin privileges. Now, you know, we see these all the time. Every month Microsoft is fixing privilege elevation problems, you know, in five or six of the various products they have.

So these are difficult things, difficult problems not to have. But it does - so first of all,

this doesn't mean that your volume can now be unencrypted. This is not a, you know, this doesn't - there's no sort of a decryption attack or a loss of security in any way. But it does mean that, if something malicious were on your machine and knew that you had TrueCrypt installed, it could gain admin privileges. And of course that's not a good thing. So this isn't a hair-on-fire, you know, immediately rip TrueCrypt out of your machines. But it's like, yeah, okay, this is - it's probably time. The VeraCrypt guys fixed their driver. They're at 1.15 is the version they just released a day or two ago. There was pending news of this. I think I knew about it last week, but didn't have any details. So I was biting my tongue until I knew, you know, what this was and could appraise it.

So the press headlines, people have been tweeting me, you know, "Newly Found TrueCrypt Flaw Allows Full System Compromise." It's like, okay, but they don't tell us what that means. Now we know. What it means is that malware could try. And in fact it's foreseeable that in, like, maybe a year from now, malware could check for the TrueCrypt driver as a matter of course in, like, a number of things it does to see where it can gain an advantage. And so anybody who had never moved away from the final version of TrueCrypt would be vulnerable. So I think it's time to do that.

I'm probably going to give this some additional coverage, that is, talk about VeraCrypt when I've had a chance to study it more. I just haven't looked at it closely. It is compatible with the existing file format of TrueCrypt. If your system partition, that is, the main bootable partition was encrypted with TrueCrypt, you must first decrypt it, and then install VeraCrypt, and then reencrypt it. But if you have nonsystem volumes, VeraCrypt is backward compatible with the TrueCrypt volume format, and it's able to upgrade those without you having to first decrypt it and then reencrypt it.

Leo: That's amazing.

Steve: Yeah. So the takeaway is, you know, this is pretty much what we expected is that we got a year and four months where there was a problem no one knew about, not only in TrueCrypt, but that's also always been there in VeraCrypt because they just took the code and cloned it. VeraCrypt is open source. I mean, in many ways it's safer than TrueCrypt was because we've got guys putting their reputation on the line, whereas TrueCrypt's original developers were always sort of clouded in secrecy. No one really knew how to get a hold of them or who they were or what was going on.

Now, it was interesting, in the posting that I saw, the first response to the article was from an old friend of mine, Jeremy Collake. Jeremy is the only person who has any code he wrote on my server. That is...

Leo: Wow. You trust this guy.

Steve: The other way to put that is that, well, actually I should restate that. One of my freeware apps, and I'm blanking on which one it was, it was something that needed some deep voodoo kernel stuff, and I was working - and he and I were of course bonding at the time, I was working on the frontend UI stuff, and I said, hey, you know, "Do you have a chance to do something really quick?" He says, "Oh, yeah." And so he produced the driver which one of the pieces of freeware that I distribute - and I've got his name on the page, wherever that was. It might have - I don't think it was DCOMbobulator. I don't remember what it was. But it was years ago.

Anyway, Jeremy knows his stuff. And so I got a kick out of seeing his name. I hadn't run across it in a couple years. And so I liked what he said. He responded to all this, saying: "At least these are local vulnerabilities - privilege escalation, to be specific. Honestly, I haven't yet decided whether I should trust VeraCrypt over TrueCrypt's last encryption-enabled release." And he phrased it that way because he's a really top-end developer, and he's careful with his phraseology, and he was intending to note that the very last release they had disabled encryption. It was only for decryption, in order to leave TrueCrypt, which is what they were trying to push everyone to do.

So anyway, he says: "I haven't yet decided whether I should trust VeraCrypt over TrueCrypt's last encryption-enabled release. It's a tough call. Why was TrueCrypt really abandoned in the way it was? We may never know. We don't really know who its primary contributors were. Now VeraCrypt is here. Do we trust them, and it? If we trust by default, then they've given us no reason not to trust them. In contrast, if we are skeptical by default, they've not had enough time to earn our trust." Which, you know, I just liked the way of looking at that.

So that's the story. This is not the end of the world. TrueCrypt is fine. Your volumes are secure. But we could anticipate that future malware could add exploiting this original TrueCrypt driver privilege escalation to its own toolkit of things to try. And so, you know, when you have a chance, maybe over the weekend, I would say new installs, go with VeraCrypt. I do like everything about the company, the way they feel looking at them, everything is up, posted on CodePlex, GitHub, and SourceForge. I mean, so all the code is there. It's all visible.

And notice, there were some comments that, ooh, this sneaked through the audit. And it's like, well, yes, because that wasn't what the audit was auditing. We always knew that this was a cryptographic integrity audit. And what this happened to be was a very subtle mistake made in the kernel driver in the handling of drive letters. And I didn't burrow into it any further because there was really no point. You know, bad is all we really need to know. And, you know, but not life threatening. So...

Leo: That's the difference between actively supported software and software that is left out on the vine.

Steve: Yeah.

Leo: I mean, there's always going to be stuff you want to get updated.

Steve: Right. And that's also why my original statement back in May of 2014 is that, okay, there's no hurry to run away from it.

Leo: Right.

Steve: Because it was supported yesterday, and today it's not. That doesn't mean that it suddenly went evil. It just...

Leo: Just means at some point it's going to superannuate. But for now it's okay.

Steve: Precisely.

Leo: Yeah.

Steve: And so, if people have already migrated to VeraCrypt, that's the direction I would recommend. And I think now there's more reason to do that. Again, your data is not in danger of decryption, even from this. This just gives malware a way of obtaining admin privileges. And we know that gives it more opportunity to do bad stuff. So it just sort of - this is a common mistake, apparently. I read that really good kernel driver authors could read this, as in fact the Google guy did, and spot it.

So the other question is, you know, who else may have known about this for the last 18 months or longer, however long that particular mistake has been in the kernel driver. Again, switching to VeraCrypt last May wouldn't have helped you because it wasn't until this came to light that we could fix the driver. And as you say, Leo, only their driver is going to get fixed, not the old driver, which now is becoming a little long in the tooth, and it's probably time to move on.

Leo: By the way, you'll be happy to know Microsoft promises that Windows 10 does not violate your privacy.

Steve: I'm so - that makes me feel so much better. You know? I'm so glad.

Leo: They promise.

Steve: That's great.

Leo: Cross our hearts and hope to die promise.

Steve: That's great.

Leo: They say the telemetry data they collect is just to deliver a delightful and personalized Windows experience.

Steve: That's good. Well, Lenovo is actually sending it to a web marketing company, so...

Leo: We'll talk about that in a second.

Steve: Yeah, that's a little bit different.

Leo: That's a little different.

Steve: So speaking of questionable, Dean Murphy, who is the author of Crystal, which was until recently the number one content filter on the iTunes App Store...

Leo: And the one I used until you told me better.

Steve: Right. He made the decision, which many people are calling controversial. I just think it's a choice. And I wanted to make sure people knew. He decided to adopt the, as we call them, the EIEIO acceptable ads deal with Eyeo, E-Y-E-O, which are the - those are the publishers behind Adblock and Adblock Plus. And as we know, somewhat controversially, Adblock Plus allows advertisers to pay them to allow their ads through, but under this acceptable ads idea.

So this is of course, depending upon where you're standing, and there are many different places you could be standing, this is either extortion, or a way of supporting the ad, or a way of allowing people to sort of softly, like, block the bad ads, but allow the good ones in, where somebody else is deciding what "good" is. And of course the for-fee, that's controversial, too. But for what it's worth, Dean Murphy will be receiving a flat monthly fee in return for the default being, when he updates Crystal, he hasn't yet, the default will be to allow the acceptable ads through.

Leo: He does put a switch in. He says he's going to put a switch in that lets you turn it off.

Steve: Yes, yes.

Leo: And I believe him when he says, like Marco, he kind of felt bad.

Steve: Yes.

Leo: He didn't really want to block all ads. He didn't want to undermine the good stuff, the good sites that use respectful ads.

Steve: Yes.

Leo: Now, I haven't seen this acceptable ads list, so I don't know. I know Google and Microsoft both are on it.

Steve: Yeah. In an interview with or a story he did with The Wall Street Journal, he write: "Given how popular Crystal has become, it doesn't provide any way for users to

support publishers."

Leo: Right.

Steve: "I decided that's a good feature to provide, and from what I've seen the 'acceptable ads' policy doesn't let through what I would classify as bad ads."

Leo: Yeah. Wouldn't that be, you know, if it just said no Flash, I mean, no takeovers.

Steve: Right. And the Eyeo guys - I guess you're supposed to pronounce it Eyeo as if it was IO. But they made it E-Y-E-O. So they're saying that the reason they charge advertisers is that a human is involved in screening the ads that they allow through and that that's a labor-intensive...

Leo: Have to pay somebody, that make sense.

Steve: ...job that they have to support. And so of course there are dissenting opinions. Matt Buchanan, writing for The Awl website, said, "If your adblocker takes money from you in order to block ads, and then takes money from huge companies in order to show you the ads that you paid it to block, then yes, it's just using you to erect a tollbooth."

