SECURITY NOW!

Transcript of Episode #605

Google vs. Symantec

Description: This week Steve and Jason discuss: Google's Tavis Ormandy takes a shower; iOS gets a massive feature and security update; a new target for bot money harvesting appears; Microsoft suffers a rather significant user privacy fail; the U.K. increases its communications decryption rhetoric; a worrisome vote in the U.S. Senate; Nest fails to respond to a researcher's report; this week in IoT nonsense; a fun Quote of the Week; a bit of miscellany; some quickie questions from our listeners; and a close look at the developing drama surrounding Google's enforcement of the Certificate Authority Baseline rules with Symantec.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-605.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-605-lq.mp3

SHOW TEASE: It's time for Security Now!. We've got, of course, Steve Gibson. I'm not Leo Laporte. I'm Jason Howell, filling in for Leo while he's gone. We're going to discuss a lot of really cool stuff today, some of it a little bit on the edge of the scary; but that's okay, that's what it's all about. The lucrative LastPass shower may sound a little bit more risqu than it actually is. Apple's mountain of security updates for iOS. What exactly is the GiftGhostBot? And Steve goes in-depth on how Google has thrown down the gauntlet with Symantec. Security Now! is next.

JASON HOWELL: This is Security Now! with Steve Gibson, Episode 605 for Tuesday, March 28th, 2017: Google vs. Symantec.

It's time for Security Now!. This is the show where we talk about, well, what else, security, privacy. I feel like right now this moment in time is ripe for a show like this, and that's obvious because Steve Gibson is here week after week, talking about security items from GRC.com. Hey, Steve. How you doing?

Steve Gibson: And everybody realizes this is not Leo's voice that has introduced the podcast. Jason...

JASON: Either that or Leo got real good at imitating my voice. No, I apologize. Leo is actually out, away on vacation, enjoying, I don't know, I hope he's like on a beach somewhere. At least that's where I'd be if I were him.

Steve: He called it a "mini vacation." He sort of disappeared. I only picked up on it when Tony shot me a note last week saying, "Hey, Jason's going to be your co-host next week." I said, oh, okay.

JASON: All right-y then. Away to the beach he goes. And in his place you get me. Now, I'm of course on TWiT every day of the weekdays, anyways, doing Tech News Today with Megan Morrone. We talk about a lot of security topics on that show. Like I was telling you earlier, you take it to a whole 'nother level. So again, Steve, I'm super humbled and honored to be on the show with you. You do such a great job with Security Now!. Thank you.

Steve: Glad to have you with us. Today we're doing Episode 605. And the nominal title, as has been the case for the last many months now, we've just been having news-packed podcasts. And I like to wrap up the podcast with what is maybe arguably the big news of the week. This one is titled "Google vs. Symantec" because, as I put it in the show notes, Google has dropped the other shoe, in this case on Symantec. We discussed, I think it was late 2014 when Google discovered some misissued certificates for themselves and for Opera, which had been issued by Symantec or an affiliate or a partner or something. And that raised some red flags.

Well, what has happened since is that it turns out the problem is way worse than was believed, to the tune of, I'm stepping on the lead here a little bit, but 30,000 misissued certificates. So Google is doing what Google does. And they're going to smack Symantec down pretty hard. Anyway, we will end with that. But we're going to talk about a very productive shower that Tavis Ormandy, our favorite security researcher from Google had, and the consequences of that, apparently in the late morning last weekend; and, unfortunately how he ended up discovering a huge, apparently very sophisticated, but also a significant problem in LastPass yet again. LastPass, of course, is on it.

We're going to talk about how iOS yesterday got a massive feature and security update, well, a minimal feature, but massive security update. There's a new target for bot money harvesting, which has been found going on in the wild, and how that affects us. Microsoft suffered a rather significant user privacy fail. The U.K. is increasing its communications encryption rhetoric worrisomely. Then we had just late last week a vote in the U.S. Senate that has all the privacy people up in arms. Nest has failed to respond to a security researcher's report. We've got, as we have been now every week for a while, This Week in IoT Nonsense, another crazy device. An interesting quote for the week. A bit of miscellany. We're going to do some quickie questions from our listeners to keep everybody engaged.

And then, as I said, we'll take a close look at this developing drama surrounding Google's enforcement of the certificate authority baseline requirements, which there's very little question Symantec has violated and is going to be paying the price for. So I think a great podcast.

JASON: You know, no big deal, just that few amount of security stories. Not a big deal at all. A question I have for you before we kind of move into all this stuff is, I mean, you've been doing Security Now! for quite a few years now. How many years exactly?

Steve: You know, shortly after the Internet began to really happen, what happened was GRC got its first static Internet connection. It was an IDSL line, you know, with a block of IPs. And something caused me to scan the neighborhood surrounding that IP address, our IP addresses. And what I found was a whole bunch of people's C drives exposed. That is, other people's Windows machines had file and printer sharing wide open. I mean, and you could, with issuing a net command, you could map their drive to a drive letter on your own machine and do a directory. I mean, this is the way it was. We talk about it like being the Wild West today. But, oh, my god, back then.

And so what happened was that, first of all, I protected ourselves from that, if we weren't already. But that was what created ShieldsUP, was I thought, oh, my god, I have to, like, allow people to easily determine whether their C drives, their Windows drive is readable and even writeable by everyone on the Internet. So I created ShieldsUP to create a simple test where anyone could just go to GRC's web page, and GRC's server would check their IP from outside and show them what was there.

Often people would, like, name their computer with their own name. So I was able to get their administrative credentials and often greet them and say - it happened to Leo on the original Screen Savers. Kate Botello found ShieldsUP. And when you went there, it said, "Hi, Leo," you know, addressing him by name, and then showed you a tree of all of the devices on your machine that were accessible to the Internet. And as it happened, back then at Tech TV they were behind a corporate firewall, so nothing was visible. But many people at home, I mean, this even predated NAT routing. So people just like directly connected their one PC to their ISP's Internet connection and were completely exposed. So I don't know, what, 15 years ago, I guess?

JASON: Somewhere around there. That's fascinating, by the way. I had not heard the back story, and I love that. It's like an example of how much things may have changed in some regards, and how much things have actually stayed the same in that that regard.

Steve: We're still fighting, but, boy, it's a lot better than it was.

JASON: Security Now! Episode 1, August 18, 2005. So right around coming up on 12 years, then, which means you've been doing the show a long time.

Steve: Yeah, well, so that's the podcast. But it was when I was in Toronto with Leo one Friday, I think it was - no, it wasn't a Friday because he had Fridays off. But so it was one of the earlier days in the week. We were in between shows, and he said, "So what would you think about doing a weekly podcast on security?" And I said, "A what cast?" I'd never heard the term. He says, "You've never heard of a podcast?" I said no. Anyway, so back then I already sort of was involved in security, enough so that that's what Leo thought of me as. And so that was probably, like, 13 years ago. And so I'd already established myself.

So maybe it was more like nearly 20 years ago that I really started focusing on this. I mean, hard drives and SpinRite was - in fact, that's what happened. When Kate Botello found ShieldsUP, Leo's first reaction was, what, a security product? I thought Gibson was a hard drive person. And it was like, well, yeah, okay, you know, that's done. And so now I'm going to go and do something else because hard drives, I've already figured how hard drives can be recovered.

JASON: And it turns out there's a ton of overlap between the two anyway, so...

Steve: Well, it's technology. I just love technology, as our listeners know.

JASON: Yeah. I guess what I was thinking is there's so - I feel like security news is so fast and heavy right now. I'm just curious, like 12 years ago, I mean, in the span of 12 years, I have to imagine security, just as a focus for the show, you have so much more to work with now than you ever did. It feels like a very intense time for security right now, I guess is what I'm saying.

Steve: Yeah. I mean, like Facebook didn't exist. And so, for example, [dropout]. And my family, they had no Internet presence. I had one because I was a web guy with a server and a website. But so think about what it means now that the world has their own content on the Internet, thanks to Facebook making it easy, basically, sort of to roll your own little personalized website. So, I mean, there's so much more individual engagement today than there was decades ago when, I mean, yes, people had email. Mom had, as she calls it, AWOL. I said, no, there's no "W" in there, Mom, it's just AOL.

JASON: Although kind of fitting in some ways.

Steve: Right. So email was like everyone's first contact. And they were consumers, but they weren't producers. Now we have blogs. We have Facebook. So there's so much more engagement. And of course we still haven't really figured out how to do security right, which is why we're in our 12th year and have no sign of running out of things to talk about.

JASON: That's right. We've got a lot of those things that Steve is talking about. All right. I guess we're getting right into the news. I noticed at the top of it, this is totally applicable to me. I am a very passionate and happy user of LastPass. And I've been away, by the way, I've been away on a vacation for like the past week. And because I was out of the country, I didn't have mobile Internet, so I was relatively offline, more or less, a few bits here and there, but not the way I am when I'm here in the states. So I had really missed a lot of what had happened around LastPass. I guess catch us up to date. Where are we at?

Steve: Well, we will. I did want to mention our Picture of the Week first.

JASON: Oh, yes, absolutely.

Steve: We always have sort of a fun thing that typically our listeners find. This one shows your classic boxy head, with antennas sticking out of his head, robot sitting behind a desk, reading a book whose title is "You CAN" - underlined and bold - "Pass the Turing Test!" And of course now the Turing test is the famous sort of thought experiment that Alan Turing developed back in 1950. The idea was - so, you know, of course he was famous for an early pioneer in computers. And so the Turing test suggests that the challenge you give a computer is for interaction with it to be indistinguishable from that with an actual human. That is, sort of to prove it's intelligent.

And so the idea would be it would be a blinded test where, for example, a person giving the test to an unknown entity wouldn't be able to see them because otherwise you could tell it's a boxy head robot. But, for example, the only communication would be through a terminal, for example. And so you ask questions, and then this entity which you can't see responds. And so the question is, can you see any sign that this is a nonhuman, based only upon its responses?

