New Year's News

Description: The last two weeks of 2015 generated so much news that this first podcast of 2016 catches us up on everything that happened since our last podcast of 2015.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-541.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-541-lq.mp3

SHOW TEASE: It's time for Security Now! A brand new year, and there's so much to talk about. Steve Gibson has the latest security news, some interesting tidbits and factoids, as always, about things like IPv6. I'll demonstrate, or at least the setup of, this Tiny Hardware Firewall, just came a moment ago. All that coming up next on Security Now!. Happy New Year.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 541, recorded Tuesday, January 5th, 2016: New Year's News.

It's time for Security Now!, the show where we save you and your loved ones from the perils of the Internet, thanks to this man, our captain, the man who sails the mighty ship Security Now!. It's Steve Gibson of the Gibson Research...

Steve Gibson: Or if we're not able to save you, at least when it all goes bass-ackwards you'll know why.

Leo: He's the guy.

Steve: It's not a mystery when suddenly something pops up and says, "All of your files are encrypted, sorry about that."

Leo: And Steve, I want to say this about you, and I really appreciate it. You're not an "I told you so" kind of guy.

Steve: No.

Leo: No. I am, though. And I will...

Steve: I don't have that.

Leo: No, you don't. You just say, "Oh, I'm so sorry." But you should be listening to the show. Then we don't have to say "I told you so."

Steve: That's a good point.

Leo: So what are we doing this week?

Steve: This week, because we skipped a week, there's just too much to talk about. So I just titled this podcast "New Year's News" because, as I was making notes, as events happened, it was one of those "a lot to talk about" weeks. So we just have a great podcast full of everything that happened since the last, since two weeks ago when we left off on 539. 540 was our holiday episode. And I have to say I got a ton of positive feedback from people who really appreciated hearing the Vitamin D podcast from '09, I think it was, six years ago.

Leo: You know what we didn't realize is that there was no video of that show.

Steve: And I watched your introduction to it, and you were explaining that this was, you know, I was reluctant to aim a camera at myself. And look, you can see why. And so you were moving to video, and I was saying, eh, everybody's listening to this. Why, you know, why...

Leo: Well, you were right. I mean, there's no - it's talking heads. You don't need video. But it's funny because it wasn't that long ago, and yet there is no video version exists.

Steve: I will say, though, that you were correct in predicting back then that bandwidth would expand, capacities would expand. I mean, it was a bigger pull originally to get video. Now it's websites are showing it to you without asking for it. So obviously this has - it has changed, and it's become a lot easier to get to.

So all kinds of things happened. We've got an update on the Get Windows 10 (whether you want it or not), a Windows 10 market share snapshot, some hysteria over the news of Windows 10 sending disk encryption keys, your disk encryption keys to Microsoft, and why it's actually not a surprise. We'll look back at the security vulnerability counts of 2015 and see what they mean. Google has issued some critical Android updates that we need to talk about. Ransomware has gone multiplatform, and we'll talk about that. There's a new Internet of Things WiFi standard which has finished all of its ratification. We'll talk about how that's different from what we've got. A new side channel attack using Smartwatches, of all things. IPv6 is 20 years old.

Leo: But that's the new thing.

Steve: That's right. And it's just about getting ready to take off.

Leo: Any day now.

Steve: And then we have just a ton of miscellaneous stuff, courtesy of our great listeners, people sending me things over the course of the holidays, the most interesting of which we'll share. So I think another great hour or two.

Leo: Well, these are a few of my favorite shows, just kind of a tossed salad of security lettuce.

Steve: Security Lettuce. There's a name. Yeah.

Leo: That was one of the rejected names for the show.

Steve: Security debris.

Leo: We were thinking of calling it, yeah, Security Debris. And we decided not to, thank goodness. Why are you smiling at me like that, Steve? You got something up your sleeve?

Steve: How do you know I was smiling at you?

Leo: I can tell. I'm like your fifth-grade teacher. I can see out of the corner of my eye.

Steve: Apparently.

Leo: Yeah.

Steve: So our Picture of the Week at the top of the show notes is kind of fun. Although IPv6 is now celebrating its 20th anniversary...

Leo: And Vint Cerf, who was like one of the guys really lobbying hard for this for the last 20 years - he's now at Google, by the way.