Leo: Right.

Steve: So anyway, I got a kick out of that. But I'm with you, Leo. I like this as a nice compromise. Now, what's interesting is that the...

Leo: You can always turn it off if you don't like it; right?

Steve: Of course, of course.

Leo: If you're seeing a lot of crap ads, say no, no, just block it all.

Steve: Yup, you know, it's like, hey, I'm glad I gave this a shot, the acceptable ads.

Leo: Right, right.

Steve: But it's not working for me. And then you flip that off.

Leo: And do other things. I took your lead, and I put 10 bucks a month into Google Contributor.

Steve: Yup.

Leo: That makes me feel better about blocking ads.

Steve: Yup, exactly.

Leo: Yeah.

Steve: Exactly. So on the other hand, now to go far out, we have Randall Rothenberg, the president and CEO of the Interactive Advertising Bureau, which is the trade association for so-called "interactive marketing" in the U.S.

Leo: I met Randall. He was at the event that we spoke at in New York a couple weeks ago.

Steve: Oh, cool.

Leo: We are not, by the way, members of the IAB. I should just tell you. But most of our agencies that sell ads on TWiT are. That's, I mean, has to be.

Steve: Yeah, yeah, exactly. I mean, that's what you do. So they're holding a press conference today about adblocking. And I'm just - our listeners should know that this interests me sort of from a drama meets technology meets the Internet standpoint, which is why I've dragged us through the last, you know, this topic for the last four or five weeks, because this is just a lot of interesting forces that are pulling in different directions with a core of technology. It's going to be interesting to see because they're talking about, you know, getting around this problem.

Anyway, he posted in response to all this, at the AdAge.com site. His title was "The Ad Industry Needs to Disrupt the Disruptors." And there are just two points that he makes, one which was, ooh, a little hot, and then which I thought was interesting for them to acknowledge. So I'm just going to read the first two paragraphs of this.

So he writes: "The digital marketing and media industry regularly confronts fresh adversaries eager to" - now, remember who this is, so keep that in context - "regularly confronts fresh adversaries eager to intercept the flow of ad dollars, often to the disadvantage of consumer choice. Adblocking is the latest crisis du jour, a potentially existential threat to the industry. To combat it effectively, it's essential to distinguish adblocking's two sources and their significance."

Okay, so here's the first one: "As abetted by for-profit technology companies..."

Leo: Oh, come on.

Steve: I know, "...adblocking is robbery, plain and simple."

Leo: Wow.

Steve: "An extortionist scheme that exploits consumer disaffection and risks distorting the economics of democratic capitalism." Now, what's interesting...

Leo: Oh, Randall, come on, now. You've got to - oh.

Steve: I know.

Leo: You've got to respect users, too. You can't...

Steve: Well, and so that's what's so interesting is that was the first sentence. Then he completely switches gears and says: "When implemented by consumers, adblocking is a crucial wakeup call to brands and all that serve them about their abuse of consumers' goodwill."

Leo: Oh, right. That's correct.

Steve: So what he's really saying is anyone who profits from blocking ads is the spawn of the devil.

Leo: Yeah. We all have to hand code our own adblockers. That's clearly the message there.

Steve: Whoa, yeah, it's like I hope he's taking some phosphatidylserine for his stress...

Leo: His dementia.

Steve: Boy.

Leo: You know, and I understand, and I've said before it's like stealing a candy bar from a shop. But I maybe have moderated that quite a bit, given that it's an abusive shop owner. You know, there's a certain amount of, you know, there's got to be a balance here somewhere.

Steve: Yes, and you could get yourself infected, and it's truly...

Leo: Right.

Steve: And it truly destroys the experience that you're trying to have of browsing the web. And there's the tracking side, too, this idea of the databases somewhere being compiled that makes people uncomfortable.

Leo: No, when you see the difference, when you start running an adblocker, and you realize how much sewage is pumped into your browser and how much of it's blocked, then you start to say, you know, you guys have pushed it a little too far here.

Steve: Okay, I have to take us completely out of sequence. Put into bit.ly today's link. It's bit.ly/sn527, no hyphen this time, sn527. And you need to put this...

Leo: Well, wait a minute, I'm running an adblocker.

Steve: I know. This is from number 10. This is the site that bypasses - even uBlock Origin can't...

Leo: I'm running uBlock with everything turned on, and, man, I'm still - holy...

Steve: The chicken walking back and forth in front of the...

Leo: The funniest thing is this isn't a content site. This is a rental car site, LingsCars.com.

Steve: Yeah.

Leo: They must make more money on the ads than they do on renting cars.

Steve: Oh, it's just - this is the first page I've seen that has made me feel good about my site.

Leo: But I have to tell you, most radio station sites are this bad. And really, always when I talk to radio stations, I say, why are your - what do you - do you not make enough money? What's going on here? This is just a horrific site.

Steve: It's just wonderful. Oh, and when you view source, it's even better. I didn't pick up on that, but I tweeted this last night, and a bunch of people said, oh, Steve, you've

got to do a view source on the page. And I thought, what, is it going to have some strange HTML? No, it's even better than that.

Leo: It's taking forever to load, so I know there's a lot in here.

Steve: It's probably...

Leo: Everybody else.

Steve: ...that we're live. If you scroll - oh, you should have seen something at the top, unless he already took it out.

Leo: Oh, yeah, look. There was - there's something that was deleted here. Oh, wait a minute, here it comes. No, no, no, no. There was something deleted. See, that's the comment block.

Steve: Of course. But he had a big block of ASCII art which was basically an ASCII version of his head, his face, and something like, in huge letters, you know, if you mess with this site's code, I'm going to get you or something like that.

Leo: I like this guy.

Steve: I know.

Leo: This is the best site I've ever seen.

Steve: It's wonderful.

Leo: LingsCars.com.

Steve: Oh, goodness.

Leo: I like this site. He's got a chicken browsing - there's a chicken browsing his Twitter feed for no apparent reason.

Steve: Oh, oh.

Leo: Just wandering around.

Steve: It almost falls off the ledge there.

Leo: I know.

Steve: And catches its balance again.

Leo: He put a lot of effort into this.

Steve: Oh, and the breathing Mercedes. There's a throbbing Mercedes grill to the left. Oh.

Leo: I've never seen so many blinking items. You wouldn't go - please, don't go here if you're epileptic. This will put you into shock. Wow. He does lease some pretty nice cars, though. That chicken, I've got to get that chicken for my site.

Steve: It's great.

Leo: Wow.

Steve: Have it kind of wandering around.

Leo: Oh, look, you've been mentioned. You're being retweeted in the Twitter feed.

Steve: Oh, no.

Leo: The chicken's pecking - wait a minute. What the...

Steve: Is it sensitive to your cursor?

Leo: Yes. There's a popover here. Wow.

Steve: Too funny.

Leo: Twenty thousand pounds gross profit, says Mr. Ling. I think this is the nicest site I've ever seen.

Steve: I know.

Leo: I am a fan.

Steve: He has clearly just poured his heart and soul into this thing. Yeah, and then...

Leo: [Crosstalk] we used to do; right? These are the...

Steve: And the listings go on and on and on. It's like, wow. But you're right, it is, doesn't it feel like a throwback?

Leo: Yeah.

Steve: It's a blast from the past. It's...

Leo: Well, look at the wallpaper.

Steve: Oh, we've got a car bouncing over there on the left.

Leo: Oh, whoa. A lot of JavaScript. Lot of JavaScript here. Wow. But, you know, given that it's getting around uBlock, it must be all...

Steve: He's sourcing all the images himself.

Leo: First person, yeah.

Steve: They're all coming from - and in fact, if you look, if you have uBlock expert mode turned on, you look, and there's nothing for it to block. It's all coming from his content.

Leo: Well, then it's all his - there's no tracking going on, believe it or not.

Steve: Right.

Leo: Wow. This is great.

Steve: And the background, the background behind all of that, you know, the wacky paisley explosion thing, oh, it's just - he didn't miss a thing.

Leo: There he is at the bottom. "You can trust me. I am Ling. Hope you're enjoying

your visit to LingsCars.com."

Steve: Oh, I never - I never got to the bottom. That's just wonderful.

Leo: He must - this is tongue-in-cheek. This is tongue-in-cheek. That's hysterical.

Steve: Oh, god.

Leo: Thank you for sharing that with us. That is a...

Steve: Well, I ruined the last question. But...

Leo: Okay. That's okay.

Steve: But anyway, it was perfect, so, oh. So adblockers. Five of the top 10 apps in iTunes for the first week were adblockers. And I think it was Crystal that was in the number one position. Things have changed. We're now two weeks minus one day down from the Wednesday two weeks ago when we got iOS9. Our chosen no-brainer adblocker is holding at number three. That's Purify. That's the one that we recommended last week.

Leo: Oh, I thought you rec- oh, I'm sorry, I didn't mean to pop Ling up. I thought you recommended 1Blocker.

Steve: Well, for the experts.

Leo: Oh, for the experts.