So that was sort of the concept that Alan Turing first proposed was, if all we know is what this thing types, can we say is this a human or a robot? And in essence, a CAPTCHA is sort of that. It's I'm a robot; I'm not a robot. The idea being the whole concept, the whole reason for a CAPTCHA was to allow a website to differentiate between a bot that might be visiting and, like, for example, trying to create a new account, or log in as a person or whatever, versus an actual human. So CAPTCHAs are a practical form of Turing test.

So anyway, this picture ties into a fun Quip of the Week that a listener of ours, Chris Schrimsher, provided. And he was quoting someone on Reddit who said, and I love this, he said: "I'm not scared of a computer than can pass the Turing test. I'm terrified of the one that intentionally fails it." Which I thought - I got a kick out of that, the idea that the computer's like, okay, I'm going to pretend I'm not intelligent, so you underestimate me. And we'll go from there.

JASON: Yeah, that's kind of terrifying. When I read that quote, I was like, oh, man, I hadn't thought of that. Great, another thing to be worried about. Excellent. There's probably a really good reason that it might want to do that at some point.

Steve: Exactly. So, yeah, exactly. Skynet doesn't want to let you know that it has become intelligent until it's already secured all the assets that it needs, and then it will spring that on you all at once.

JASON: It's like a reverse-Turing test.

Steve: Exactly.

JASON: Or quasi.

Steve: Being smart enough to deliberately fake you out and fail the test because it's not yet ready to reveal itself. So, yeah, that'd be a little worrisome.

JASON: There's no reason to expect that this won't happen at some point, and there will be a really good reason for it. I've wondered if at some point we're going to get to the stage where there will be social networks specifically for robots, essentially, robots communicating with each other. And I wonder if, at that point, they will be able to identify on a large scale whether they are in fact talking to other robots, or they are talking to humans.

Steve: Well, you know the smart...

JASON: I don't know what the purpose would be for that, but there you go.

Steve: A commonly asked question of smart people like Bill Gates and - I can't think of any other smart - Alan Kay.

JASON: Bill Gates is pretty smart. He's good enough.

Steve: Dean Kamen and, I mean, like real thinking people, is are you worried about this, like, explosion in AI? Like could Skynet happen? And the more well-informed these people are, the more worried they are. I mean, it's not like it's 50-50, or we're not sure, or no, probably not. But, I mean, the guys that understand are, like, yes, we need to be paying attention. Because famously we tend not to. I mean, the whole history of security and the Internet is one of not paying sufficient attention. The good news is the damage is well distributed.

For the longest time viruses were just annoyances. They only existed for the sake of their own existence, rather than do anything. Now, of course, we have things like cryptomalware that encrypts all your files and demands payment. So, I mean, and this was a foreseeable development. Well, let's hope that at some point in the future we're not looking back on how quaint it was when computers were word processors, and now they're our masters, because I'm one of the people who thinks, yeah, that's, you know, we're not that special that it's not impossible to, I mean, look at Watson winning, you know, chess is not anything that people can play anymore. And Watson beat the best "Jeopardy" people. I mean, I couldn't. So it's like, okay, that's a little worrisome.

Anyway, Tavis Ormandy, our favorite security researcher and penetration tester at Google apparently does some of his best thinking in the shower. On 12:20 in the afternoon last Saturday, March 25th, he tweeted, apparently shortly after toweling himself off, he said, "Aha. I had an epiphany in the shower this morning and realized how to get code execution in LastPass 4.1.43. Full report and exploit on the way."

So, okay. So the version 4 - and, by the way, this is Chrome and Firefox. It's the most recent version of the browser extension for LastPass. The 3 version they are in the process of deprecating. And I would imagine most LastPass users would have already moved to 4 and be current. LastPass responded by 5:00 p.m. on Saturday, so they were paying attention: "Our team is currently investigating a new report by Tavis Ormandy and will update our community when we have more details." And then Monday, yesterday, they put up a formal blog posting saying: "Over the weekend, Google researcher Tavis Ormandy reported a new client-side vulnerability in the LastPass browser extension. We are now actively addressing the vulnerability. This attack is unique and highly sophisticated."

Oh, and I'll just interject here that Tavis has since said there's a fundamental architectural problem, that is, apparently this not a buffer overrun where you go, oops, we forgot to check for null or the length of a buffer. This is something apparently very sophisticated, but also that's going to require some reengineering. Tavis has given them 90 days and said don't rush this because, first of all, no one's providing any additional information. Nobody has any idea what this is. So this is being kept very close and quiet while LastPass addresses this.

And then they continue in their blog post: "We don't want to disclose anything specific about the vulnerability or our fix that could reveal anything to less sophisticated" - than Tavis, but I added that - "but nefarious parties. So you can expect a more detailed post mortem once this work is complete." So anyway, so again, this is the kind of thing we want to have happening in our industry. One of the common things, Jason, that we've developed in the podcast over the last couple years, really just from looking at the reality of what we keep finding, is that though we don't want it to be, security is porous.

In last week's podcast we ran through an enumeration of the recent Pwn2Own competition at the CanSecWest conference that was also last week, where basically every browser and OS and even the VMware virtual machine system was just cut through. The ante has been upped a lot. In some cases it required a chain of individual vulnerabilities in order to leverage that into a full exploit. So it's not like one problem was found. It took five or six, all used in sequence, in order to make this happen. So it is difficult. But the point was that when researchers were incented by sufficient prize money, in this case a million dollars aggregate for all of the breaches, and generally they were getting 25, 50, $100,000, just that incentivization was enough to cause them to look closely enough to find problems. So of course all of those problems were exploited, but then fixed.

So from my standpoint, this is only good because we would rather have Tavis find it in the shower and have LastPass fix it on the QT, so that we get the update. And then LastPass will tell us, and Tavis will tell us, and we'll figure out what it was that he came up with. But nobody else. And we would rather have that happen than for somebody else to figure this out independently and be silently and quietly exploiting this without us knowing. So the modern model of security is we need researchers to be permitted to tear into these products as deeply as they need to, to responsibly disclose what they find, and then for the party responsible to respond immediately.

And what we have seen over and over again - and, I mean, so, yes, unfortunately it is over and over again with LastPass. But they are always responding within hours. And it's funny because the previous problem that Tavis found was resolved within hours of him informing them. And he had started his 90-day counter, and it didn't even count down one day before this was fixed. So that's what we want to see. And we'll have a story that we'll be talking about a little bit later on in this podcast about Nest and how they have done just the opposite, how they ignored a report from a researcher, after confirming it, for four months, and just said, eh, you know, okay, we'll get around to it. And then the researcher finally said, okay, sorry. I've given you four months. So I couldn't ask for anything better from LastPass.

And there was a comical tweet that followed this that someone sent to me, saying "We can all agree that Tavis is the problem with infosec. And if he'd just stop finding bugs constantly, then cybers would be secure." And of course he was joking because it is Tavis continually finding problems in all kinds of different systems which is increasing their security. And somebody else sent me a tweet saying "LastPass: Security done wrong." And of course that's not what I think. I've got LastPass browser extension loaded onto all of my systems. It's what I use. I would rather be using something which is, as a consequence of its popularity, has a history of being attacked and made more solid as a consequence, than some unknown, lesser product which no one has bothered to take a close look at because not enough people use it to incentivize anyone to look at it closely.

So all this is doing, I mean, these problems are the consequence of someone looking harder at the product they want to make more secure. Clearly that's Tavis's goal. That's why he's thinking about this in the shower is to make this the best product he can. And he is.

Now, I should mention that this morning I had a dialogue with someone on Twitter, asking about KeePass, which is a non-browser extension, multiplatform, encrypted database used for keeping passwords. And I've not talked about it because I've been so happy and still am with LastPass and the job that they've been doing and how responsive they are. But the problem that LastPass has, and any browser-integrated password manager will have, is that the browser is like the hardest thing to secure. In fact, we'll be talking about the - in fact, we'll be talking next about this iOS version 10.3 update that we got yesterday. And I enumerate the security fixes in it. And not surprisingly, WebKit, which is the Safari browser core, by far, well, the kernel was number two, but WebKit was number one in the most number of problems.

I mean, we're really asking browsers to do something technically they weren't designed to do. They were designed - originally the concept was you'd have static content, and you'd use the browser to browse. That's why it's called a "browser." You use it to browse the web. Well, now they've become application containers. And they're highly complex application containers that are struggling to do that in a secure fashion. So if you want integration of your password manager, I still think LastPass is, without question, the most secure solution. If you want more security, the only way to get that, at the cost of convenience, is not to integrate in any way your passwords with the browser.

Now, unfortunately, a complex password is really something that you're going to have to stick on the clipboard in order to move it from your password manager database into the password field of the browser. And so that represents a little bit of danger. But if the password vault wipes the clipboard proactively, or if you make the point of overriding it, then you're okay. So but if you decide that you don't need browser integration as much as you need more security than a browser can provide, then I think KeePass is a great solution. The crypto is done right. It's multiplatform. You can run it on iOS and Android and Windows and Linux and Mac. It's everywhere. It's K-E-E-P-A-S-S. Again, you have then the responsibility for synchronizing and managing and also copying and pasting the passwords which it has decrypted into your browser. So you have to do more work, but then you do have the benefit of nothing being in the cloud and there not being this vulnerability.

I have no idea what Travis found. No one does except he and the LastPass guys. But whatever it was, it was probably exquisitely subtle. And I think we'll have fun talking about it once we find out. But so as a consequence I don't think LastPass is security done wrong, obviously. I think they are doing it as well as they can, given the inherent tradeoff of wanting the convenience of a password manager integrated into the browser. Which was always a challenging thing to do in a secure fashion.

So again, it's like, yes, Tavis is finding problems. They're fixing them often. I mean, it's getting their attention instantly. In some cases an instant is all it takes to fix a URL, which was the problem last week, where they were able to fix that essentially on the fly, instantly solve that problem. This one is going to take more time. But again, they immediately turn themselves to the work of fixing it. And I think that's all anyone could ask for. It's all I'm asking for.

JASON: Absolutely.

Steve: Until we completely get rid of passwords, which is what I'm working on.