Steve: Yeah. And, I mean, these guys were right to realize that, wow, you know, we

thought that 32 bits, oh, my god, that's 4.3 billion IPs. We will never need more than that. Anyway, that was like the 640K RAM ceiling.

Leo: Oh, we'll never need more RAM than that.

Steve: The Apple II had 64K. We're going to make the IBM PC, we're going to give it 640K, 10 times as much. We'll never need more than that. Well, so it is probably safe to say, certainly in our lifetimes, Leo, we will not need more than 128 bits of IP, which IPv6 gives us.

Leo: That's a big jump. From 32 bits to 128 bits is a big jump.

Steve: Yeah. Again, it's difficult for our human brains to wrap ourselves around the idea that every bit we add doubles the number because 128 doesn't seem like, you know, it's only 96 more than 32. And it's like, eh, okay, that's only four times more bits. But, oh, boy. It's 2^96 times - it's 2^96 Internets, essentially.

Leo: It's enough IP address for every grain of sand, every molecule. I mean, it's incredible.

Steve: Well, yes. So much so that ISPs are just giving their individual single subscribers a block of 64K IPs. It's like, "Here you go. This ought to be enough for your light bulbs." Anyway, so this chart on the first page, the Picture of the Week, is Google's measurement of IPv6 adoption.

Leo: If you squint, it looks pretty good.

Steve: Well, yes. This is, however...

Leo: Like a hockey stick.

Steve: This is the most recent 10 years. So for the first 10 years it was flatline. It was like, you'd have to have another one of these charts over to the left that just shows nothing. So, and the bridging technologies existed briefly. You can see the little red line that kind of was making an effort, then it kind of faded out. That was the IPv4/IPv6 bridging stuff. But now, I mean, it's doing a nice - it's not quite exponential because it ought to be accelerating more, if it were. We're still showing some reluctance. So it's sort of a straight line with an exponential liftoff.

But the point is Google is measuring the - what they do is some small fraction of Google visitors get a little bit of extra JavaScript added to see if they're able to directly access IPv6 resources, which would indicate that they have a local IPv6 stack operating in their system. So this is a way for Google to sort of salt their followers, their users, with little probes. And that's how this chart has been developed. What's significant is that - and I don't know how, on what side of this you would stand. But we are now at 10%.

Leo: That's what I mean by, if you squint, the curve looks positive. But the top is only 10%.

Steve: Yeah. And in fact, one of my own personal pet peeves is graphs that are not zero-based. Now, this is. But it's not - but they didn't set the top to a hundred. If they set the top to a hundred percent...

Leo: You know why they didn't.

Steve: Yeah.

Leo: It looks stupid.

Steve: Yeah. And it's like one of the ways of lying with charts is you use non-zero-based...

Leo: I agree. People do that all the time. It's terrible.

Steve: ...scales. And it completely artificially inflates the differences between things. Which, you know, just sort of always seems like a cheat to me. But anyway, in this case the shape is nice, and the timing is nice. It sort of began to happen five years ago, at the beginning of 2011. And 2012 was maybe about twice that. 2013, a little more than twice 2012. 2014, it's accelerating, so about 2.5 times, and so on. And clearly this is where we're headed. No one expects this is going to stall out or anything. But it'll be fun to see over time what the shape of this is, if it does in fact begin to sort of flatten as there are people holding out, keeping their IPv4 because it works, and not feeling the need to move.

And as we know, there are countries - this is probably - it'd be interesting also to see a geographic distribution. Actually, there was one on the page that I got this from. But the map that showed the geography didn't have a key. They had, like, red zones and green zones. But then I looked, it's like, okay, what do those colors mean? And there was nothing shown. I didn't dig down too deeply. Our friend Simon Zerafa sent the link to me that I found this. But I'm sure what we would see is a huge amount of geographic non-uniformity where countries that are - oop, there it is, that's the chart. Now, does that show anything? Can you see what red and green...

Leo: Yeah. Green is - the darker the green, the greater the deployment. Orange, which is a little too close to red for my taste, but orange is where - I'm sure the Google engineers are colorblind. Orange is where IPv6 is more widely deployed, but users still experience significant reliability latency issues connected to the IPv6 websites. And regions where IPv6 is not widely deployed and unreliable is bright red. So then there's some pink. I don't know what the pink means. But apparently the U.S. is strongest in this.