Steve: So 1Blocker is the power user tool, and Purify is the "set it and forget it" because it has a feature that Crystal didn't have, which was a simple whitelist. We can presume, and in fact, I didn't have it in my show notes, but lots of sites are beginning, I think the Washington Post is become infamous for being one of the early adblocker detector sites. And I think it either admonishes you, or you have to give it your email address in order to read articles because it sees that you have an adblocker in place. So as we expected, this is the first round of responses. And I think it's entirely their right to say, oh, you're blocking ads. We need you to lower your shields because this is how we pay for our content. And then you decide. Or you can give them your email address as another way of opening the spam portal.

So I think it makes absolute sense. But what you want then is an easy way of whitelisting sites that you decide you want to support, who bring it to your attention that that would be something nice. And Purify does that. It's holding at number three, and Crystal is at 21 right now. The others, there was Blockr, B-L-O-C-K-R. It's nowhere in the top 150,

although it was near the top two weeks ago, or for like the first week.

And then ours, 1Blocker, the one we recommend, which is also the performance winner, remember, of all the ones, there are 15 of them that Lifehacker benchmarked. And 1Blocker was not only the most bells and whistles and deep level of control, where for example you could actually see the rules that were being blocked and individually turn them off, so you could tune the list for specific needs, if you wish to. You would expect it's not for the masses, it's for listeners of the podcast. So that's where the industry is; you know? They're no longer in the top. They spent a week up in the top five of the top 10. Now people have them, and it's calmed down as iOS9 is becoming something that everybody has.

So it was a listener of ours who is also a columnist for Computerworld. Michael, this is a shout-out, Michael Horowitz is Computerworld's Defensive Computing columnist. He sends me stuff from time to time via Twitter. And I got a kick out of going - in following the story and backtracking, I came to his column, which he wrote last week. And Michael wrote: "On a recent edition of the Security Now! podcast, Steve Gibson read a note from a listener saying that, while Lenovo was corrupting their consumer PCs, [Lenovo] have kept their hands off the ThinkPad line. Both Gibson and the show host, Leo Laporte, proceeded to sing the praises of ThinkPads. But there's more to the story."

Leo: Uh-oh.

Steve: And Michael writes that he had recently purchased two newly refurbished ThinkPads from IBM, a T520 and a T420. And just because it's who he is, I mean, he's writing the Defensive Computing column for Computerworld, so he's a security-focused guy. So he ran Nirsoft's very nice TaskSchedulerView utility, N-I-R-S-O-F-T. It is another site of really great homegrown, just a variety of neat little utilities to do useful things. I used them when a restaurant I was frequenting secretly put in their WiFi password because they didn't want me to know it, but they were willing to enter it. And Windows won't allow you to get what was entered, but NirSoft has a utility that will give you the hex version, which Windows has. And as we remember from our coverage of WiFi years ago, you can always put the hex version of the password in, and it will be accepted, in addition to the ASCII version. And so that way I was able to obtain the password that the manager of the restaurant had entered secretly into one laptop, and I was able to move it to another. So actually I think I moved it over to my iPad. And then of course it went to the iCloud, and now everybody has it. I mean, all of my...

Leo: Everybody.

Steve: All of my devices have it. So the takeaway is that ThinkPad is not being held in some special, you know, from IBM or off limits or executive level or special sanitized, we're not putting any spyware, using the term loosely, in that particular brand. It's there with the rest. And in fact Lenovo has a support document on their site, I have a link in the show notes, where they say, right in big bold type, just like Ling is using on his site, "Lenovo systems may include software components that communicate with servers on the Internet - all ThinkCentre, all ThinkStation, all ThinkPad." So, and then they explain, later on down the page, that on Think brand products, Lenovo collects two types of data: application usage data, or metrics, and preloaded application inventory data.

So, now, the only downside is that - and Michael's column covers this in more depth for

anyone who's interested - is that the domain that this stuff is going to is not Lenovo. So their software that they install is sending this off to a third party for that third party's processing. Maybe they're a subcontractor of Lenovo or who knows. But they are a well-known web aggregator company of some sort. So it might be that Lenovo is actually generating revenue from sending this stuff off.

And of course then there are, in these links that I have, if anyone's curious, both in the Lenovo link and in Michael's, lots of advice for finding this stuff, turning it off, removing it from the, like, de-installing it and removing its autostart-ness. And there was some mention of within 90 days it will delete itself, if it sees it's no longer running. But apparently you can do that, too. So that's the story. I just wanted to close this up and, unfortunately, remove the ThinkPads as being separate. And Michael, thank you for the great find and discovery. I got a lot of tweets from people who were reading your column and wanted to make sure I knew about it.

Okay. So Tavis Ormandy, who is, we've spoken of often, a member of Google's Project Zero vulnerability research team. He recently analyzed Kaspersky's AV and quickly found what has been described as a "raft," I think the raft means a bunch, of easy-to-exploit, as he characterized them, bugs that made it possible to remotely execute malicious code on the underlying computers. Now, that's as bad as it gets. I mean, if we were talking about Windows having remotely executable malicious code on underlying computers, everyone, I mean, it would just be the end of the world. We'd be going crazy. But so this is Kaspersky's AV where this was just found, just recently. And to be fair, FireEye's products, Sophos's, and Eset's were all also looked at, and all also had problems.

So what Tavis wrote is: "We have strong evidence" - this is Tavis of Google, so, you know, they have data collection capability. "We have strong evidence that an active black market trade in antivirus exploits exists," he wrote, referring to recent revelations that hacked exploit seller Hacking Team - remember them? This is the folks that lost gigabytes of their database, and it turns out they had all of this previously unknown zero-day exploits that they knew about, a bunch of Flash stuff. And apparently in here were exploits against a broad spectrum of antivirus utilities. They were selling - so the Hacking Team were selling weaponized attacks targeting antivirus software from Eset.

So Tavis continued: "Research shows" - and this is from his blog posting last week. "Research shows that security and AV is an easily accessible attack surface that dramatically increases exposure to targeted attacks. For this reason, the vendors of security products have a responsibility to uphold the highest secure development standards possible to minimize the potential for harm caused by their software. Ignoring the question of effectiveness, attempting to reduce one's exposure to opportunistic malware should not result in an increased exposure to targeted attacks."

So this really, you know, you and I, Leo, know that we're not running third-party AV. We just don't. We understand the risks. We have all kinds of other things we do, like we're not accepting every ad that sites want to give us. For the longest time I was running NoScript. We've talked about Sandboxie and running browsers in VMs, I mean, there's lots - and making sure that your browser is running as a limited user and not with admin privileges, and on and on and on. So but for the person who doesn't understand that, maybe it makes more sense.

But as I said at the top of the show, teasing this further discussion of this, when you stop to realize, it's like, well, of course the AV has to be perfect because its job is to examine every file that you download and to, in many cases, filter your Internet connection. And as we know, unfortunately, many of them do that by installing a root certificate in your system, which nobody likes, because then they are minting - they're basically creating

forged remote certificates to make your browser happy in order that they're able to peek inside your TLS connections for the purpose of scanning that.

So the point is there is no - there could not be, by definition, a larger attack surface. They are looking at every file you download and your Internet connection, which is the way all this stuff comes to you, whether email or web browsing or what. So how many times have we talked about, like, subtle parsing errors in JPEGs where viewing a JPEG allows a remote code execution exploit in your machine. These exist in today's AV tools because it is nearly impossibly hard for them not to exist. And we know the amount of effort that Microsoft must go through not to have these problems. Yet we get monthly updates fixing these problems constantly.

And so this is an aspect of the third-party antivirus utility that hasn't had a light shined on it. And this is a big problem because, as Tavis says, in the Hacking Team dump was weaponized attacks on Eset being sold. Meaning that, if you had installed the Eset AV, they were selling attacks to allow remote compromise of your machine of that software. So a machine without that installed wouldn't have responded, but one with it installed would. And Kaspersky is still fixing these problems. They've fixed a bunch. But a raft, I mean, like, it was a field day of a very good, well-known, popular antivirus. So, yikes. And but again, with everything we know, and we've learned from this podcast, yeah, duh, this is going to be an issue because it's the definition of attack surface. You've turned your entire connection into an attack surface.

Leo: Sometimes security makes things worse, not better. Which brings me my question.

Steve: Ah.

Leo: So I noticed, setting up this new iPhone, that Apple is very security conscious. I had to enter my password, my iCloud password, five times because I was starting from scratch. I wasn't restoring.

Steve: Right.

Leo: And it struck me as I'm going, you know, hey, we love how secure Apple is and how serious they are about security. But I have, thanks to you, a 25-character, very random, LastPass-generated iCloud password that's a real pain in the butt to enter.

Steve: Good. And, yes, it is.

Leo: And five times is an awful lot. And I don't have it memorized. I had to every - I went, "Not again."

Steve: You're not supposed to be able to memorize the password.

Leo: Not again. So I have to fire up LastPass, show password, okay, type it in. And of course Apple hides it with dots. So if I miss, if I make a mistake, there's no way to look at it and correct it. I've got to do it all over again. It was a major pain in the butt. Now, I understand Apple wants to be secure. I can think of, you know, I'm not sure how much that helps my security, frankly. I mean, they've got a secure store. They've got my fingerprint. Making me reenter that password. In fact, it struck me that there is a negative impact to doing this on security. First of all, I'm incented not to have a strong password.