JASON: Well, thank you for that because we need it. Yeah, I guess the big challenge, because I hear all the time, like I've recommended LastPass personally because I feel like the tradeoff of convenience and security is worth it for me, right, to have all of my passwords scrambled and long and everything, and let that deal with it. Sure, there are potential issues; there are potential security exploits that might happen.

I think the big fear people have commonly is, well, it's one place that stores all of your passwords. So if they get it wrong once, if they get it wrong once in a very critical way, there goes your trust in everything you have stored there. The challenge is you never really, I mean, in the case of this, you never really know if the hacker also had a similar shower and came up with a similar thought in the shower, or not.

Steve: That's true. Yup, that is, you know. And in fact the problem we always face is you can't prove a negative. So, for example, when the CIA has with Vault 7 all of these exploits they've been keeping to themselves, the problem is many of them are, like, zero-day attacks. Well, we don't know that other people didn't independently figure those out and aren't using them, too. So it's one thing for a bad guy to keep them to themselves. A good guy like Tavis doesn't. The moment he's dry, he goes and sends a note to LastPass, with whom he now has a dialogue open, and says, hey, I found something else you guys are going to have to take a look at, sends them a proof of concept after he verifies it, and then they're on the project.

The problem is here's the CIA is sort of in between that. They're not wanting to give up their vulnerabilities that they find the way Tavis does. They're not, you could argue, they're not a malicious attacker; yet they're wanting to be able to leverage these for their own intelligence-gathering purposes. So they're really in a dicey sort of gray zone.

JASON: For sure. So you mentioned the iOS 10.3 update, which I heard of, with the new file system, is making things faster, some AirPod, Find My AirPods, CarPlay improvements. Of course, you zeroed in on all the security improvements, of which there were a lot. Tell us a little bit about that.

Steve: Oh, my lord. Well, yeah. So the first I knew about it was that Apple has had something called HFS, the Hierarchical File System, and HFS+, which is old. And so one of the things that they did with 10.3 is they updated to a much more modern recent file system architecture. Maybe users will see a little, like their storage requirements drop a little bit because it takes advantage of all the latest thinking in the way you arrange and store files. But there were also, in 10.3, a ton of security fixes.

And in fact I enumerated them just sort of for giggles here in the show notes. But, I mean, it's like, okay, how many pages of this? Let's see, one, two, three, four, five, six, seven - seven pages with, like, many things per page. And so I don't want to drag everyone through it. But here again is another example of the reality of today's security. There's no question Apple is as security focused as any company in the industry, I would say on a par with Google; and I give Google lots of props for the level of their security focus. In the same way that Tavis is thinking about this 24/7, clearly, and Google's Project Zero, and they're finding problems all over the place.

Well, Apple's focus, of course, is their own stuff. But they make a big point, I mean, security is a selling point, is a marketing feature for them, so they really care about it. So they fixed a problem, or found and fixed a problem in the Audio system, in the Carbon subsystem, two problems in Core Graphics, three problems in the Core Text system. And, for example, in Core Text, processing a maliciously crafted font file may lead to arbitrary code execution. Okay, now, that's one of the things that we've been discussing also. We've seen malicious images. We've seen malicious documents. Any time you are interpreting something, the interpreter has to also be perfect.

And so here font files are now, they're not just static data representations. They are interpreted things. And so you can make one that is deliberately malicious that will leverage a mistake or some bounds-checking lack in the thing that's doing the interpretation. So in this case a maliciously crafted font file could cause a memory corruption issue. And they fixed it by improving the input validation, that is, they found where somebody could do this, and so they added a check to make sure you could no longer do that.

And actually, so there were two instances of maliciously crafted font files and then a maliciously crafted text message, which leveraged some failure in their text message handling in the same fashion in this Core Text module. There was a problem in the Data Access module. There's a Font Parser that had three parsing problems. HomeKit had a problem. It said Home Control may unexpectedly appear on Control Center, and they said a state issue existed in the handling of Home Control. This issue was addressed through improved validation.

HTTP Protocol had a problem. The Image IO processing, in fact, here it is: "Viewing a maliciously crafted JPEG file may lead to arbitrary code execution." So we've already had some of those, and they're still having these problems. They had four problems in Image IO. The iTunes Store had a problem with an attacker in a privileged network position might be able to tamper with network traffic. The kernel had one, two, three, four, five, six, seven, eight problems that were found involving code execution. One, two, three, four, five, six, seven, eight - actually all of them were arbitrary code execution, which you don't want. So they fixed those.

Keyboard subsystem had a problem. The Libarchive, Libc++ application binding, the ABI had a problem. Pasteboard had one. Phone, Profiles, Quick Look. Safari had four. The Safari Reader had one. Safari View Controller. Under the Security module they have four. Siri had a problem. And then WebKit, as I said earlier, one, two, three, four, five, six, seven, eight, nine, 10, 11, 12, 13 problems. Oh, no, 14, 15, 16 - it continues on the next page - 17 problems. Because web stuff, I mean, a web browser is the massive nightmare interpreter of all time. It's interpreting HTML. It's interpreting CSS. It's interpreting JavaScript. I mean, it is a security nightmare.

And so here, mature as Apple's iOS is at version 10.3, or previously at 10.2 point whatever it was, even so, this far downstream there's still this much being fixed. And so all of what we see in the actual way security works says that today the best we can do is to try not to introduce new bugs as the existing ones are found and eradicated. And of course this is why I'm sitting in front of Windows XP SP3. That's the system I'm still using. I've got a system built for Windows 7, but I have a lot of life left in me. There's no way I'm going to 10 because new code also has new problems.

And I'm much more comfortable using something that is time tested and well proven than anything brand new out of the box. And XP was famously a security disaster for many years. Steve Ballmer was prancing around on the stage of Microsoft saying Windows XP was the most secure operating system Microsoft will ever be introducing. And of course that's not something you can ever say beforehand. The only way you can make any assertions is looking back and seeing how it fared. And it was a disaster in the beginning. So all of those early Code Red and Nimda and MSBlast worms, all those worms were Windows XP worms that caused huge problems for the Internet. It was like, whoops, well, you know. So it took time to get it fixed.

So again, this shows, with 10.3, how many problems there still are. I would argue iOS - and we were covering just recently that iOS, due to the tighter curation and the tighter environment that Apple has created, while it offers its users far less choice than the Android platform, because Apple has as much control over it as they do, it is demonstrably more secure probably than any other operating environment on the Internet today. Even so, it's still having problems found and fixed. All we can hope for is that the rate of creating new problems is substantially lower than the rate at which we're finding and fixing the old ones.

JASON: As an Android user - I do a show about Android on this network.

Steve: Of course.

JASON: It's called All About Android. You should check it out. I mean, that's one of the main things that I am very envious of on iOS. And I think most Android users would probably agree, even though I'm using, you know, I've got the Google Pixel phone, so it's Google's phone, which means that they're going to do a great job of keeping this updated with their updates as they happen. The majority of Android users don't enjoy that benefit. And, man, if iOS, like, is this normal for Apple to have this security rich of an update? I was looking through, I was like, man, does this happen like every time they update? And I just had to go back and think about what we're not getting on Android from security updates.

Steve: This was a big one. Yeah, this was a big one. You know, we've seen a bunch of little double-point fixes, like 10.2 point something, and point something, and point something. This feels like something they've been working on for a while. And so they just said, okay, we're ready to go, and they dumped all these out. And what we want is for them to be responsibly reported and then fixed quickly and then pushed out to us. And so that's what Apple's been doing. So yay for them.

JASON: Okay. Apparently a bunch of sites shouldn't look a GiftGhostBot in the mouth. I prewrote that. I hope you appreciate that.

Steve: Who was it who was asked, "Why do you rob banks?" And the answer was, "Well, because that's where the money is?"

JASON: I don't know, but they're brilliant.

Steve: Yeah, I always loved that line. But so it shouldn't surprise anyone that, as we were mentioning before, cryptomalware has happened because, if you encrypt people's files, you can extort them for getting their files back. So another place where there's money is in online gift cards. So a company, Distil Networks, based in San Francisco, is in the position of monitoring the traffic of lots of websites. And they observed a spike in traffic that immediately set off alarms and came to their attention.

What they found was a newly observed bot pounding on the websites of nearly a thousand companies offering gift cards which allow legitimate users to check their balances. So someone gives you a gift card for Amazon, for example, or for Domino's Pizza, who knows. And so often those sites have a page where you're able to turn the card over and enter in the gift card number and look up the balance that has been electronically transferred or assigned to that card. And armed with that, because that's essentially the gift card number is the only authentication needed, because the idea is someone gives it to you and says here's, you know, 50 bucks on a gift card. Spend it on pizza. And so that's what you do.

Well, unfortunately, once again, we attack where the money is in cyberwarfare. And so there is now something that has been called the GiftGhostBot, which is pounding on gift card supporting or issuing websites, brute-forcing millions of gift card account numbers per hour. In one case, this Distil Network monitored more than 4,000 guesses in brute-forcing in the course of one hour, and so determining the card number, getting the balance available on the card. And then, if found, the cards can be used and are used. Essentially, the balances are drained one way or the other, used to purchase goods at the site; or, in aggregate, bunches of the card data is sold on the dark web to people who then resell them in order to drain the balances.

So for a cyber thief, the beauty of stealing money from gift cards is that they are inherently anonymous, and it's untraceable transactions once they've been stolen. So the advice to people who may have received gift cards without standing balances is, if you can, not leave the money unused because the whole point of this GiftGhostBot is to pound on the website, crack the card number that is yours, find a balance, and then either use it immediately or send it off somewhere to be used by other crooks somewhere.

So the problem, of course, is that there had been little protection for this. In response to this attack, companies are starting to take their easy lookup, you know, look up your balance pages offline in order to prevent bots from abusing them. And so you may have to now make a phone call in order to check your balance. At the same time, if that page is offline, then it's likely that the bot can't get it. So what you may do, if you have any - if you know you have any gift cards you haven't used, is just go see whether you're able to check the balance online. If you are, that's a problem. You want to make sure you still have a balance and that the bot hasn't already drained it from you without you suspecting it. And, if so, you probably want to do that yourself before the bot can.