Steve: Yeah.

Leo: As well as Portugal, which has a whopping 24% adoption for IPv6. That's almost as much as the U.S. Greece, where apparently the drachma is strong because it's got 20%. Belgium, 44%. That's the EU talking; right? And Switzerland, which is 30%. The U.K. is a woeful 2.96%. I'm sorry, U.K. But so Canada is 7.4. Brazil is 6.5. Ecuador, bad news in the latency, 40ms latency. Zero percent adoption in Botswana, and 40ms latency. So there you go. Botswana's the worst, so don't go there for your v6.

Steve: Yeah. Stay on a boat. I heard that your cruise ship was just like amazing Internet connectivity.

Leo: Oh, my gosh, yeah. Sometimes if you want I'll talk a little bit about how that technology worked because I got the lowdown from Kirk Harnack, who's apparently worked with some of the people who installed that stuff. There is satellite Internet that's pretty darn good.

Steve: Nice.

Leo: Apparently boils down to basically a dedicated satellite aiming at the ship, like this is yours. It's not cheap for them. But the boat cost $1.4 billion. It's not...

Steve: Well, and you've got to figure, I heard you mention that it was $10 per day.

Leo: $15, yeah, for the Internet.

Steve: Oh, I'm sorry.

Leo: Unlimited, which is very unusual on a ship. It's very unusual. Almost always they have significant bandwidth caps.

Steve: $15 a day. And would there be anybody on the ship that would not have Internet service?

Leo: No. Well, you pay for it. Everybody can have it.

Steve: Right, and so...

Leo: They have two WiFi networks, one for crew and one for guests.

Steve: So I'm just thinking it is a revenue generator for them. Wouldn't you say? I mean, if like a huge population, a percentage of the people on the ship...

Leo: 5,000 times $15 a day, yeah, I think they could afford it. This is - the technology is 03b Networks, if you want.

Steve: Yeah, see, we need to get that for Elaine because - although I think she had an upgrade to her HughesNet satellite some time ago. Things seem to be better for her now.

Leo: Yeah. Yeah, this is, well, I mean, yeah. Maybe you saw my speed test at 3:00 a.m. I had to get up in the middle of the night to kind of guess what the maximum was. It was about 25Mb down.

Steve: Gosh.

Leo: Really surprising, I mean, in the middle of the Atlantic. That's pretty impressive. O3b Maritime, if you want to read up on more.

Steve: So we've heard some reports on the 'Net of the disabled "Get Windows X" switching itself back on. We now have our own listeners reporting that it has happened to them. Charles Killmer was one, who tweeted to me and made it into my notes. He said, "This morning the GWX Control Panel" - which is the app we talked about recently - "alerted me to OS updates being reenabled. I have not installed anything recently. Update history shows only Windows Defender updates." And he said, "Thanks for the tip on GWX Control Panel."

So I wanted to remind our listeners, who may have heard about it, meant to deal with it, but didn't, that if you just google "GWX control panel," it'll take you to UltimateOutsider.com, which is the guy who developed this. And it's becoming quite popular because it's the way to keep control. Essentially, for whatever reason, and it just must be because Microsoft is determined to push Windows 10, even if you turn it off, Microsoft just unilaterally turns it back on. So we now not only have sort of a generic report from the industry, but our own listeners are saying the same thing.

And the other bit of news that's related came from someone whose handle is OneEye Rabbit, who tweeted. And he said, "Steve, in 539 you talked about GWX." And he said, "For me, I tried WinX from the 7th of December through the 22nd of December. Finally I had enough and tried to revert to my previous Windows 7. Microsoft said you have 30 days to revert, but for me after two weeks that option was no longer available."

Leo: Yeah, I've had the experience, too, that it doesn't always work, yeah.

Steve: Yeah, he says, "I used a restore point to get back to Windows 7. Now I'll have to deal with GWX again." So I did want to note that apparently, again, for whatever reason, maybe Microsoft is starting the counter earlier than users choose to install it, who knows.

Leo: Well, it's not an inconsiderable amount of space, remember. You know, saving an image of your previous install.

Steve: Yeah, yeah. And of course downloading beforehand...

Leo: The next one, yeah.

Steve: ...the number of gigabytes of Windows 7.

Leo: So it may be - it may have something to do with free space. I mean...