Steve: Precisely the problem.

Leo: Strongly incented. But second of all, each time I'm doing this it's sending it. Somebody could see it over my shoulder. Every time I enter the password I'm adding a little risk to the whole process. And they already have it secured it by my fingerprint. So I'm - and by the way, Apple continues to do this every once in a while with iTunes. It wants you to re- you know, you turned the phone off, we'd better re-enter the password. Google does not do this on Android.

Now, I understand that, when you choose Apple, you're choosing security. That's one of the things. And so to say, well, Android doesn't do this is to say exactly what Apple wants you to say, which is I'm more secure on Apple. But I wish there were some way to say to Apple, look, I'm not that paranoid. I'm careful, so I don't put stuff on my phone that's, I mean, admittedly, my credit cards are on there, so maybe there is some stuff on there. But what I'm saying is there should be a way to say to Apple, tone it down a little.

Steve: What I believe is that, in every instance, there was a provable need to ask.

Leo: To reenter it, okay.

Steve: Yes. And that's, I mean, and unfortunately, well, so first of all, the good news is I'm - I don't have it within reach. But I'm staying with my 6 because, as I heard, I think it was Patrick say on Sunday that, you know, his 6 is still brand new, the one from - just the 6 Plus, not the "s." And that's how I feel, too. I'm not getting on the annual - although I've been fascinated by listening to you talk about it, and I am drooling...

Leo: It's pretty impressive.

Steve: ...drooling over the technology. So we'll see. Maybe in a couple of months I'll buckle, and I'll go with just the gold, which is the one I have, although no one could tell because it's in a case.

Leo: Right.

Steve: But I just like that. For example, one of the tricky exploits is the hardware

intrusion power cycle exploit, where you make a guess, and you intercept the recording of the guess in nonvolatile memory so that it doesn't count against you. You immediately short out the power, and then you bring it back up again. So, for example, the only real way to prevent that is that a reboot of the OS or a coming up from power off, which means rebooting the OS, has to ask you once.

Leo: Right.

Steve: If they don't, then you really are vulnerable.

Leo: That makes sense. And, yeah, and so I do know that that's what happens if you turn off the iPhone. You'll have to reenter your code.

Steve: And the point I was going to make was that, for what it's worth, I think this was just initial setup frenzy because on an ongoing basis it's really not something that you encounter. And I did hear the MacBreak Weekly guy saying the same thing, essentially, well, okay, but, you know, that doesn't seem to be a problem for us.

Leo: Well, and I talked - every time I mention this, a lot of people say, yeah, that drives me crazy, too.

Steve: Yeah.

Leo: So I don't think it's unusual. I think, you know, if you restore from your encrypted backup you don't have to do it, probably. But I wanted a fresh install. So I guess, you know, I don't know, I can't look at it and say, oh yeah, there's a good reason why it asked me at this juncture.

Steve: Yeah. I would bet, I mean, knowing Apple, they're not going to inconvenience people without a reason. And they are a highly attacked platform. So, and they really do focus on this. By the way, they just posted the iOS9 security update document. And so I will digest it, and we'll talk about it, the things that have happened to iOS. So, but anyway, I feel what you're saying, and I have the same problem.

Leo: Well, for instance, LastPass is - I've set up LastPass to ask for my password a lot. I understand why I would want to do that. But as a result, I have to memorize my password. It can't be a truly good random password.

Steve: And with the fingerprint reader that we know you have fallen in love with as much as I have...

Leo: Yeah, love that, right.

Steve: You would think that it would be enough, that you would say, look, this is really me. So, you know, let me just use the fingerprint reader to bypass this over and over and over.

Leo: Actually, to be fair, Windows does this, to a lesser degree, but Windows does this, as well. It does ask for your Microsoft account more than I would like.

Steve: Well, and even SQRL, because I don't have biometrics necessarily on a Windows machine, as I've talked about, I do reprompt for the first "n" characters of your password. You can change "n" to "1," if you want, so that's just a matter of hitting the proper key. But if you press the wrong key, then it'll say, oh, that was a wrong guess. Give me the whole password.

Leo: Right. So you need to revalidate, yeah.

Steve: And the reason is I don't know that you haven't walked away, and SQRL is empowered to represent you to the Internet. So we just have to have some way of reauthenticating who you are. And, I mean, as Rene quoted me, saying, "There just isn't a way around the tradeoff between security and convenience."

I have a wonderful fun story. This is not quite as good as the - was it a SEAL team in Afghanistan who used SpinRite? They were absorbing bullets with a Panasonic Tough Book or something years ago.

Leo: I remember that, yeah.

Steve: Anyway, this person explicitly withheld his name. And the subject is "How SpinRite Saved the Plane."

Leo: Hmm.

Steve: So he said, "Dear Mr. Steve. Please note that some details in this story have been changed to protect my identity, which is quite important as you'll soon see. I'm a senior IT director at an airline that shall remain unnamed, but I did not land" - so to speak - "this role overnight. I worked my way up, all the way from tech support. Naturally, I still have the gift of geek in me and always carry around several USB drives and some mini CDs" - he said in parens the 8cm ones - "full of Linux distros and troubleshooting tools.

"On a recent international flight, just before takeoff, I noticed that the crew were having trouble with the IFE, the in-flight entertainment system. Every time the media library was loaded, it stopped, and the system rebooted." We all know where this is going. "After a couple of tries they disabled output to the passenger screens, but I knew they were having some hard disk trouble.

"I deliberated about what to do because, even as IT director, I cannot touch the IFE without authorization. Access is highly restricted, and only senior technicians on the ground have root access. The crew can only use the built-in troubleshooting tools. But

after the seat-belt signs turned off, I promptly introduced myself to the co-pilot, who was taking a stroll through the plane, showed him my ID and badge, and offered to help. He was surprised and said he'd contact ground and get back to me. So I waited. Ten minutes later I got a note from the captain authorizing me to try and fix the IFE."

Then he asked me to snip out some stuff that was not for public disclosure, so I have, but it involved the security details surrounding access to that device. So he says, "I popped in my SpinRite bootable USB," and he says in parens "(corporate license). And since we were in a rush, with the passengers getting grumpy, I only did a quick scan on Level 2. At about 11%, SpinRite found and fixed quite a few sectors of the media drive; and, when it got to 30%, cruising along with no additional errors being found, I decided to stop it and try my luck.

"There was a jubilant outcry when the FML" - which is the flight media library - "loaded without a hitch; and, to the passengers' and my delight, we could continue to enjoy the flight, of which we still had nine hours. So allow me to express my sincerest thanks for you and your marvelous product. You shall be blessed a hundredfold and live long and prosper. Name withheld due to possible breach of protocol."

Leo: Wow.

Steve: So thank you very much. And that's neat. A site license is 10 purchases of SpinRite. I've talked about the - I'm sorry, not the site license, the corporate. The site license, if you buy four copies, you can use them on all of the systems forever at a physical location. So if, for example, a company had two locations, then to be fully licensed they would buy eight copies, four for one location, four for another. But I didn't want to continue that endlessly because companies like IBM - and IBM, for example, is a corporate license holder of SpinRite, as are many other Fortune 500 companies with offices all over. The corporate license is 10. So if a company purchases 10, they can use them anywhere, anytime, forever, on all of their machines. And so this unnamed airline has bought 10 copies, so they were able to fix their in-flight entertainment system.

Leo: I think I was on that flight, but I won't say any names. You do sometimes see that. They'll restart. And almost always they're Linux machines. So you actually get to watch little Tux penguin, and the thing scrolls up, and you can tell they're having trouble because they reboot it three or four times.

Steve: Well, and it's a hostile environment. And the heads may have been - it sounds like there was, like, one physical region...

Leo: That's all it takes.

Steve: ...where there had been some trouble, and SpinRite was able just to, you know, basically replow that land on the drive and get everything going again.

Leo: We're going Ling crazy, by the way, in the chatroom and on Twitter.

Steve: What's happening?

Leo: Well, there's apparently - turns out Ling is a lady. Lily Ling is her name.

Steve: No kidding.

Leo: Here she is.

LING: So you will hear this Chinese National Anthem...

Leo: She's wearing a helmet.

LING: ...[indiscernible] all the time.

Leo: She's giving a keynote address at the Future of Digital Marketing. She obviously...

Steve: She is just wonderful, isn't she.

Leo: ...is kind of aware of - and she's smart. There's a lot of good code on there.

LING: [Chinese]...

Leo: And I love it that she's wearing a safety vest and a helmet.

LING: [Chinese]...

Steve: And something about rocket bang bang.

Leo: Rocket bang bang, a missile. I don't know what's going on.

LING: I got my bachelor's degree in Guangzhou in environment...

Leo: So she's actually quite something. Well, I'll put a link somewhere. Thank you, chatroom. She's a chemist. She's got a degree in applied chemistry.

Steve: Wow.