Retailers will likely install CAPTCHAs. This is someplace they should have put CAPTCHAs before, where, like, for example, all the other sites where you can create accounts and are doing something sensitive which had been previously subject to bot attacks have done so. Now it's going to be the gift card sites that do that.

And I should mention also this is a pretty sophisticated bot campaign. The bot itself masquerades its queries by rotating among more than 740 different user-agent simulations. So it just doesn't look like the same thing making a web query every time. It's captured at least 740 different profiles of ways browsers can query, and it chooses them and rotates among them at random so it doesn't look like a bot repeatedly doing the same thing. It's widely and heavily distributed across various hosting providers and datacenters throughout the world. So it's not just coming from one IP that would be easy to block. And it's able to execute JavaScript, which it receives from the website, in its pseudobot client in order to fully appear like an actual web browser that a user is using. So, I mean, so this is a sophisticated piece of work because apparently there are a lot of people with outstanding balances on gift cards, and this thing's just going to go out and find them all.

JASON: Yeah, you get one of those gift cards, I mean, there's no urgency whatsoever.

Steve: No.

JASON: I discovered one not too long ago. And I was like, wait a minute, I don't even remember getting this. You run it through, it's got a balance, excellent. So one question I have about this. If it's already happened, and it's untraceable because gift cards are very anonymous, as you say, how does the merchant know that a customer that happened to is telling the truth when they say, hey, I have no balance?

Steve: You are exactly right. And the problem is none of these cards have fraud protection, unless Visa and MasterCard and American Express and so forth. The major credit cards will all hold you harmless in the event of fraud against your card. But you're exactly right, there is no way for you to prove to the site that you didn't get the cash. And the site will say, hey, sorry, we're out the money. We gave it to somebody. You're claiming it's not you. First of all, you have no way of proving it's not you. And so the loss is distributed among all the people who are holding gift cards with nonzero balances when they're zeroed. Basically it's like a debit card where your money is stolen from your account, and it's gone, unlike a credit card where you are protected.

JASON: Wow.

Steve: Yeah.

JASON: Basically this was a little more complex than a war dialer. Just a little bit.

Steve: Yeah.

JASON: This is like a war dialer on steroids.

Steve: Yeah, war dialer was quaint. What a quaint idea.

JASON: Exactly.

Steve: So what's not quaint is what you're just about to take us into, Jason, is Microsoft's very disturbing default settings for documents uploaded to its Docs.com site, D-O-C-S dot com. Over the weekend, users were very upset to discover that documents they had uploaded to Docs.com were publicly visible and searchable through the Docs.com search. And to this day I don't understand what Microsoft was thinking. If you use Docs.com, which you're able to to connect with Office 365, as your iCloud repository for Word and Excel and other similar documents, those are private by default. You can choose to share them publicly, but you have to do that deliberately. Inexplicably, if you upload documents to just store them there, too, they are public by default.

And in the show notes here I have a screenshot of the settings page for a user. And in the third section under "Content I Like," there's one checkbox that says "Allow everyone to see documents and collections you like." And it's enabled by default. So this wasn't a mistake. This was what Microsoft thought people wanted. And the problem was, I mean, it's not even clear to me what Microsoft's actual policy is on this because they immediately reacted by removing the Search bar in order to presumably protect people from being able to use that in order to search. The problem is, they were publicly posted. So Google and other search engines all sucked them in and archived them.

I mean, so like these things are, you know, the famous expression is "Once you put it on the Internet, you can never get it back." And so this happened by mistake. In the various coverage of this over the weekend, some news outlets looked at - and also the original discoverers of this looked at what was there and found, for example, a list of maintenance logins and passwords for a number of devices, including metal detectors and other security devices; a list of names, addresses, Social Security numbers, bank account numbers, email addresses, and phone numbers, apparently passed to a debt collector on behalf of a number of payday loan and finance companies; medical data, including one physician's treatment logs and photos, as well as credentials for logging into medical records systems; a new employee enrollment document with instructions on how to connect to a corporate Intranet gateway for the first time, with default username and password information; employment acceptance letters; investment portfolios; divorce settlement agreements - I mean, you can't make this stuff up. Credit card statements. Files containing - multiple files containing login and password information, saved as Word documents. So major privacy breach.

And in response to this, Microsoft says, officially: "Docs.com lets customers showcase and share their documents with the world." Uh-huh. Yes, indeed. They said: "As part of our commitment to protect customers, we're taking steps to help those who may have inadvertently published documents with sensitive information." Gee, I wonder how that happened? "Customers can review and update their settings by logging into their account at www.docs.com." Wow.

JASON: I mean, I'm looking over the FAQ, and I'm looking at kind of the landing page for Docs.com. The landing page says to upload your documents. "Later, you can choose who may view your documents," which tells me that there will be some sort of element or step in there...

Steve: Proactive. Proactive.

JASON: ...before it kind of goes out to everyone. But then when you actually dive into the FAQ, you know, it repeatedly says, like, this is about getting your work noticed for a broader audience, posting it publicly for everyone to see. It seems to me like, I mean, maybe a service like Docs.com that's all about publishing documents for the public to see deserves to exist. There just needs to be better education on Microsoft's part to say this is what it's for. You might want to think twice about sharing certain types of documents because it's going out to everyone by default.

Steve: Yeah, it's called a blog. No one thought they were blogging their employment contract.

JASON: That's true, obviously.

Steve: When they uploaded it.

JASON: Yeah.

Steve: Oh, goodness. Just a bonehead move. Oh, boy. Just crazy. Anyway, so the bad news is that stuff is out there. The good news is hopefully, you know, Microsoft is being as proactive as possible. But once the search engines index it, you can't ever get it back, essentially.

JASON: Yup, yup.

Steve: Wow.

JASON: Okay. So I've been very curious to hear your thoughts on the next couple of stories. We have, of course, last week's terror attack in London, which, horrible event, I think everyone would agree. In kind of response, the U.K. government's stepping up its efforts to, well, I guess weaken or break or give us some sort of a backdoor into encrypted communications. Tell us a little bit about this.

Steve: Yeah. And of course just last week we had the four people killed in Westminster, which again reamplified this. So the U.K. government is once again rhetorically upping the rhetoric, pushing for access to all encrypted communications and has singled out WhatsApp specifically. Or as ZDNet phrased it in their coverage: "The U.K. government is gathering itself for an assault on end-to-end encrypted messaging services, demanding that providers, including WhatsApp, offer intelligence agencies access to content following the London attack."

So last week, following the attack, the U.K. Home Secretary, Amber Rudd, said there must be - and we've heard this before: "No place for terrorists to hide." And it's important for spy agencies to have access to the encrypted messages sent by the terrorists; or, or failing that, a future way to do so. Rudd said that providers of end-to-end encryption services such as Telegram, Signal, and WhatsApp provide a "secret place for terrorists to communicate with each other," and such services are "completely unacceptable. We need to make," Amber said, "sure that organizations like WhatsApp, and there are plenty of others like that, don't provide a secret place for terrorists to communicate with each other."

Continuing, she said: "It used to be that people would steam open envelopes or just listen in on phones" - yes, those days were quaint, too - "when they wanted to find out what people were doing, legally, through warrant. But today," she says, "we need to make sure that our intelligence services have the ability to get into situations like encrypted WhatsApp."

And so as our listeners know, this is why I suspended work years ago on my own, I called it CryptoLink. I still have the domain, CryptoLink.com, and I have the trademark. But I stopped working on it because I was reading the handwriting on the wall, from the saber-rattling that we were seeing in the U.S., that our government and the crypto community were going to be coming to blows. And I didn't want to be in a position of having invested hugely in a truly super-secure encrypted networking solution. It was going to be my version of a VPN where it just worked, I mean, it just like did everything right, and it worked. But the problem was I didn't want to be in a position where the government could say, hey, Gibson, you need to let us into this. This is the position that all of these communications, these secure end-to-end encrypted communication companies are now facing.

So I don't know what's going to come of this. We spoke last week about, no, a week before, I guess, yeah, about Vault 7. And my takeaway from that was the fact that the NSA with the Snowden disclosures and then the CIA with the Vault 7 and WikiLeaks disclosures had demonstrated, if nothing else, they were unable to keep their own secrets. So how can we possibly trust them to keep any sort of a master backdoor key secret? They've demonstrated they can't. I understand that they want more access to encrypted communications. The fact is the Vault 7 documents also demonstrate they have ways to get that, even in the case of Signal and Telegram and WhatsApp. And specifically, Telegram and WhatsApp were both singled out in the Vault 7 documents as they have a way to get that by either intercepting before it's encrypted, or intercepting after it's decrypted at either of the endpoints.

So again, I don't think this is going away. The reason I wanted to just bring this up again is that, once again, another terror attack is used as an opportunity for the government to, in this case, the U.K. government to say the way things are today cannot stand. And the technical community has to push back, as it and we have been, saying the way it is now is the way it has to be.

The only give that I think makes sense is for legislation that I expect to happen to force individual companies to provide some individual means on an individual basis, that is, not some master key, not some golden key that a third party can independently use in order to surreptitiously decrypt, but continue to force, at least as is the case in the U.S., to get a warrant from a judge proving reasonable cause, go to a company like Apple and say, "We have a warrant, and we also have some new legislation which says you must be able to provide us visibility into this particular person of interest's communications." We know Apple can do that.

Bill Gates famously was asked by Charlie Rose a couple months ago, I happened to watch the interview, Charlie's very interested, he's an iOS user, said, "Can Apple see people's communications?" And Gates said, "Yes, of course they can. They control the iOS. They can do anything they want. End of story." And so I think that - I think, much as I don't even like that, given the fact that law enforcement needs to see into communications, this is what I expect to have happen is that we will see some legislation. And in fact this next story, speaking of legislation, leads into that perfectly. And I made the little quip, this is not my own, I saw somebody say this on the 'Net: "'ISP' may soon stand for Invading Subscriber Privacy."

Last Thursday the U.S. Senate voted to eliminate broadband - new, that is, rules that were imposed under the Obama administration in October of 2016. The U.S. Senate voted to eliminate broadband privacy rules that required ISPs to obtain consumers' explicit consent before selling or sharing web browsing data and other private information with advertisers or other companies. Those original rules, as I mentioned, were approved in October 2016 by the FCC's - our U.S. Federal Communications Commission - leadership, which was at the time in the hands of the Democratic political party here in the U.S. But those rules are opposed by the FCC's new Republican majority and the Republicans in Congress.