Steve: That's a good point.

Leo: ...there's a lot of reasons why it might not work. I've had it work, and I've had it not work. So I always advise people not to trust the 30-day rollback. You should make a copy, make an image.

Steve: Right. Good, good, good. And speaking of Windows 10...

Leo: I don't know - by the way, I'm going to mention real quickly...

Steve: Yeah.

Leo: We had the CMO of Microsoft on Windows Weekly two weeks ago.

Steve: Right.

Leo: Chris Capossela, who's great. And I asked him specifically about this GWX thing. And he was, I think, is it fair, listeners, to say he was a little embarrassed by it? He knew about the problem. He'd heard about it. And they felt like they maybe misstepped a little bit.

Steve: Well, it's generating a lot of negative press.

Leo: Yes. And I think he's aware of that.

Steve: I mean, so you don't want that.

Leo: Right, right.

Steve: So Windows 10 market share is climbing and now getting close to where Windows 8.1 was. There's a neat site, and I want to commend our listeners to it, just because I really like these sorts of time change charts. And the site is - I've got two pages here in the show notes. But it's gs.statcounter.com, gs.statcounter.com. And you can, there, you can select a number of different charts over time. And but the one that I pulled out shows that the black line in their chart is Windows 10 adoption, which took off from zero on July 2015 at launch. And it initially climbed a little faster. Now it's sort of on a linear trend. And it looks to me like it's more than 10%, actually, it's sort of maybe like 12%.

The biggest loser, but which of course proportionally makes sense because it has the largest market share of Windows, actually of all because iOS is in there, as well, as is OS X, is Windows 7. Windows 7 was up at 50%, and it's been pulled down to 40%, pretty much almost in line with Windows 10 going up.

Leo: Yeah, it's kind of what you'd expect because those are [crosstalk].

Steve: Yeah, and 8.1 never got above about 15%, and it's been pushed down to looks like about 11%. So just sort of I really like these time varying charts. I also have a pie chart that sort of shows where everything is overall, showing Windows 7 with still the majority OS in the entire industry at 55.68%. XP, yeah, XP's in number two, 10.93, followed by Windows 8.1 at 10.3. And then Windows 10 at just shy of 10%. So this chart looks like it's a little bit dated. The pie chart did come from a different site. So it's either different data collection, or it's a little bit older because it looks like in the chart that we were just talking about, Windows 10 had a higher adoption, and actually 7 had been pushed down from 55 down to about 40%.

Leo: Where does StatCounter get its stats? How do these, I mean, this is not from Microsoft, obviously.

Steve: No. I didn't dig into it.

Leo: Microsoft says 200 million installs. Which would be actually a higher number, I think, a much higher number than this shows. But they also admit that they're including Xbox One. Not that that would make a huge difference.

Steve: And then while I was at StatCounter, I was curious about - they also offer browser utilization. And I thought this was really fun. I pushed it all the way, I pushed the starting date all the way back to as old as they were collecting. And more than anything else, this shows the crash of IE and the rise of Chrome. From January, the beginning, actually a little bit earlier, it was about midway through 2008 it begins. And IE at the time was at 70%, and it's collapsed to about 14% now. And Chrome was at zero back then, and it's now the dominant browser at looks like well over 50% of share. Of course Firefox has been depressed. It never had the starting share that IE did, but it's pretty much taken the brunt of the rise of Chrome. And Safari's sort of been puddling along. Or, no, wait, where's Safari? So Safari's been growing, but then in the last year

and a half sort of stopped its growth for whatever reason.

Leo: Now I remember StatCounter. People used to use this on the web all the time. Remember you'd have a hit counter on your website. It was a free little JavaScript bug that would do a hit counter. So I guess my question would be I don't know how many sites still use this. There's a lot of sites that probably would avoid it because their users would say, "What the hell are you counting me for?"

Steve: Or they're just blocking scripts on their site now.

Leo: Right. So I don't know how accurate their numbers are because it's basically, in order for this to work, the websites have to install this on their website. I mean, it's probably, I mean, it's a smaller sample size than the total, but it's relative numbers [crosstalk].

Steve: Yes. And really it's the shape of the curves.

Leo: Right, right.