Leo: So she's obviously super smart. And I love it that none of that stuff is blocked by uBlock.

Steve: Yup, it just cuts right through all of our adblockers.

Leo: It replaces Zombo.com as my favorite website.

Steve: It is, it's just so over the top.

Leo: I love it. Thank you, Mrs. Ling. All right, Steve. Questions are ready. They're fired up. I've got them ready for you, if you've got some answers.

Steve: You betcha.

Leo: Let's dig right in here.

Steve: Our illustrious viewers.

Leo: And they are illustrious. And mighty fine-looking, as well. Question 1 comes from George Hartmann, but it's a tweet. But I don't know how you did this, Steve, because it's a really long tweet.

Steve: That's probably a DM because DMs are...

Leo: Probably a DM.

Steve: Yup.

Leo: Yeah. He says: Hi, Steve. Newly minted and big fan of Security Now!. Because I'm only at the beginning of my foray into infosec and privacy practices, I was wondering, can you explain the value, or lack thereof, in using a browser-based VPN like Hola versus a VPN that installs a client like Private Tunnel - which, by the way, I used while I was behind the Great Firewall in China. Thanks, and hope all is well. George.

Steve: So Hola is an interesting concept. I would describe it as a peer-to-peer VPN. So in the same way that BitTorrent creates a network of machines that are linked over the Internet, Hola is a browser add-on that is available for a whole bunch of different browsers. I don't think IE. For IE I think you need to install a Windows client. But I know Opera and Chrome, I think Firefox, and others. And so the idea is that you join, sort of in the same peer-to-peer networking spirit, you join this Hola VPN network, and sort of like,

sort of reminiscent of - I can't believe I'm blanking on this. Tor.

Leo: I was going to say Tor, yeah.

Steve: Yeah, sort of reminiscent of Tor, although with not making any of its privacy guarantees. Your traffic will be encrypted and sent to somebody else's system, where it is decrypted and then put out onto the Internet. So, okay. Think about what that means. So there's some good, and there's some bad. The controversial thing about an old-school VPN, where you have a central server, is that everybody who's connecting to it has their traffic being decrypted there and emitted from that point. So it's like, you know, a fire hose.

So what the NSA knows, for what good it does them, but I'm sure it's on their radar, they know that there's a VPN server. And for some reason everybody who's using it has encrypted their traffic up until it gets there, and then this massive flood is coming out at that location. On the other hand, you can choose what that location is for high-end good commercial VPN providers, so you could have your stuff come out of whatever country that you want, so you look to the Internet like you are there with one of those IPs, typically. So there's a benefit of just being lost in the noise. And because, you know, your traffic isn't necessarily identified as you. It's just it's coming out, you're a little droplet amid this fire hose. The alternative is a fully distributed peer-to-peer VPN network.

Now, there's a couple problems. Oh, and I should also mention that we're pretty sure that the VPN provider has no interest whatsoever in any of this traffic. That is, first of all, it literally is a fire hose. I mean, it's almost daunting in its volume. And, you know, their business is not to care. And in fact we've talked about how proXPN explicitly no longer even logs their customers' connections to their servers.

You can't know that, though, if you're in a peer-to-peer VPN environment. You could very well have someone join the Hola VPN network specifically to spy on other Hola users because what's going to happen is somebody's encrypted traffic is going to come into their machine and get decrypted in their machine and go out unencrypted from their router. So all you do is fire up Wireshark and capture it. And anything that they're doing which is not independently HTTPS tunneled will be in the clear and visible to that person who is peering on the network.

So the advantage is your traffic is not coming from a known major VPN termination server. It is diffuse throughout this network. On the other hand, it seems to me way more - I would be a little nervous about, you know, whose peering node my traffic is being decrypted in. And, if nothing else, you want to be sure that you're providing your own encryption through HTTPS. But on the other hand, then the only advantage you're getting, since the VPN is giving you encryption, is changing your IP around. So anyway, I think, George, those are the tradeoffs. They're completely different architectures in each one due to the difference in the way it handles traffic, and sort of just the structure sort of has a different set of tradeoffs.

Leo: Question 2 from Seattle, Don Wood. He says we don't talk about steganography. I was talking about it on the radio show the other day: In light of the recent attempts to cripple encryption in the U.K., India, and even by our own FBI director, please consider a propeller-head episode on steganography. Include, if you would, the limitations in some algorithms demonstrated in academia to reveal the

presence of the hidden message, along with how they do that. Finally, perhaps, any open source software or algorithms that seem resistant to these attacks. It might take a propeller-head episode to cover adequately, but considering all the governmental efforts to outlaw encryption, flying under the radar may be the best course of action. Big fan of yours since the InfoWorld days, with my first site license for SpinRite 25 years ago. Don in Seattle.

Steve: Okay. So we have never discussed it. And I guess it's because - I guess I should have. But I've never been that captivated by it. So for those who don't know, steganography is the practice of hiding something in plain sight. You can kind of phrase it that way, the idea being - so here's my best example. You take a full-color, 24-bit photo. And it would have to be in raw mode for this to work, but I'll just give you this example. So you have a byte of R, a byte of G, and a byte of B - RGB - and eight bits of each color, so 24-bit color total.

Now, the way the bytes work, as we know, the byte contains a binary luminosity or intensity value for that color per pixel. The least significant bit is probably noise in the picture. It probably has no actual information value. It's just going to be - it just could be digitization noise, converting the incoming luminosity lux into a binary number. The fact is analog-to-digital converters are noisy. Down in the least significant bits they can be kind of random. The point is that that last bit in the byte contains nothing of visual value. But it would be a perfect place to stash a message. Meaning that you could take a picture of 24-bit RGB, and you would have at least one bit per byte with three bytes per pixel, so three bits per pixel times the number of pixels.

And so the point is you could set those least significant bits to anything you wanted, and the picture wouldn't change. You'd see no difference in the picture. Yet it's now carrying what is kind of metadata. You could think of it as, you know, metadata is normally stuff we think of stuck in a header at the top. This is distributed metadata, distributed throughout the image. Now, if somebody were to specifically suspect that you had done that, then, you know, any intelligence agency could strip off the least significant bits and recover the message. But if you went a step further and encrypted it, as we know, encryption is indistinguishable from noise. So now it returns to looking just like absolute digitization noise, and no one could prove any differently. So unless they had the key that went with that message, there'd be no way to prove that that wasn't, that that hadn't come out of the noise from the analog-to-digital converter that took the picture.

Now, you can't compress that, of course. The moment you compress it you lose typically the least significant bits that don't actually convey anything visually important. That's what compression of images does. But for a non-compressed image, it works. So that's the idea. And, I mean, and there have been variations of this. Many movie plots have involved circling certain characters in books where you need to know which book it is and which page it is, and then the key is a mask of cutouts where the different letters show through. So you have to place the mask over the page. That's not really the same, but it's sort of related. And so anyway, that's it. And I don't really have anything more to say about steganography, which is why I haven't given it a whole podcast. It's clever.

Leo: Yeah.

Steve: It sort of feels like an antique means of hiding something in plain sight. And the problem is, it is not subject to compression, and it's low bandwidth. I didn't make that

clear. But you can't mess with the original too much or you're going to the change the original in a way that might become obvious. So you have to only operate around the margins, which inherently means that it cannot convey much data. But there's lots of, you know, like just to send some GPS coordinates of something, that's not very big. And I would be very surprised if it weren't being done all the time now. That is, it's probably in practice, in use, but it's not something that we've spent a lot of time talking because there's really not much more to say.

Leo: There's a great book that probably covers this in detail that anybody who's interested in crypto probably should read, from Simon Singh, S-I-N-G-H. I'm sure you know it.

Steve: Yeah, in fact I read a chunk of it for one of our podcasts a couple years ago. I remember seeing it in my library. I thought, why did I get that? And then I remembered what it was, that...

Leo: It's a great book, yeah.

Steve: ...I wanted to do some deeper research.

Leo: So it has a history of crypto going - they say "The science of secrecy from ancient Egypt to quantum cryptography." So I would be surprised if steganography is not pretty thoroughly covered here. I don't remember if it is, but it's a great - even if it's not, you should read this book. It's just really great, the history of crypto.

Steve: Well, and we've talked about how obscurity is not good security.

Leo: Right.

Steve: And so steganography is the classic instance of obscurity. You are obscuring the message with something that no one sees. But it's not safe if anyone finds it.

Leo: Another great one, and I know you've read this, too, it's a little thicker, a little harder going, "The Codebreakers" by David Kahn, also a history of secret communications. This one was, when this came out the NSA was so worried that they instructed everybody who worked for them never to mention its name.

Steve: Oh, wow.

Leo: Do not mention this book ever.

Steve: And, you know, we've seen some of that. Remember when we were talking about the Snowden documents, that government employees were not allowed to view them

because - it's like, okay.

Leo: They'd violate, they would no longer be - they would no longer have their security clearance.

Steve: They'd blow their security clearance.

Leo: Their computer would no longer have it.

Steve: It was the Washington Post had, you know, it was covered all over the Internet.

Leo: You can't look at it on your computer.

Steve: Everyone, la la la la la la la no no no no no.