So using its power under the Congressional Review Act to ensure that the FCC rulemaking "shall have no force or effect" and to prevent the FCC from issuing similar regulations in the future, the vote was 50-48 split straight down party lines. But because the Republicans are currently the majority in the Senate, that's the way it went. Of course, they also have a - we also have a Republican majority in the House. And the way legislation works, both of those congressional bodies need to vote on legislation. Then, if there's any difference between the legislation, that gets worked out. And then, finally, the President signs it into law. All of which is expected to happen.

So the only silver lining here is that all an ISP can see of encrypted communications - almost all of which is now the case thanks to Let's Encrypt, thanks to the NSA Snowden revelations a few years ago, which hugely increased the rate at which we moved into TLS connections and HTTPS - the only thing the ISP can see is our DNS queries. If we're using their DNS servers, well, then they know exactly what domains we are looking up.

If we're using somebody else's DNS servers, but we're not encrypting the DNS using DNSCrypt, for example, then they're able to see the DNS traffic moving through them on its way to us. So that's sort of metadata, inasmuch as they're not seeing what we are sending and receiving, but they do know to whom we are sending and receiving it. And if we're not using a VPN, they're also seeing the IPs to which our traffic, the public IPs to which our traffic is going and coming from. So if they look the IP up, they can see what website we're visiting.

So again, it's not clear what they want to do. In the same way that I fear we're doing to see legislation in the future that could compel encrypting companies to provide, to be able to respond to warrants, I greatly fear the day when part of subscribing to an ISP, like Comcast or Cox or any of the others, will require us to accept their root certificate, which would then enable them to run a TLS decrypting middlebox, as we've called them, to decrypt our traffic on the fly, specifically for the purpose of then getting into it. And then that requires us to trust them and all of their employees and the behavior over time of their organizations. And that's horrifying because our ISP is a single point of failure for all of our traffic and all of their customers' traffic.

The advantage we have now is where we're talking to all these different websites, if a given website loses control of its certificate, then it's only that one site whose traffic is potentially exposed. But if an ISP does this, it's a nightmare. But again, this really does look like the way things are going, which is not good news.

JASON: With a House vote right now, possibly. But I know it's supposed to happen today, so we're going to hear about it tonight.

Steve: Yes, yes. I wouldn't be surprised if it does - I expect it to pass. I think that they - no, and of course it's in the guise of this "less government and less regulation." So this is all part of that. Trump famously said, you know, for every one new regulation, we're going to remove two. And it's like, okay. I don't know that you can just count them like that. But that's what he's doing. So the goal is less government involvement in regulation. And so they're trying to deregulate this. Unfortunately, some of these things are good because ISPs don't clearly have our privacy rights in mind. They want to monetize what they see us doing.

JASON: And, I mean, there are good, there are ISPs that are seen as being better in this regard versus those that are clearly not. So there will, I mean, I guess there will always be a market for the ISPs that dedicate themselves to not following the herd in this regard; right? And I guess you just have to hunt those out and go with them.

Steve: Yeah, and I wonder also if we're going to see ISPs becoming VPN hostile because the other thing you can do, of course, is run out through a VPN, and then they're unable to see anything that you're doing. You're just this pipe of pseudorandom noise is all they see. Now, of course the VPN has its own problems because the endpoint where you terminate is where all of the traffic for all of their customers comes out. And that's a perfect place for the NSA to stick some of its taps, if it wants to see what's going on. But then again, at least then, if your traffic is encrypted, you're getting it out of your ISP's control. Anyway, yes, lots of interesting activity in the security world.

JASON: That's the cheery news I was looking for. Thanks, Steve. No, I mean, this topic, man, this topic just keeps coming up and keeps getting crazier and crazier.

Steve: And that's the problem is I don't think it's going to go away.

JASON: No, I don't think so either. And it goes hand in hand with the encryption topic, as well, and the reduction in Net Neutrality laws which, I mean, the ISPs can understand when they're seeing potentially encrypted traffic. Could they, at some point, make some sort of - draw some sort of line in the sand that says, if it's encrypted traffic, we throttle it to death? Or something like that. There's probably a lot of unintended consequences, if you go that route, just make life really difficult for those using encryption.

Steve: Yeah, in fact it's not practical. You could throttle a VPN, but you could not throttle HTTPS because 100% is HTTPS now. I mean, all of the sites, all of your use of Google. GRC won't let you connect to it without HTTPS, nor will an increasing number of sites because, you know, we're all moving to HTTPS all the time.

JASON: PCGuy8088 in chat says "Breaking: House narrowly votes to repeat broadband privacy rules, 215 to 205."

Steve: Yup, right down the party line.

JASON: Yeah, there you go.

Steve: Okay. And so there's no doubt that our President will sign it, so what happened in October '16 will be reversed.

JASON: And so then we go back to the way it was prior to the rules? And if that's the case, was life bad on the Internet then? You know what I mean? Are we now at this point venturing into uncharted territory? Or we've already been here before, we just understand more now why that's not good?

Steve: Okay. So what the legislation that was put into law in October did was it was going to require ISPs to get individual customers, that is, subscribers' explicit permission. And so now they won't have to. They'll be able to silently look at our traffic. And, of course, they know who we are. That's the other problem. It's not like a website where they're able to say, oh, you know, the cookies are anonymous, and we don't know who you are. We're just aggregating this anonymously. No, you have a fiduciary relationship with your ISP. They have your billing information. They know who you are. And now this law allows them to take our behavior, connect it to us, and monetize that, sell it to advertisers, without our permission.

JASON: Crazy stuff.

Steve: Yeah, it's a little annoying.

JASON: Yeah, just a little bit. "Annoying," I don't know if that's a strong enough word, just to be honest. I feel like "annoying" is kind of light.

Steve: So we talked about how LastPass has been so good about responding to problems found. The flipside of this, unfortunately, of this typical good behavior was just shown to us by Nest. Overall, Nest has been a disappointment. And it appears to be a classic instance of beauty only being skin deep. I immediately fell in love with that thermostat because it was gorgeous. I think, you know, if they have nothing else, they have an amazing industrial designer because that Nest thermostat is just - it's a piece of art. I mean, it looks like something that came from Apple, as opposed to some random startup.

But from all accounts, Nest's CEO is extremely difficult to work with. And their corporate and product performance has disappointed many. Last summer Ars Technica covered, I think it was in June of last summer, they had a headline reading: "Nest's time at Alphabet: A virtually unlimited budget with no results. Nest quadrupled its employees, launched no new products, and caused constant bad PR."

So anyway, back in 2014 Nest purchased Dropcam, an acquisition which itself has not gone very well. Dropcam's people were not happy. A whole bunch of them quit. But Nest has now a camera, thanks to purchasing Dropcam. Well, back in, when was it, October of last year, security researcher Jason Doyle was poking around the Nest/Dropcam devices and found some troubling problems. Nest sells these cameras as security cameras, the Dropcam, now Nest cameras. Yet it's trivial to cause them to drop off the network, effectively blacking out the region the camera was designed to observe.

And it's worth noting, as we've said before on this podcast, that the very phrase "wireless security" has big problems and is a self-contradictory oxymoron. My own home security system, as are all professional security systems, is low tech and hard wired. Yes, it's more expensive to install. And it's harder to install. But by being wired, you're not relying on the ether to cover the security signaling over the air that all these little things that you just stick on your windows are doing. And we've previously talked about the problems of jamming these systems and how possible it is to do that.

Well, Jason discovered three different denial of service, or maybe in this case it would be, instead of DoS, it would be a DoV, Denial of Video problems that he named Bluetooth-based buffer overflow via SSID parameter, Bluetooth-based buffer overflow via encrypted password parameter, and Bluetooth-based WiFi disassociation.

In the first case, it's possible to trigger a buffer overflow condition when setting the SSID parameter on the camera. The attacker must be within Bluetooth range - but of course that's 40 feet, 10 meters typically, or 30 feet at least, and longer if you use a directed antenna. So the attacker must be in Bluetooth range at any time during the camera's powered-on state.

Bluetooth - and here's one of the big problems - is never disabled, even after setup. So this is one of those devices, an IoT device that has Bluetooth for setup and WiFi. Yet, for reasons that it's difficult to understand, maybe they just didn't want to have an extra button on the back where you would press it in order to enter setup mode, and then the Bluetooth would disable itself until you pressed the button again. Anyway, Bluetooth is always on. Which means at any time, as long as a bad guy can get within Bluetooth range, they send a packet to the camera or cameras and knock it offline by triggering a buffer overrun in the handling of the SSID parameter.

In the second case, the same thing can be done with the encrypted password parameter. Shoot that into the Nest cam, and it knocks it offline. Now, in both of those cases it will reboot, but you have about a minute and a half before it comes back. And of course you can do it again if you want.

In the third case, it's possible to proactively give the camera a new valid SSID, which it will then attempt to switch to. If you have also provided it with a bogus access point, it'll associate with that one and just sit there happily forever after. If you don't give it one, it will wait about a minute and a half and then finally decide, okay, that must have been spurious, and switch back. So again, you've got about a 90-second blackout, or an infinite blackout, if you camp it on some other WiFi access point that, for example, you just brought along with you.

So, again, I never have problems with anyone making a mistake. Now, I have a problem with policy versus a mistake. And I would argue that the policy of leaving Bluetooth enabled for a WiFi device, that's something that is indefensible. They should have simply had a little button on the back that temporarily enables Bluetooth until you're through the configuration and setup, and then it shuts down. But they wanted to make it even easier to use. Oh, just sort of magical, so you don't have to press any buttons. Yes. And unfortunately, neither do the attackers.

So there's a policy problem there. But everybody knows mistakes happen. But what matters is the way they address those mistakes. So Jason - it was Jason; right?

JASON: Yes.

Steve: I think that was his name. Yes, Jason Doyle.

JASON: Every time I read the name Jason...