Steve: So, okay. There was a lot of concern, I mean, everybody got into the mix. The Intercept has an article. Cory Doctorow spoke up. SlashGear wrote articles. Ars Technica got in. Because the news was it struck everyone apparently by surprise that when you were using a Windows 10 machine, your hard drive encryption keys were sent up to the cloud, up to Microsoft, where they were available to help you recover if something should happen.

Now, the reason this is not news is this so-called "device encryption" was introduced in Windows 8.1 back in 2013. So this is what Microsoft has been doing for a while. So I think this has people digging deeper into Windows 10 and saying, hey, wait, you know, wait a minute.

Leo: Well, you remember how it used to be. Before they started doing this as a service, you had to save your certificate for your whole disk encryption. And if you neglected to do so, which most people, I think a lot of people didn't, you were out of luck.

Steve: Right. And so, for example, this is the case where all the responsibility rests on the user. TrueCrypt famously made you burn a CD and then made you insert the burned CD to prove to it that you had actually done that. I mean, so that they did everything they could to help you keep yourself out of trouble while not sending your TrueCrypt master key elsewhere. So exactly to your point, Leo, if you're in a really Trust No One mode, then you have the responsibility for managing your keys.

So this is, I mean, this is the tradeoff that Microsoft decided was in their users' best interest, which is export the keys to the cloud. Well, and for example, in BitLocker and in whole drive encryption, the TPM, the Trusted Platform Module, contains the key. But that could get struck by lightning, or your motherboard could die, and so that it would - you

no longer have access to it. So exactly as you said, Leo, you are able to export your key locally, but most people don't.

Leo: Can you turn it off, though? Can you say don't upload it?

Steve: Actually, you can't. The best you can...

Leo: Ah, that's a problem, see.

Steve: That is the problem. There's no notice. There's no opt-out. It always uploads it. Now, what you can do is go and delete it. The problem, of course, is that the keys have already been uploaded. So Matthew Green weighed in, our often-quoted Johns Hopkins cryptographer. He said: "The gold standard in disk encryption is end-to-end encryption, where only you can unlock your disk. This is what most companies use, and it seems to work well. But there are certainly cases where it's helpful to have a backup of your key or password. In those cases, you might opt to have a company store that information. But handing your keys to a company like Microsoft fundamentally changes the security properties of a disk encryption system. Your computer is now only as secure as that database of keys held by Microsoft, which means it may be vulnerable to hackers, foreign governments, and people who can extort Microsoft employees."

And of course other people observed that Microsoft could be served with a subpoena that compels them to turn over the decryption keys for an arbitrary user's hard disk, which presumably they would have to do if they had that information.

So you are able to delete the key that's been sent. And I was a little confused because Microsoft has done, of course, their normal thing where the Home version is different than the Pro, which is different than the Enterprise. Because Home doesn't have BitLocker, as I understand it, it has something called Device Encryption, which is sort of a weaker or watered down or less UI or something than BitLocker. But there is information, for people who are concerned, to allow you to change your key and not have that change uploaded to Microsoft. So you can get back to TNO. And then of course the caveat is make sure you've got your keys backed up, if you take the trouble to do this.

So my only issue, I guess - and it isn't a big one because I recognize that Windows 10 is not for me. It's not for many of our listeners who fundamentally want an OS that is more on their side. So, but that's not most people. Most people would like to have encryption so, if their laptop gets stolen, then bad guys don't have access to what's on it, and the idea of having access to the keys to decrypt it through their Microsoft account. Oh, and this is tied to the Microsoft account. That's the other thing. If you go through that extra procedure of not using a Microsoft account, but only use local, create a local identity, then your keys never get sent to OneDrive, which is where this is, because your computer isn't associated with a OneDrive presence in the cloud.

So there are ways around this. But by default, everyone's encryption keys are being held by Microsoft. So the first step back from that would be simply to make a local copy or copies, make sure that they're secure, then delete them from the cloud. And then the stronger solution is change your key in a way that doesn't resend it to the cloud. Then you've regained full TNO security. I've got links to various articles, and there's been a lot of discussion over the last two weeks, ever since this arose. And again, this has been going on since 8.1, but it generated a lot of headlines and generated a lot of tweets to

me from people saying, oh, boy, what's this about?

Leo: Before we...

Steve: And Microsoft...

Leo: Go ahead.

Steve: I was going to say Microsoft...