Leo: Whit Diffie says that "The Codebreakers" was very influential in his crypto studies. So that's a pretty high recommendation.

Steve: That's the top of the peak. That's the top of the heap.

Leo: Here's a question I'm very interested in your answer to. Chris Murphy in Denver says how come you use Google Contributor? I quickly looked into the Google Contributor both you and Leo are saying is something you hope takes off. I agree, websites need to get paid, but wait a minute. How does Contributor work? I would imagine that I've got to browse logged into my Google account so they know when to display those pretty patterns instead of annoying ads, and take my money and give it to the website. Well, if that's the case, haven't we just given Google even more permission to track us? And does Google share or sell that information to websites anyway? I couldn't find any technical details on how this magic works, so I trust you will give us a thorough breakdown. Thanks in advance, Chris.

Steve: So my answer is I don't - this is another one of what I would call a soft, yeah, well, a soft solution.

Leo: Right.

Steve: I want to support the web. I don't have any problem with that. You and I give to Wikipedia. Sometimes I see a great piece of freeware, and the guy wants $10, but it's really good, and I'll shoot him 25. I mean, I just...

Leo: Right, all the time.

Steve: I want to, I mean, I've got listeners who have bought SpinRite and never used it because they wanted to support me and the podcast. And so this is my way of giving back, in addition to doing the podcast, of course. And so I'm into Contributor for the max amount. It's fun to see that I'm supporting iMore by going there. That makes me feel good. So this is just, I mean, we are - this is what's so interesting to me about this is that we are - this is a time of tremendous change in, like, these glaciers colliding, the collision of forces in this particular aspect of our industry. And so I'm not telling everyone that, like, this is the answer. It's the answer for me.

So but Chris is exactly right. Google needs to know it's I who am surfing so that the ads are from Google. Google is receiving my Google session cookie when the website I visit causes my browser to pull those ads, so Google knows that Steve Gibson, I mean, it knows a lot about me. It's not guessing. It knows that Steve Gibson is on this site and is wanting to fund it through the advertising system. So if you are concerned about tracking and privacy, then you really are, you're really lowering your anonymity when you use Contributor.

Leo: I would disagree because, unless you are always incognito surfing, I mean, if you have a Google account, and you're logged into that, there's a cookie on your machine that establishes your identity, whether you use Contributor or not. That could be passed to any website with Google ads on it anyway.

Steve: Correct, correct.

Leo: So if you're worried, you could be...

Steve: Oh, I see. So in terms of the incremental exposure, yes, very good point. It's not a lot of additional incremental exposure.

Leo: It's probably none at all because what you're contributing to is sites running Google ads. Because they're running Google ads, almost certainly the Google identifier that identifies you uniquely through your Google account is being passed each and every time you go to that site, whether you pay for Contributor, whether you use Contributor or not. The only way to avoid that would be to surf in incognito mode.

Steve: Yeah. The only thing I would say is that - well, and if you were in incognito mode, then you can't use Google Contributor.

Leo: Right.

Steve: So, yeah.

Leo: It does, it requires a login to Google account; and that inherently, whether you're using it or not, is leaking information.

Steve: And the fact is there's so many benefits for being logged into Google as you do things now...

Leo: That's my choice. I like to stay logged into Google.

Steve: It's my choice, too.

Leo: That's an example, though. See, that's the thing. So on an Android phone, unlike an iPhone, once you log into your Google account, every time you use anything, any other Google service, it just says, is this still you? And you say yes. You don't reenter your password. Whereas Apple, no matter what you're doing, says "Please reenter your password to prove that you're you."

Steve: I would just add to Chris's question, Google is very unlikely selling this to anyone else. They don't need to because they are the "else."

Leo: They're selling the ads, yeah.

Steve: So, yeah, they own DoubleClick and everything else, so.

Leo: Channel 4. Question 4 from Hendrik in Germany. He wants some calibration on the utility of today's antivirus utilities.

Steve: Oops.

Leo: Yeah, well, we just talked about it. I've been a listener to Security Now! since about two years ago and currently listen to the older archived episodes. I still have much left to listen to. But since you are so deep into security, I wanted to hear your opinion on antivirus and similar protection software. I personally do not use any AV on my Windows box because I know what to install. I always look for valid signatures. And if I encounter a suspicious file, I upload it to VirusTotal, et cetera. On my Debian-based work computer I do not use one either. However, on my parents' computer I install an AV simply because, well, they don't know how to detect malicious behavior. And even though I do not believe it helps much, at least it helps some and "pretends" to secure my parents PC. Now I would like to know if, and if yes, how you protect your devices from malicious software? Do you consider AV necessary, or is it snake oil? Keep up the great show, and greetings from Germany.

Steve: So this question absolutely fits with today's news of the inherent attack surface that any AV utility presents to the Internet. So I think by now Hendrik knows that I'm not an AV user, but I do turn on Microsoft's. I think that's the right compromise.

Leo: It's kind of free.

Steve: Yeah, it is free, and Microsoft is trying to protect their OS and your experience from bad things on the Internet. Microsoft crept into this in the same way they always do, because they don't want to be slapped with antitrust suits instantly. So in the same way that they didn't want to compete with firewalls, so they kind of brought in a weak one and left it off by default, then turned it on, and now we've really got one...

Leo: It tiptoed in.

Steve: Yeah. Similarly, they've tiptoed in with AV, saying, oh, don't worry, we're not going to compete with anybody else. And then, you know, now we've got the Microsoft built-in AV. Absolutely use that. That's what I would - Microsoft Windows Essentials or whatever they're calling it now. That's what I would use.

Leo: I guess I would say that one of the reasons antiviruses are not as useful as they used to be is the prevalence of zero-day exploits.

Steve: Yes.

Leo: What you really want to be protected against is not the five-year-old virus that everybody knows about. You want to be protected against the stuff that's coming out and spreads like wildfire. And that's exactly what antiviruses can't protect you against. They don't about it yet.

Steve: Right. And notice, I mean, he really is up to speed.

Leo: Oh, he knows what he's doing, yeah.

Steve: He's using Debian at work, and he's uploading things to VirusTotal to see if something is suspicious. So, yeah.

Leo: Things have changed, that's all. I mean, in the past an antivirus would be a good idea because there were lots of old viruses floating around. But now the preponderance of viruses you're going to encounter in an email fraud or in a click fraud is going to be - or on a website is going to be modern.

Steve: And they're normally only getting in because of a vulnerability. And now those are all being patched very quickly, too. So once upon a time we didn't have connected systems where the systems themselves could check pinging, could continuously ping the mothership to see if there's any updates to them. And now we do. So, yeah, I agree. I think that, you know, just going with what's essentially built into Windows, for me...

Leo: The other thing I would say strongly is do not use the free antiviruses, with the exception of Microsoft's free antivirus, because, well, now we know AVG is selling your data.

Steve: Yup.

Leo: And, I mean, these free guys, they really, I mean, you always wonder, well how are they free? And I always just assumed, well, they'll upsell you to the paid product. But maybe not. Maybe there's other things they're up to.

Steve: Yeah. They're monetizing you.

Leo: If you're cheap, and you don't want to buy an antivirus, and you think you need one, use Defender. It's free. Comes with Windows 10.

Steve: Yup.

Leo: I know, I know, you'll never use that. But it comes with Windows 8. And you can download it for previous versions of Windows.

Steve: Well, and I had it on 7. Or, I mean, I had it on XP until...

Leo: Right, you download it. Just go to Microsoft.com.

Steve: Until it stopped working. And then I'll get it again when I go to 7.

Leo: Microsoft.com/security - what is it called? Defender; right?

Steve: Yeah.

Leo: Security_defender. Vigen Galustian in Los Angeles - I first of all apologize for butchering your name - says: Steve, love your show. A while back you spoke about password length and referenced a list for ranking the companies based on the password length and how secure they were. Yeah, I was chagrined the other day, I created a new password for my bank, which is kind of routine - I'm speaking now, Leo - as routine hygiene, and they said, oh, it can't be longer than 12 characters. And I went, oh, crap. I remember Apple was number one on the list, based on password length. I've been unable to locate it, though, in the show notes. Would you by any chance be able to point me to the site for this ranking list?

Steve: So I don't think I ever talked about that. I'm wondering maybe if we're being

confused with some other outlet or podcast.

Leo: Yeah, I don't remember it either, yeah.

Steve: I don't think so. But I chose this question because this did trigger something I wanted to mention, and that is I would agree that 12 is a little short. But I've had people complaining about 20.

Leo: That's plenty. Twenty's plenty.

Steve: Yes. And that's my point. I just wanted to say that, for the record.

Leo: If it's 20 good characters; right?

Steve: Yes. If you have a 20-character high-entropy password - and remember, GRC.com/passwords, and there they're minted for you. For some reason, people are getting them all the time from there. I've seen people saying, I have me and my whole family goes to GRC.com/passwords whenever we need a piece of a password. It's like, okay. You know, LastPass does the same thing. It just makes them up.

Leo: All password vaults will give you good random passwords, I think, yeah.