Steve: No, wait a minute, that's also my co-host today. So he informs Nest on October 26th, reporting the security bug through Google's vulnerability reward program guidelines. On October 27th, Google's security team acknowledges the report was received and being investigated. On November 1st - this is all moving along perfectly - Google's security team validated the reported vulnerabilities and filed the bug. Two weeks later, November 15th, Google's VRP panel issued a $100 reward under nonintegrated acquisitions, so Jason gets a little token $100. Then four months goes by with nothing happening.

Finally, out of frustration, on March 17th, Jason goes public with his disclosure, and Nest scrambles around saying, oh, oh, oh, oh, we'll get this fixed immediately. That is not the way you want a company whose products' security you care about to act. This is an example of the worst possible action. The problem was reported responsibly. The receipt of the report was verified. The problem itself was verified. And then four months goes by with no action at all until a public disclosure forces their hand.

Gizmodo, reporting on this, wrote: "Now that the code for the exploit has been published, a motivated and knowledgeable burglar could theoretically use it on your home tonight. If you own one of these cameras, the only real bulletproof solution to avoid the flaw is to disconnect them until Nest pushes a software fix. Of course, disconnecting a camera doesn't exactly make you any safer. Given that Nest has not updated the firmware in over a year, that's cause for concern. Let's hope they hop to it with a fix."

JASON: Yeah. What this screamed to me is like we hear about IoT security over and over again. I mean, this past year it's been a recurring issue. And then I look at this, and I'm like, god, even IoT hardware owned by one of the largest companies in the world, Google, can't get it together to tackle something like this with urgency. I mean, that's a great issue for all, but it's an even greater issue when a company like Google can't pull it off, or chooses not to.

Steve: Right. Well, and in fact we have an acronym on the podcast - we have many because we like them. IDIOT stands for I Don't IOT. Because it's just not very secure to do that these days.

JASON: So you don't have any IoT devices in your home.

Steve: Do I?

JASON: Any Hue light bulbs?

Steve: I don't think I do. I don't think I...

JASON: It's be really hard for me to get rid of my Hue light bulbs.

Steve: Those light bulbs, though, those are malware bait.

JASON: Oh, great. Excellent.

Steve: Yeah.

JASON: Ugh. They've got to get their stuff together.

Steve: Anyway, so this week in I Don't IOT we have the report of a dishwasher/disinfector, I guess it's the Miele Professional PG 8528. I saw a photo of it, so it's not something you're going to have in your kitchen, that's the good news, or at least not this version. This is more of an industrial commercial size thing. But it turns out that it is apparently based on some sort of an embedded Linux, and it has an embedded web server that identifies itself as the PST10 WebServer.

There's a classic web server flaw that actually IIS, Microsoft's web server early on had, which is called a "directory traversal" bug. As anyone who's used the command prompt in any of our OSes know, dot refers to the current directory, and dot dot refers to the directory one level up or back the directory hierarchy. So a common attack is to say GET /../../../. And you keep doing that maybe, doesn't matter how many times, like 12 or 13. And so what that does is, when a web server that hasn't been protected from this sees that, you don't know what directory the web server root is in. That is, the web server's root, where you'd have like the default home page, that's not in the server's root. That's in, like, maybe /www/myserver or something.

So that's in a subdirectory somewhere. And so that's the root. So if you tried to access a file on the root, it would be looking for that file in that subdirectory. But for servers that haven't protected from this - and by the way, this has, like, got to be one of the oldest web server bugs there is, is you do this /../../... What that does is that walks the GET request back up the file hierarchy to the actual server root, out of the web server root to the actual server OS root. And then in this instance the guy who found this said /etc, you know, E-T-C, then /shadow, which allowed them to have the server retrieve for them what's known as the password shadow file, which then allows you to get access to the passwords in the OS. Linuxes use this for additional security.

But it's just nuts that any server, any Linux web server that anyone could write in this day and age would be victim to this simple directory traversal attack, which has been well known, as I said, literally for decades, probably for 20 years. And so in this proof of concept, this dishwasher has a web server open on port 80 of its IP. And anyone who is able to arrange to get to port 80 is then able to issue a simple GET request, obtain the passwords for the server, and then of course presumably it's got Telnet listening. And so then log into the server, get the admin credentials - because in this proof of concept we're seeing the root password entry from the file.

And then lord knows what it's going to do. Maybe flood the kitchen by turning, I mean, you know, you have an operating system that has full control over your dishwasher. It's probably, you know, this OS is probably running the various motors, the pumps, the valves. And so you could get up to any kind of mischief like this. And the way into your kitchen, by the way, Jason, would be through your light bulb.

JASON: Oh, okay.

Steve: So that's the way...

JASON: So what you're telling me is don't get this dishwasher. That's like the overarching rule. There's nothing more important than that one rule. Oh, wait a minute, no. Probably starts with a light bulb. But I - they go all sorts of colors, Steve. That's really difficult, for me to give it up.

Steve: I know, they're very seductive.

JASON: And I can just push a button on my phone, and it turns colors. Like that's so cool. But I know. I get it.

Steve: So a friend of the show, Simon Zerafa, sent me a fun tweet, forwarded from Jerry Gamblin. He said: "Sometimes hacking is just someone spending more time on something than anyone else might reasonably expect." And of course, you know, that ought to be the byline of this podcast. I mean, that's what we keep seeing over and over. Tavis is thinking 24/7, even when he's showering, about how to get into LastPass, and coming up with new and clever ways to do that. "Sometimes hacking is just someone spending more time on something than anyone else might reasonably expect."

And we've also talked about how the reason or the way the CIA was able to develop this stuff is on one hand, they were just scouring all of the public fora and conversations, looking for some way, you know, for all the different ways people were finding of getting in, and aggregating them. And presumably they've got a big budget, and so they're paying people to be hackers, to spend their time looking at this, at the targets of opportunity, much more than anyone might reasonably expect. And of course we saw the same thing with that crazy iOS security batch of fixes. Somebody, a whole lot of different somebodies, took the time to find the problems.

JASON: That's the reality of technology as it stands right now. Somebody needs to spend that much time poring through the minutiae. And thankfully there are people that enjoy that. I'm not sure [crosstalk] enjoy that minutiae.

Steve: Yes, and for the well-secured things, like today's browsers and OSes and VMs, it is much more difficult now. Now you've got to string five or six different vulnerabilities together to create a serialized exploit in order to get something done. So, I mean, you've really got to have your propeller well wound up on your beanie in order to be able to pull this kind of thing off.

JASON: It's going to be really, really long shower.

Steve: So, yes. So a couple bits of miscellanea and some quick dialogue with our listeners. We've been talking for the last couple weeks about Conway's Game of Life. A number of people mentioned to me that Google was already ahead of the game. We were talking about apps for that last week. It turns out, you google "Conway's Game of Life," Google runs it on the page of answers that comes up, which I thought was just so fun. You don't even need an application. You just C-O-N-W-A-Y-'-S, "Conway's Game of Life." And so for anyone who hasn't even bothered to grab an app, just google "Conway's Game of Life."

JASON: Oh, yeah.

Steve: And actually I watched it for a while yesterday. It's very cool. You'll see some loafs and some blocks. Some gliders get spontaneously created and go sort of shuttling themselves off the page, and blinkers, and stoplights, and all kinds of classic Game of Life structures get created. So nice going, Google.

JASON: Sorry, I'm lost. I'm staring at that life flash before my eyes on a Google search page.

Steve: So several people have asked me, because we've been talking about one-time tokens, and in fact we were just mentioning - I didn't have it on-hand when I mentioned it last week. But we covered the news that eBay was officially discontinuing the use of this, what we always called the "football" because it's sort of football-ish shape. I still have mine, and mine still works. I push a button, and up comes a little number there.

And it's funny because I knew that we would have a problem if the battery died. Apparently you cannot change the battery in this without losing the code which is only stored in RAM. It's not stored in any kind of an EPROM. So I wouldn't even let it, like, timeout itself. It actually - I would look at the code, quickly memorize it, and then turn it off again in order to preserve the battery. So consequently mine is still working after all these years. But eBay was sending people news over the last couple weeks that they're increasing the security by discontinuing the use of the football.

Well, that was the time-based one-time password. They're now switching to an SMS-based password. And so several people have asked me, "Will the football still work? Or will it stop working," he says in this one case, "because I don't want to change to the SMS version." And the bad news is Google was paying VeriSign, which became Symantec. I think, I don't know whether Symantec purchased the identity portion of VeriSign or only the domain registrar portion of VeriSign. But eBay was paying per authentication, which I think is probably the reason that they've stopped supporting that.

They could certainly have switched to what everybody else is switching to, which is the software-based time-based token, the TOTP, Time-based One-Time Password, rather than going SMS. I just think they're not that concerned about security. I mean, so they're like basically backing off from the best security, which was to allow people to use a hardware token, to the least secure of the second-factor authenticators, which is SMS.

JASON: Well, okay. So speaking of this, there was Instagram news late last week that Instagram now supports two-factor authentication. I went in to set it up today. And sure enough, the only way that you can do it through the Instagram version is by SMS. Why do some companies choose, because I would prefer to have it all inside an app and not have my SMS code being flown around everywhere, why do some companies choose not to do that? Why do they stick to SMS, knowing what they know?

Steve: I think it's for the same reason that some companies say that your password can only be a certain length, or it's not going to be case-sensitive. Case-sensitive passwords are much stronger, but they're more trouble-prone. And so by saying, oh, your password's not case-sensitive, they think that'll make it easier for their users. Unfortunately, it's at the cost of security.

So I think that SMS is easier to use than an app. But the tradeoff is, and in fact this came up for me a few months ago, we were talking about this because I've switched away from Network Solutions. I've switched to Hover as my domain registrar. And when I was setting up, they gave me the option of SMS or a time-based one-time password. Of course I went with time-based because it's fundamentally more secure.