Leo: I'm going to interrupt before you get to the next subject. But go ahead.

Steve: Yeah, I was going to say Microsoft has confirmed that it automatically uploads Windows 10 disk encryption keys to its servers and said that it's a deliberate decision based on weighing the worst-case scenarios. And they feel that it's better for them to be able to provide restoration keys in the event of any catastrophe that would cause the user to otherwise lose all the data on their drive.

Leo: It's a tough one. I mean, I don't know what to - you understand, I mean, LastPass apparently, in its new version which came out today, has now allowed support for key recovery of some kind.

Steve: Yup, LastPass 4.

Leo: Yeah, I presume you'll talk about that at some point.

Steve: Yup.

Leo: But I understand why you want to have key recovery.

Steve: Yes.

Leo: And the thing is to implement it intelligently.

Steve: Yes.

Leo: Because people are going to make mistakes.

Steve: Yes. And what I've done with SQRL is, I mean, recognizing that there is no third

party, and that's on purpose because we don't want one, is to come up with what we call a rescue code, very much like TrueCrypt. I make people write it down, and I make them type it in just once. And all it is, it's one and a half times the length of a credit card number. So it's 24 digits. And that's all you need. Just write it down and put it somewhere, and that will always recover your identity. And it's long enough, and it's purely random, so it's full entropy, that it's infeasible for it to be attacked. But that was a tradeoff I made. And it is the case, I think what we're seeing is LastPass is trying to find ways to compromise on a rigid security model where you would be up the creek and say, okay, yeah, it would be nice, but that's not practical.

Leo: Right.

Steve: So to make a practical system for an increasingly expanding user base, who are not super technically oriented, you know, you have to back off a little bit from that. So sending your drive encryption keys to Microsoft is the tradeoff Microsoft made. The only thing I guess I would wish for is more clarity. Microsoft should present a dialogue that says...

Leo: Yeah, explaining this, yeah.

Steve: ...for your safety, well, and also...

Leo: And an opt-out.

Steve: Imagine that you didn't know that your keys were backed up, and you had a catastrophe. You'd go, oh, crap, now what? And you wouldn't be able to take advantage of the fact that they were backed up in the cloud. So you really do need to know that. So Microsoft should say this is what we're doing, and maybe give you the option not to. Or maybe say, if you're really sure, or maybe say we already did this. If this is really not what you want, go there and delete them. But if you do that, make sure you've made copies first.

Leo: Don't hold us responsible.

Steve: Exactly.

Leo: All right. We're going to talk about what was the most insecure OS of 2015 in a little bit.

Steve: Oh, lord, yeah. So I love that you led into this next topic with the most or the least secure operating systems because what I wanted to highlight is that a count of vulnerabilities is meaningless. VentureBeat had a article, and actually a neat table. You want to click that link, Leo, and bring up the whole chart titled "Software With the Most Vulnerabilities in 2015: Mac OS X, iOS, and Flash." And sure enough, if you look at the - and we often talk about the CVE numbers, the Common Vulnerabilities and Exposures.

That's from the National Vulnerability Database, where vulnerabilities are registered as they are found.

So sure enough, Mac OS X leads the pack at 384. iPhone, or iOS, is number two at 375. Flash Player, actually I would say this one is more deserved, in the third place at 314. But to give you a sense for why just a number is meaningless, OpenSSL, which has been the source of massive scurrying all over, is way down the bottom at 34. So it's not the number. It's the fact that, for example, in the case of OpenSSL, they were doozies. I mean, they were industry grind to a halt, run around with your hair on fire.

Leo: All you really need is one really bad one; right?

Steve: Exactly. And so it is the case, you know, I mean, here's Apple tweaking their software and fixing problems, I would argue none of which have been, like none of those 384 were as bad as any one of the Flash Player 314. You know, every one of the Flash Player vulnerabilities was really remote code execution by visiting a web page sort of problem. Whereas Mac, the Apple stuff is like, oh, yeah, we found some stuff that somebody privately reported, and we fixed it, so...

Leo: In some ways you're penalized on this list if you are forthright about the problems.

Steve: Yes, yes.

Leo: Because the number, I presume that number ultimately comes from the company. Right?