Steve: Yeah. And that's what you want. But my point is 20, in terms of brute-force cracking, in terms of the number of bits of entropy, you know, if it's - it probably can't be eight bits because that would require a large character set. But it's - and I should have this on the tip of my tongue. It's like a 96-character set. So you can do the log math. But it's maybe seven bits, so times 20 is 140 bits. That's a lot, I mean, we're protecting communications with 128 bits. So your password would have at least that much entropy, if you chose it well at random. So my point is, 20, for everyone who complains about it being a length of 20, it's fine.

Now, it's true that the idea that they even know the length is annoying, and this may be what people are concerned about, is that it sort of suggests they're not just hashing it and not caring about the length. They should actually not care. But there are, in fact, banks we've talked about, in some cases banks have the web as the frontend to old-school mainframe software, and the web password is being passed through to something, you know, it doesn't have spinning reels and mag tape any longer, but it may have some blinky lights like mine over my shoulder. Anyway, 20 is enough, and just make it a good 20, exactly as you say, Leo.

Leo: Yeah. Although sometimes I'll do, you know, there are sites where you can do, like, 30 and 40. And it's just fun to see - well, you have, what, how many, 64-character passwords on yours?

Steve: I do. And as our listeners will find as soon as I formally publicly release the SQRL

demo site, you know me, I had to have some fun with it, so mine are 256 characters.

Leo: Well, that's the point. If you're using a password vault, the length is arbitrary. It doesn't matter. Make it as long as they'll allow you. I was just really disappointed when my bank said 12. Of course, I made a very good random 12-character password. But I'm looking at it, and I'm thinking, if I can memorize it, how good is it really?

Steve: Right.

Leo: You know, if I can look at that and say, well, I can remember that...

Steve: That's the test.

Leo: Yeah. How good could it be? Judy Ruby-Brown in Coppell, Texas worries about Windows 10 and whether she has an open network and whether she needs to rename her router: Steve, I've been a listener for only a few years. I have SpinRite; I hope I never have to use it. That's nice, Judy, thank you. I have a new Windows 10 computer. I've disabled all the normal things recommended. But I've been left with two questions after studying Microsoft Windows 10 FAQs as best I could: One statement from "What should I know about connecting to an open network?" Their answer begins, "An open network is a WiFi network that doesn't require a password to connect, which means that the network isn't secure." My network is encrypted and password protected, but standard Verizon FIOS for home use. That seems to mean my network is NOT an open network; am I right? Yes, you're right.

Steve: Yes.

Leo: Further on, "How do I opt my WiFi network out of WiFi Sense?" This is that technology we talked about that Microsoft has for sharing your password with friends. The statement is, "If you don't want WiFi Sense to connect people to your open WiFi network or allow people to share access to your password-protected network, you can opt your network out of it by including '_optout' somewhere in the WiFi network name, also called the SSID" - oh, that's interesting - "for example, 'mynetwork_optout.'"

Steve, if you agree my network is not an open WiFi network, do I need to rename my SSID to keep Microsoft from snapping it up? And do they get my network password? Perhaps others are equally confused. Thank you.

Steve: So I wanted to revisit this because the industry has calmed down a little bit from the initial hair-on-fire Windows 10 release, where we looked carefully, and there was a huge concern about social networking leaking your WiFi passwords by default. And it took a while for people to realize, oops, not by default. So first of all, we do know that Judy's network is not open. She has a password, so it is encrypted.

So the second part is she clearly wants to prevent her network password from being

shared promiscuously with others. So there are two ways to do that. But first you don't have to do anything at all for it not to be shared, which is to say you have to explicitly enable it to be shared from a given Windows machine. Under the Settings, the big Settings panel you get up, one of the big icons there for a section is Network & Internet. So if you click that, then you'll find Manage WiFi Settings. And if you click that, then you'll find a switch, which is off by default, which says Connect to Networks Shared by My Contacts. And if that's off, a lot of other things are hidden.

So if you're curious, you could turn it on. And when you do, then down below that, well, first of all, then there's a list of available networks which you have to manually enable one by one to turn sharing on for your contacts that are on those networks individually, like Facebook and Live and whatever Micro - I think I have three on my Windows 10 system. But even then the individual wireless networks that that machine knows about will also have sharing off for them individually, and you must turn it on.

So the lesson here is Microsoft did not do what we were initially worried about, which was just instantly and automatically assume that you wanted to share your own private network's password with anyone who you know from any other social networking site. All of that portion of it was properly disabled by default. Although it's worth noting this is sort of machine granularity. That is, this is you telling this machine and Microsoft through this machine not to cross that bridge to allow others who you know on other networks to obtain the password through the cloud. That's different than the "_optout" option. So, and I've been looking around, and I have not seen a single SSID that has added the "_optout" to its name. I just, in the wild, I have not yet encountered one.

Leo: Can I weigh in on this one? Because I think I know what's going on here. So WiFi Sense does two things. It does the thing you just described, which is make it easy for you to share passwords with other Windows 10 or Windows Phone users, who are your friends. And most people never will use this. But it's also designed to automatically log you into captive WiFi portals.

Steve: Ah, right.

Leo: So those are the coffee shop place where you just join it, it's not password protected, but then you get a page where you agree, and you may be...

Steve: The terms of service.

Leo: Terms and all that stuff. That's what's called a "captive portal," as we've talked about before. It breaks the Internet. It's a terrible idea. But everybody uses it. And I understand why they want to do that. My guess is this "_optout" or whatever it is, is really about a temporary way to keep - or maybe a permanent way to keep WiFi Sense from automatically joining a portal. So if I'm Mr. Coffee Shop Owner, and I don't want people using WiFi Sense because, by the way, it puts spurious credentials in there, if I don't want people using WiFi Sense to get onto my thing, I just put "_optout" in there, and...

Steve: I see, right.

Leo: And that's my guess, it's a total guess, that that's what that's for. It's not for home users.

Steve: That absolutely sounds right because I was going to say, I was going to wrap this by saying, essentially, it's an "and."

Leo: You're already opted out.

Steve: Right, exactly, by not opting in.

Leo: Right.

Steve: Yes.

Leo: So they don't need to add that. I understand why you were confused, Judy, because they should really put that in some other part of the FAQ. But that's what I think. It's my guess.

Steve: I think that's exactly right.

Leo: Home users don't have to even think about that. That's not relevant to you.

Steve: And if you don't turn all that stuff on, I mean, you have to deliberately go through a lot of hoops in order to turn it all on.

Leo: It even asks you each time. I mean, it's like, it's - yeah. They're not idiots. They're not going to turn on something like that. I think, I mean, we've got to give them a little credit for something, whether you like Windows 10 or not.

Steve: With the flippy tiles.

Leo: Some people like that, Steve.

Steve: And they're welcome to it.

Leo: Keep your flippy tiles. Mark Withers, Hayward, California, cannot get any new content filters to install: I have tried to download all of the recommended iOS content blockers from the App Store. Every one of them reports my iPhone 6s Plus is an "unsupported device," so it won't install them. Any thoughts on why those apps

are being blocked from install? Thanks for a fantastic show. Mark. You don't usually do tech support on this show. You're being very generous with this one.

Steve: I've seen it. And in fact it's funny because the previous question was a The Tech Guy question.

Leo: Yeah, total Tech Guy question.

Steve: That's what you get on the weekends. And this, too, we both know that Mark forgot to update to iOS 9.

Leo: That's what I would have said, except he said it's an S Plus, a 6s. Which ships with 9.

Steve: Except that I think that the question, he may have posted it immediately upon - oh, a 6s. Oh, I see what you're saying.

Leo: 6s comes with 9.

Steve: Ah. You're right. I just was assuming that the problem was 9.

Leo: Unless he's wrong, that he doesn't have a 6s, he just has a 6.

Steve: Yes. And if it's a 6, okay, so Mark, if you're listening to the answer of your own question, in Hayward, make sure you're using iOS9 because iOS8, this is exactly what would happen. And we were at, what, 8.4.1 before we went to 9.

Leo: Right.

Steve: And now we're at 9.0.1. So just make sure you have 9. And if you do, I don't have an answer for you because I think it should work. It has for everybody else.

Leo: This is, by the way, why you should never be a tech guy on the radio.

Steve: I don't want to be.

Leo: No one should. Me either.

Steve: I don't know how you do it.

Leo: Because what happens is people misreport the condition. And then you're scratching your head, saying, well, that shouldn't happen. And then what it turns out, oh, I thought it was a 6s. No, it's just a 6. And, you know, and you've been wasting all this energy trying to solve it.

Steve: Oh, you mean I shouldn't be standing in an inch of water when I do that? It's like, no.

Leo: Being the Tech Guy is tough because sometimes you just, you don't feel, I know I don't feel like I'm getting all the information that I need to get, or the information's being misreported. It is, I mean, it's not normal. If it really is a 6s, the real answer is, and this is also one you don't want to give on the radio, "Bring it to the Apple Store. They'll fix it."

Steve: Yeah.

Leo: By the way, it's a little confusing that there is no content blocker setting in the settings until you install a content blocker.

Steve: Yes.

Leo: So that's completely backwards from what I'm, after 30 years of using computers, used to.