The problem with SMS is that, on a per-login instance, you're using your insecure cell phone network to send you an SMS message. And we know cell phone networks are not secure. So it is way better than no second factor, but it is the least secure of the several second-factor alternatives, the most secure being that one time the website gives you a code, which then is used to key a software authenticating app, and you only need one of those apps because they're all able to store multiple keys. And the beauty is then on a per-login basis, they're not sending you anything. They're just asking you, based on the time of day, what is your app currently showing you in a 30-second period, enough to see it and type it in.

And in fact several people liked the tip that I gave last week. We were talking about this, and I said, you know, the problem with these authenticating apps is none of them will export that key. They are all write-only. You cannot read the key back out. So what I have taken to do is, because I have four different sites that I am now using the time-based token with, is when the QR code is displayed on the screen, I print that piece of paper. I print the page.

So I now have four pages containing the four QR codes. That way when I'm setting up a new device, and I'm just using Google Authenticator because I like how many it lets me put on one screen, you know, there are a bunch of them. They're all compatible. You choose whichever one you like. Leo likes, I think it was Authy. And that one does cloud synchronization, which again is a convenience tradeoff for security. I'm not putting my master time-based tokens in the cloud. The whole point of having them is not having them anywhere anyone can get them.

So I like Google's Authenticator. And in fact, in a dialogue I was having with someone, he said that when his Android device, he has a Samsung, and he said he wipes and reloads his phone from scratch rather than updating it, which he says he feels keeps it operating at peak performance. But that also means he's constantly having to reconfigure, re-set up his authenticator app. And so he loved my tip and recommendation from last week of just printing them on paper. Obviously, you need to store them securely. But that should be something you're able to do because we're not worrying about a home invasion. We're worried about somebody in Russia or China or somewhere else doing an online attack or a phishing attack or somehow spoofing us or intercepting our communications.

So the point is making it more convenient to use an authenticator I think ends up increasing your security. And so I have these four pieces of paper for the four sites that I'm currently authenticating against. And that number will grow over time as more people offer this feature because it's the best security available now, while we're still stuck using all of this ridiculous, how do we make our passwords more secure technology, until we're able to obsolete passwords completely.

JASON: [Ahem] SQRL. [Ahem]

Steve: Exactly. Which brings me to my next note here. What's the status of SQRL? Yesterday I just finished all of the server-side code. It's completely wrapped up. After the podcast today, I am going to work on the finishing details of the client, and then we will have something for people to play with probably pretty soon. While that's happening, I'm going to go back and catch up all of the online documentation to make it current with what the spec which is currently implemented in the software does. But that can overlap with people playing with it. So I just - I have no idea when. But it doesn't feel like it's far off from now. And I can't wait for everyone to be able to play with it and see what they think.

JASON: That's exciting. Everybody's waiting for that, too.

Steve: Yay. Me, too. So I had someone ask: "Apps like Google Authenticator support only the default HMAC SHA-1 version of the RFC," the time-based token RFC. "I don't think collisions matter here. Do you?" So he's noting that SHA-1 is a concern, as we just saw, because the first collision in SHA-1 was mathematically found after a huge amount of processing was performed.

And the answer is no. In an Authenticator app, we don't care about collisions. We're just using the SHA-1, a keyed SHA-1, that's the HMAC SHA-1, as a key-based pseudorandom number generator. So the secret key keys the hashed MAC, and then the time is put into it, and out comes an unpredictable number that changes every 30 seconds. And so in this instance we're using the SHA-1 as part of a pseudorandom number generator where collisions do not matter.

Someone else asked, and we referred to it earlier in the show: "Have you guys talked about DNSCrypt on Security Now!? If so, any comments?" And I've never done a deep dive into it. It does use my favorite encryption, which is the Bernstein 25519 curve. And DNSCrypt, D-N-S-C-R-Y-P-T dot org is the site where you can find it. I would say, if you want to hide your use of DNS from your ISP, and also bring the security of your DNS up a bit, DNSCrypt is today the way to do it. DNS is otherwise just UDP packets in the clear. There is no protocol encryption for DNS the way there is for HTTPS, for example. So everything you do with DNS is in the clear unless you wrap it in DNSCrypt, which is currently the only game in town, and I think a great solution.

Some guy asked: "Hey, Steve. While listening to Security Now!, you mentioned a small two-port router for isolating Internet of Things things. What was its name and model again?" Anyway, I have no problem remembering it because it's my initials. It's the SG-1000. And if you just put "SG-1000" into Google, that'll take you to the Netgate.com site, where this, I mean, it's just an adorable little thing, which is able to run the pfSense router firewall, and which you're able to use for really good network isolation.

And then, finally, someone said: "FYI. Don't know if you're watching. 'The Good Fight' continues to explore technology and the Internet like 'The Good Wife' did." Back when "The Good Wife" was on CBS, we were talking often about they had some fun episodes where some guys at the NSA were listening in on the various conversations going on in the law firm. I did watch the first episode of "The Good Fight," but it's CBS All Access. And I love to binge watch serialized shows when they're available, and there's nothing else that I need CBS All Access for. So I'm just going to wait till the end of the first season, and then I'll sign up for the free week and watch "The Good Fight" all in that week and then unjoin because they let me do that. But I did watch the preview, and I loved it.

JASON: I haven't heard of it.

Steve: Huh?

JASON: I haven't even heard of that show. No. And I never saw "The Good Wife." I did hear a lot of good things about it, especially [crosstalk].

Steve: "The Good Wife" was a great show. And this is basically, they called it "The Good Fight." So it is a continuation of "The Good Wife." But they decided, okay, we're going to make people pay for it. So it's like, ah, okay. Not me. I'll wait till the end.

And finally, I love this note from a listener and SpinRite user because this is the textbook perfect way of using SpinRite. Someone named Alfred wrote to me, and he said: "Hi, Steve. I've been a long-time listener and a long-time regular proactive SpinRite user. I have never lost any data yet," and he says, "knock on wood. But I have always changed drives whenever I see that SpinRite is finding an unusually high number of incidents, as it has a number of times." Then he said: "Additionally, your podcasts and research in security and health have made me a healthier safer life. Thanks."

So I just wanted to mention that that's - I've said before, I understand that most people are going to purchase SpinRite when they are hit by a disaster, and SpinRite can hopefully bring them back. And that normally makes believers out of them. But Alfred is doing the best thing possible, which is periodically, like maybe every quarter, you know, quarterly, every three months, run SpinRite. And on the SMART screen it shows you lots of detail about the rate at which things like error correction are occurring. And so that is the most sensitive test ever created for metering the current health of your drive. And if you just took a note of the numbers that are shown at the end of a SpinRite run, and then looked at them every three months over time, you would notice if there was a change. And on a hard drive, change is not good. There's no way that a drive is going to change for the better. It's going to change for the worse. I mean, if the numbers go down, that's sort of a miracle, but okay. Probably they're going to go up.

And so what Alfred has done is when he's seen that happen, with hard drives being as inexpensive as they are nowadays, he just takes that as an early warning indication that things are not looking so good, and he moves his data to a new drive and continues. As a consequence, he's using SpinRite for maintenance, proactively, preemptively, and never had any data loss. So, yay. Thanks for sharing that, Alfred.

JASON: Fantastic. Yeah, data loss is no fun, especially when you realize you could have done something, and it would have been a heck of a lot easier prior to.

Steve: Oh, it's like...

JASON: It happens to you once, and then you change your habits.

Steve: Yes. Who hasn't gone ooohhh.

JASON: Dang it.

Steve: Gah.

JASON: You can't go backwards.

Steve: If only. If only.

JASON: Yup, exactly. All right, Steve. Tell me why Google doesn't trust Symantec anymore.

Steve: So, okay. Ryan Sleevi is another security researcher at Google. Good guy. I follow him on Twitter and watch his postings. He, well, the title of his announcement was "Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates." Which is cataclysmic. I mean, it's earthshaking for the industry, and arguably cataclysmic for Symantec.

As we've previously covered, back toward the end of 2015, in October, Google first discovered misissued certificates for itself and Opera. Remember that Google knows, Google's Chrome browser knows the fingerprints of all of Google's certificates explicitly, so-called "certificate pinning." And so the moment any Chrome user goes to any site that has a fraudulent Google certificate, Chrome phones home. Chrome immediately tattles and says, hey, Google, guess what I just found in the wild. So you can't get this over on Google. And of course now Chrome is the majority browser on the Internet, is the number one web browser in the world. And so Google has extreme vision into what's going on.

So three years ago, or two and a half years ago, they discover misissued Symantec certificates for itself and Opera. But subsequent research has since revealed that the problem was much worse. Google announced last Thursday that it will begin downgrading the level and length of trust Chrome, the major browser in the world, will place in certificates, that is, all certificates issued by Symantec. Now, this is my opportunity to tell everybody how glad I am I left VeriSign. Remember that Symantec purchased VeriSign back in 2015. And VeriSign, as a consequence of having been around from the beginning, from like the dawn of the Internet, had a market share of around 30% of the web at that time.

I was with VeriSign because they were the granddaddy, in the same way that I was with Network Solutions because they were the granddaddy over on the domain registrar side. And I have since left both. Everybody knows who's been listening to this podcast that, whereas all of GRC's certificates were once VeriSign, I made the switch to DigiCert and have never been happier in my life and have never looked back. And obviously I'm more happy today than I ever have been before.

I've met the DigiCert people. I've asked them to help me with all kinds of bizarre things that I can't even imagine even asking VeriSign or Symantec to do, like dual-issuing a certificate, both in SHA-1 and SHA-256, and expiring the SHA-1 on midnight of New Year's Eve a couple years ago so that I could keep Chrome happy with not having an SHA cert which was valid in, what was it, 2016, yet still allow people using XP service packs earlier than 3 to access GRC, which was only available over HTTPS. My point is, how could I ask, you know, VeriSign and Symantec couldn't care less. DigiCert made this all possible. So I am so happy that I made the move. And as everyone knows I recommend them without hesitation.

So Google has determined that Symantec has not been taking its responsibilities as a certificate authority seriously, and has issued - are you sitting down, Jason? - 30,000 certificates, not a handful, 30,000 without properly verifying the websites that received them. This is, of course, a serious allegation that undermines the trust users can place in the encrypted web. And Google says it will begin the process of distrusting Symantec certificates in its Chrome browser. Now, again, cataclysmic for Symantec. They, of course, lashed out at Google's claims, calling them irresponsible and exaggerated and misleading. To which I respond, yeah, uh-huh. Who do we believe here?