Steve: Yes. It is the company registering vulnerabilities with the National Vulnerability Database. The other thing that's misleading, if you scroll down a little bit from where you are, is like the Windows versions. They show, like, all these vulnerabilities with Windows, except we know that they're all the same vulnerability.

Leo: Right.

Steve: So it's one problem that is across all of the common codebase of these.

Leo: Right. And Windows 10, which is fairly low on the list, number 35 with 53 vulnerabilities, it's brand new.

Steve: Right.

Leo: So it was only out for five months of the year.

Steve: Well, and remember that they didn't rewrite Windows. They gave it a new sugar coating, but basically it's the same Windows. You just keep seeing the same dialogues after you drill down a couple layers of the froufrou UI. It's like, oh, yeah, there's the actual dialogue that I've had since XP. So Windows 10 basically has the advantage of the maturity of the codebase, and it's all the new things they've added that have the problems. The bulk of the code is still, is now becoming more time-tested. So I just sort of - I wanted to put a little reality check on the fact that just a number of vulnerabilities, I mean, if they're trivial, we're fixing this because we can, as opposed to OpenSSL, oh, my god, this has been out there for six years, and it's exposed everybody.

Oh, the other thing with OpenSSL is notice that it's a library that has been, that is massively cross-platform. So it's being blamed for, I mean, it shows 34 vulnerabilities, but all of the Linux distributions were using this vulnerable version of OpenSSL. But they're not counting independently the OpenSSL vulnerability, even though this is a library. So anyway, the numbers are sort of interesting, but really need to be taken with a grain of salt. And so a headline that says Mac OS X had the most vulnerabilities is like, eh, okay. But Flash did the most damage. And so I think it's - and OpenSSL, arguably.

Leo: Be hard to measure that, though. I mean, it'd be hard to have like a chart of who was the most vulnerable or whatever.

Steve: Yeah, yeah. Only the NSA has that.

Leo: Yeah, they know. They know.

Steve: They're using it. Meanwhile, Google did patch five critical Android security flaws. They're doing a OTA, an over-the-air update as part of their Android Security Bulletin Monthly Release process, they call it. And once again, receiving a multimedia message allows for remote code execution. That Mediaserver library is just causing a real bunch of pain for them. They must be really regretting the day that they just said, oh, yeah, we'll incorporate this into Android. Because, I mean, it's just replete with bugs. Five of the dozen that are being fixed in this are critical, meaning remote code execution. And then they dropped down to moderate and severe.

So anyway, again, as we've discussed, I think it's becoming increasingly clear that sort of the telco or the smartphone model needs to incorporate the same kind of on-the-fly continuous security patching that we're now all accustomed to in all of our desktop OSes. You just can't have a phone that has a operating system as sophisticated as Android is that, once purchased, is then abandoned, because there will be problems. Everything we're seeing teaches us that.

Meanwhile, the first instance of, get this, JavaScript-based ransomware has been found in the wild. Now, when I saw this, I thought, wait, no, you can't have JavaScript-based ransomware because the presumption is that JavaScript is tightly sandboxed by the browser. We know that. We know that JavaScript has no access to files in the OS. Well, it turns out that this is JavaScript in the same sense as we were discussing a few weeks ago, where remember someone left-clicked on a .js file and ran it in Windows because Windows has its script engine bound to files with that extension. And so that was running JavaScript natively on the platform where it is not sandboxed at all.

So what's happened is a well-known JavaScript kit called Node, the Node-Webkit, that's

now known as the NW.js, which is, you know, NW stands for Node-Webkit. That's now available, bound to an EXE wrapper. So essentially what this means is that someone has written ransomware, meaning just like CryptoLocker, where it goes out and encrypts your files. In this case there's a sort of a weird model where the developers are offering this as a service, and they're taking a piece of the action from the miscreants who get it from them and then arrange to get it into users' computers.

So we're now sort of seeing a two-tier system where authors of the ransomware are making it available under a software-as-a-service (SaaS) model to people who then figure out how to get end users to run it and get themselves encrypted and then have to pay up. There's a security researcher, Fabian Wosar with Emsisoft who said that, by using NW.js, Ransom32, that's the name this thing's been given, could easily be packaged for both Linux and Mac OS X, even though so far it's only been seen in a Windows EXE format.