Steve: Right.

Leo: There is no setting to turn on at all. So you may look at your phone and say, well, I don't see a setting. You have to first download a content blocker. And then you can turn on the setting.

Steve: Oh, and you have to run it. You have to start.

Leo: Oh, yeah, you have to run it before it even knows it's there, yeah.

Steve: Yes, in order for it to register itself. And then they go, oh, okay.

Leo: And by the way, most of them, when you run them, nothing happens, just puts up a blue screen, that's it, I'm here. Thank you.

Steve: Or they say, okay, now here's how to turn this on.

Leo: Yeah. That's what they should do.

Steve: You need to go over to Settings and blah blah blah.

Leo: Yes, that's what they should do. Filbert Long, who has a fabulous name - he's from Nottingham, so he probably has a fabulous accent, as well. He's unhappy with iOS9: Steve, your last podcast [SN-526] had me thrown me into a bit of a tizzy. Well, he said "dilemma," but it feels like Filbert should say "tizzy." I'm sorry, Filbert. You recommend upgrading to iOS9 as soon as possible because of all the security improvements. Well, I did my upgrade a couple of weeks ago, but since then I have reverted back to iOS 8.4 just so I can enjoy your show. I watch your podcast on my iPad using the Apple app, but since iOS9 - he's talking about the podcast app - the app is a disaster. Yeah, a lot of people have complained to me about it.

Steve: Yeah.

Leo: Apart from the poor UI, my main gripe is there's no full-screen option. No, there isn't. You cannot watch the video full-screen on the Apple podcast app in 9. You're now reduced to a small image. And to add insult you're surrounded by big white borders, making it difficult to see you and Leo. So my question is, what should I do? Upgrade to iOS9 and see you as a shadow of your former self? Or stay with 8.4.1, risking the security implications, and watch you and Leo in full-screen grandeur? Thanks for your podcasts. Filbert Long, SpinRite owner.

Steve: So this was an opportunity for me to mention that a number of apps were broken by iOS9. I saw a communication this morning from Jeff in the U.K., who has been moving the SQRL client for iOS along beautifully. It broke with iOS9. And he noted that when he - he had to go to, I think he said Xcode 2.0 from 1.2. And 59 syntax errors when he tried to recompile under 2.0. And so he's not there yet. And one of my favorite apps, and this is just a shout-out to my favorite iOS client for NNTP. Yes, old-school newsreader, newsgroups, because of course those are GRC's groups are NNTP newsgroups, is called NewsTap. And it also died when I went to iOS9. And I seriously considered moving back because I really - I was dependent upon it.

Well, the guy who did it was just on the verge of updating it. He has updated it. And so if anyone ever looked at it before, there is a free version, NewsTap Lite. And I think maybe it limits you to one group you can subscribe to, or one server. I'm not sure what. But, you know, I have the paid one. It is beautiful. So there really is a lovely newsgroup client for iOS, both for iPhone and iPad, called NewsTap. And iOS9 did break a bunch of things. I would imagine you have an alternative podcast viewer for Filbert Long.

Leo: Yes. In fact, it always amazes me that people use the Apple podcast app, which was terrible when it first came out. Remember it had big reel-to-reel tape? They spent all this energy that the tape would go down.

Steve: Skeuomorphic, yes.

Leo: Yeah. And but it also didn't work very well.

Steve: Oh, my god, the tape was leaving the reel?

Leo: Yeah.

Steve: Oh.

Leo: They spent a lot of - it was clear they spent a lot of energy on this reel-to-reel tape machine and very little on subscribing. And then it got better and actually was pretty good by the time 9 came out and broke it again. But that's just the Apple one. I mean, there's many great podcast apps. Overcast, which is Marco Arment's app, is fabulous. But it's audio-only, I think. So then you might want to try Downcast, if you want video, or Pocket Casts. There are many better choices. And of course we have - iOS has at least three or four different TWiT apps, which will allow you to subscribe and watch the video full screen. And I think many of our apps are being updated now because of the new API. And we are writing our own iOS and Android app that will use the new API. Those will be out by the end of the year, I hope. And they will, of course, also allow full-screen playback subscription and all that stuff. And watching live, which is kind of nice, something you can't do in the podcast app. So...

Steve: Nice.

Leo: Yeah. I think why should you use the Apple app? There are so many better apps out there.

Steve: Time to move on. Stay with 9 and ditch the Apple app. And it's 4:00 o'clock, and we're at two hours for the podcast, and number nine wasn't any good, well, it wasn't necessary.

Leo: Sucky question, sorry.

Steve: And we've already done LingsCars that was the surprise number 10. So we're done.

Leo: Love LingsCars. And we've got, now, I tweeted it because I thought it was so cool. And I thank you. And now we've gone down a rabbit hole because there's much more going on with Ling. I'm fascinated. We're going to try to get her for Triangulation. Right there, that's it.

Steve: That'd be great.

Leo: Wouldn't that be awesome?

Steve: It's an Internet meme, LingsCars meme.

Leo: She's amazing.

Steve: Yeah.

Leo: So thank you, Steve. Yeah, we'll wrap it up. Next week, we don't even know. Could be anything.

Steve: There is, well, we're going to do some technology. And there's been a problem found with cookies where, because, I mean, cookies are the universal session glue. We just were talking about how, like, if you log in with Google, and then you go to any Google property, or you are served a Google ad, they get your cookie. Session management is the way we stay logged in on the Internet. Turns out some researchers, old and venerable as cookies are, they found some problems with cookie session management. And also our friend Nadim Kobeissi - god, I hope I didn't mangle his name - the guy who did Cryptocat did a really intriguing blog posting about what the VW emissions software scam tells us about software encryption, really an interesting take.

Leo: And the DMCA, gosh darn it...

Steve: Yeah, that prevents anyone from looking.

Leo: Yup.

Steve: So a couple neat techie topics for next week. I think we'll have a great podcast. And of course whatever news happens in the meantime.

Leo: If you want a three-hour Security Now!, just email me or tweet me or tweet Steve. I'm thinking, maybe we need to make some room in the schedule. We could go to 5:00. I don't know. I'm just thinking. Would you do a three-hour show if I got you the time? Tape is cheap, Steve.

Steve: And I have lots of coffee.

Leo: We'd have to have a bathroom break, though, in the middle. We'd have to have an intermission. Let's all go to the lobby. Steve Gibson is at GRC.com. That's where you'll find SpinRite, the world's best hard drive maintenance and recovery utility. That's his bread and butter, so buy a copy before you need it. You'll be glad you did

someday.

Steve: And use it before you need it, and then you won't. Wait.

Leo: That's good.

Steve: Yeah.

Leo: That's your new slogan. Use it before you need it so you won't.

Steve: You know that we just had, what was it, Yogi Berra who just passed away?

Leo: Yeah, that would have been a Yogi Berra-ism.

Steve: When you come to a fork in the road, take it.

Leo: Take it. Turned out...

Steve: No one goes to that restaurant anymore because...

Leo: It's too crowded.

Steve: It's too crowded.

Leo: Turns out that, now, some of these are apocryphal. But I was reading an obituary of Yogi Berra, I think in The New Yorker, and it said it turns out that that was accurate directions to his house. Either fork in the road got to his house.

Steve: Perfect.

Leo: He was smart, that Yogi Berra guy.

Steve: Perfect.

Leo: When you get to a fork in the road, go to GRC.com. There's lots of free stuff, fun stuff. Passwords, for one thing. SQRL, for another thing. And this show. You can get the audio and transcripts of this show at GRC.com. Leave questions for Steve at

GRC.com/feedback. Tweet him, @SGgrc. That's another way to get a hold of him. Um, or direct message him. If you have a longer question, you can always do that, as well. We have audio and video on our website, TWiT.tv/sn. You can also find all our other shows when you get there, TWiT.tv. And you can watch live. We are generally on from about 1:30 in the afternoon to 6:00, 7:00 p.m. I'm just teasing. Seriously, I would do three hours. I would have no problem with that.

Steve: I saw somebody tweeted, and they explained how long they had been with the podcast by saying, "I was watching when you were only two digits of minutes long." And it's like, yeah. And we started at, like, 18 and...

Leo: I remember that.

Steve: I know.

Leo: You're one of the most popular hosts, if not the most popular host on the network, Steve. So you can get as much time as you want.

Steve: Glad to be.

Leo: So do watch live. Come in the studio, we have a lovely visitor in the studio. Is this you, Christopher - yeah. He's on vacation. He's an IT guy from Wilmington, Delaware and learned everything he knows from you.

Steve: There's a lot of data processing going on in Delaware.

Leo: Yeah.

Steve: That's the major...

Leo: Do you work for a three-letter agency?

CHRISTOPHER: Mmm, no.

Leo: He said, "Mmm, no." That's a long "mmm."

Steve: He works for someone we've heard of. And that was the "mmm."

Leo: Mmm. If you want to be in the studio, you can, no problem. We have limited

space in this little studio, my office. But just email tickets at TWiT.tv, we'll let you know if there's a seat for you. And we'll see you next time on Security Now!.

Steve: Thanks, Leo.