So Ryan wrote in his Google posting: "Since January 19, the Google Chrome team has been investigating a series of failures by Symantec Corporation to properly validate certificates. Over the course of this investigation, the explanations provided by Symantec have revealed a continually increasing scope of misissuance with each set of questions from members of the Google Chrome team. An initial set of reportedly 127 certificates has expanded to include at least 30,000 certificates, issued over a period spanning several years. This is also coupled with a series of failures," Ryan writes, "following the previous set of misissued certificates from Symantec, causing us to no longer have confidence in the certificate issuance policies and practices of Symantec over the past several years."

Ryan wrote that Symantec's behavior failed to meet the baseline requirements for a certificate authority, creating what he called "significant risk for Google Chrome users." Symantec allowed at least four parties access to their infrastructure in a way to cause certificate issuance; did not sufficiently oversee these capabilities as required and expected; and, when presented with evidence of these organizations' failures to abide to the appropriate standard of care, failed to disclose such information in a timely manner or to identify the significance of the issues reported to them. These issues, and the corresponding failure of appropriate oversight, spanned a period of several years and were trivially identifiable from the information publicly available or that Symantec shared.

Ryan wrote in another post that Symantec partnered with other CAs CrossCert, which is the Korea Electronic Certificate Authority; Certisign Certificadora Digital; Certsuperior S. de R.L. de C.V.; and Certisur S.A. that did not follow proper verification procedures, which led to the misissuance of 30,000 certificates. Ryan explained: "Symantec has acknowledged they were actively aware of this for at least one party, failed to disclose this to root programs, did not sever the relationship with this party." And he wrote: "At least 30,000 certificates were issued by these parties, with no independent way to assess the compliance of these parties with the expected standards. Further, these certificates cannot be technically identified or distinguished from certificates where Symantec performed the validation role."

He writes: "To balance compatibility risks versus the security risks, we propose a gradual distrust of all existing Symantec-issued certificates, requiring that they be replaced over time with new, fully revalidated certificates, compliant with the current baseline requirements. This will be accomplished by gradually decreasing the 'maximum age' of Symantec-issued certificates over a series of Chrome releases, distrusting certificates whose validity period - the difference of notBefore timestamp and the notAfter timestamp - exceeds the specified maximum.

"To restore confidence and security of our users, we propose the following steps: First, a reduction in the accepted validity period of newly issued Symantec-issued certificates to nine months or less, in order to minimize any impact to Google Chrome users from any further misissuances that may arise." So essentially over time, and I'll explain what the schedule is in a second, but over time they're going to start squeezing down from three years down to nine months, successively with future releases of Chrome. That will allow websites who now have Symantec certificates to get updated ones.

However, that will, over time, they will have to be updated to shorter and shorter durations, down to nine months. So essentially Symantec will no longer be allowed to issue a three-year cert or a two-year cert. The only certs that Chrome will honor when it gets to the end of the successive set of changes is any certificates from Symantec with a life that has never been longer than nine months.

He said: "We propose to require that all newly issued certificates must have validity periods of no greater than nine months, 279 days, in order to be trusted in Google Chrome." And that becomes effective with Chrome 61. I guess they're at 59. now. "This ensures that the risk of any further misissuance is, at most, limited to nine months."

And, see, this is the problem. Right now, unless they start mistrusting all Symantec certificates, since there's no way to determine where the certificate came from, they have to start throttling the duration of all of them in order to minimize the security risk. Because they found 30,000 of them, or evidence that 30,000 were misissued. But there's no way to determine on a specific certificate programmatically who issued it. So they have to treat all of them from Symantec, that is, signed by Symantec's master certificate as increasingly untrustable.

So an incremental distrust is what they're going to be imposing, spanning a series of Chrome releases of all currently trusted Symantec-issued certificates, requiring that they be revalidated and replaced. So with Chrome 59 (both the Dev, the Beta, and the Stable) that will only allow certificates to be 33 months old. Chrome 60 (all three, Dev, Beta, and Stable) reduces that to 27 months. Chrome 61, all three versions, to 21 months. Chrome 62 to 15 months. Oh, and Chrome 63 Stable to 15 months. Chrome 63 Dev and Beta will be a little more aggressive at nine months' validity. And then with Chrome 64, all three (the Dev, Beta, and Stable) will set the maximum, the acceptable certificate life from anything issued by Symantec to nine months. And they will be in that purgatory until such time as they demonstrate that they are able to responsibly issue certificates.

And then, finally, quoting again from Ryan: "Given the nature of these issues and the multiple failures of Symantec to ensure that the level of assurance provided by their certificates meets the requirements of the Baseline Requirements or Extended Validation Guidelines" - oh, I forgot this part, woohoo - "we no longer have the confidence necessary in order to grant Symantec-issued certificates the 'Extended Validation' status." So they are no longer, even if certificates are EV, they are not going to show that in Chrome.

"As documented with both the current and past misissuance, Symantec failed to ensure that the organizational attributes, displayed within the address bar for EV certificates, meet the level of quality and validation required for such display. Therefore, we propose to remove such indicators, effective immediately, until Symantec is able to demonstrate the level of sustained compliance necessary to grant such trust, which will be a period no less than a year. After such time has passed, we will consider requests from Symantec to reevaluate this position, in collaboration with the broader Chromium community."

Ryan finishes: "This proposal allows for web developers to continue to use Symantec-issued certificates, but will see their validity period reduced. This ensures that web developers are aware of the risk and potential for future distrust of Symantec-issued certificates, should additional misissuance events occur, while also allowing them the flexibility to continue using such certificates should it be necessary."

And so my take is Symantec got caught playing fast and loose, and rather clearly failed to appreciate that the privilege of essentially printing money by charging people for a pattern of bits comes with a significant and serious responsibility to assure the integrity of the identity assertions which are implicit for a certificate's holder. They screwed up, and Google's going to hold them to account. And I say bravo, Google. I mean, it's not easy. Google doesn't want to hurt Symantec, but Google's taking the trust implicit in certificates seriously. And I think they should. And I hope this serves as a lesson, not only to Symantec, I'm sure it will, but to the other CAs that are printing money and not earning the right to do so by being sufficiently responsible.

JASON: Any reason for other browser makers to follow suit in this regard?

Steve: It would be nice if they did. I'll be surprised if Mozilla doesn't. I would be surprised if Microsoft did. But again, being the premier browser, the majority browser, more than half of the Internet is using Chrome, that forces Symantec to change. You know, I mean, if Chrome doesn't - okay. And understand, this is driven at the web server end. Anyone using Symantec certificates is going to be inconvenienced by the need to update their certificates, and they're not going to be able to get a three-year or a two-year cert. They're only going to be able to get a nine-month cert.

So this clearly hurts Symantec significantly, which is why it's not something Google does lightly. I mean, this is a huge blow, but it's one that Symantec deserves. And what will happen is they're going to significantly lose market share. I mean, they lost me for other reasons, just because of who they were a long time ago, and I switched to DigiCert, and I'm obviously glad I did so. But this essentially forces other websites, either to, I mean, maybe they'll discount their certs in order to hold onto market share. But it's going to be an inconvenience for all the websites which are using today Symantec certs, probably just due to inertia, from the early days when they were using VeriSign.

And of course that's why Symantec purchased VeriSign because they're a money printing press. But they've demonstrated they don't have the discipline to have that privilege. And so websites are going to be switching away from Symantec or having to continually get new certs, if for some reason they decide to change. I think everybody should leave. And you know where I think they should go.

JASON: And I imagine it's a lot of work. Like when Google spells out issuing new certificates, I mean, that's a huge pile of work for Symantec to do properly.

Steve: Yeah, yeah. I mean, this is a big deal. This is, you know, this is, yikes. And you can't, I mean, EV. I mean, all of my certs from DigiCert are EV because we're GRC, and I want to have that look. I go through hoops with DigiCert to reverify that I am who I say I am, for the privilege of that extended validation that I want to have show on the browsers. And nobody who has an EV certificate from Symantec will get that any longer because we can't trust that the person holding that certificate from Symantec is who they say they are.

JASON: The prime reason you have a certificate in the first place.

Steve: Exactly. The only reason. That's what it is. It's just an identity assertion. It's an identity assertion.

JASON: Yeah. Explicit reason of existence. Thanks for explaining that. Is there any final thoughts before we wrap it up?

Steve: We're done until next week. And we'll have more next week for 606.

JASON: Right on. Steve, this is awesome. It's such an honor to get to do the show with you. And this is a lot of fun. You know, Security Now! is filled densely with information, some of it slightly scary because security can be a scary thing when you're talking about security and privacy and identity and all that online. But always fascinating deep dives, and I love it. So continue the great work. Really appreciate it.

Steve: Thanks. And Jason, you were great. It was great to have you. And whenever Leo takes a vacation, glad to have you back.

JASON: Just let me know. Just let me know, and I would be glad to hop in. Of course GRC.com, if you want to check in on all things related to Security Now! and everything that you're working on, Steve. SpinRite, of course, must-have hard drive maintenance utility we talked about a little bit earlier. Definitely go there if you haven't already, and a whole lot more: GRC.com. You can also find, I think, Security Now! audio, transcripts. You post those on the site, as well; right?

Steve: Yup, yup. And the show notes for this episode are already up and on the site for anybody who wants to grab them because the show notes have links and things for additional information.

JASON: Awesome. And you can find the show also on our site at the show page for Security Now!, that's TWiT.tv/sn, as well as anywhere you're going to find awesome podcasts like Security Now!. You're going to find them in the index. Just look for Security Now!, and you'll find it there. You can watch live, of course, every Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC at TWiT.tv/live. Just go to the page, select the service that you want to stream it from. They're all listed there, makes it super easy to hop in and join in real time. Thank you, Steve. This has been a lot of fun. Appreciate it.

Steve: It was a pleasure, Jason. Talk to you next time.

JASON: Will do. Leo returns next week. We'll see you next week on another episode of Security Now!.