And of course, as we were saying, although JavaScript in the browser is heavily sandboxed, NW.js allows for much more control and interaction with the underlying operating system, which enables JavaScript to do the same things that native programming languages like C, C++, and Delphi and so forth can do. So that's not good. It means that we have ransomware that's cross-platform. And given a platform-specific wrapper, so Linux would need its own wrapper, Mac OS X would need its own in order to get that script to be able to run.

But the Node.js, I'm sorry, the Node-Webkit.js, it provides the cross-platform interface, essentially making it easier to do. So when we first saw ransomware a couple years ago, it was immediately clear to us that we were in trouble, that this was going to make money, and if it made money, we would get more of it. And we're seeing, ever since, we've been seeing more of it.

We've been talking about security certificates, root certificates, and how various packages add certs to users' machines. Sometimes corporations will add a cert. And it's a constant question now I'm getting, how do I tell if my system is infected? Or, well, not infected. Well, maybe you consider it an infection, you know, that AV software is doing it, employers are doing it. We've seen rumblings about governments doing it. And I'm worried about the day that ISPs will do it.

Our friend Mark Russinovich has a cool utility. Remember that he used to be Sysinternals, and Microsoft bought Sysinternals in order to get him, mostly. He has a utility called SigCheck, which is not yet at v2.4. Right now it's at v2.3, and it's one of his, sort of that Sysinternals, very nicely written, lightweight, I think it was something like 180K. It's just a simple program that runs. You don't have to install it. Right now it's a utility for verifying signatures of files, showing you the signing chain and expiration dates and verifying the signatures of files and so forth.

In beta is v2.4. I was alerted to it by a friend of the show who tweeted me about it, and I've got my eye on it, too. 2.4 will add a check for non-Microsoft root certs. And that will be great. So I've got my eye on it, and I wanted to let everybody know that it's coming. And as soon as it happens, I'll mention it again because something from Mark would be the way to do this, just to verify that your root store is still clean, and nothing has added anything to it. Or at least to enumerate what has been added so you know that it's things you want or maybe need, and not something that has crept in under the radar.

Okay, now, this - this is just too wonderful. This is old. But it is still apropos with everything that's going on with certificates. I just saw, didn't have time to get it into the show notes, that Let's Encrypt has crossed the quarter million certificates mark in, what's

it been, maybe a month? Maybe six weeks. They have issued more than 250,000 domain validation certs through the Let's Encrypt facility, meaning that there are - it may be that they are replacing existing standard, issued-from-certificate-authority certificates. Or, more likely, these are sites that have never been encrypted before, that want to add TLS and HTTPS. And we're now at plus a quarter million, thanks to this effort.

Leo: That's awesome. That's incredible.

Steve: It really is great. However, our listeners who've been listening from the beginning will remember that the podcast when I shared my shock over opening up, I think it was probably Windows XP, maybe 2000, I don't remember how far back it was, probably XP, I looked at the certificate manager. And back in the day, as they say, there were maybe, oh, 10 certificate authorities. And it was like, okay. And I remember, I looked at XP, and there were 400. And of course that's when we began beating up on the Hong Kong Post Office, because it was among those that I was just scratching my head at, saying, okay, why am I trusting, is my machine by default trusting certificates issued by the Hong Kong Post Office? Among many, many, many, many others.

So we've never really talked about the process by which an entity, any of these 400, appeals to or submits a request somehow, what's the process for getting yourself certified so that you're going to be a certificate authority? Well, there was an application submitted to Mozilla back in 2011 by an entity calling itself Honest Achmed. And this is - it's in Bugzilla, which is how these things go. In Bugzilla it's Bug 647959. And the title of this submission was "Add Honest Achmed's root certificate."

Leo: Oh, of course, yeah. He's honest.

Steve: Yeah. Well, and if you had any doubts. And so this says, "This is a request to add the CA root certificate for Honest Achmed's Used Cars and Certificates."

Leo: [Laughing] I thought maybe it was flying carpets. But okay, used cars. That's good, okay.

Steve: This, well, because we're not so sure about flying carpets, used cars, yeah. "This requested information as per the CA information checklist..."

Leo: Oh, lord. Oh, lord.

Steve: "...is as follows. Name: Honest Achmed's Used Cars and Certificates. Website URL, and this is priceless: www.honestachmed.dyndns.org."

Leo: Yeah, because he doesn't know. He's getting ready - he's a mobile guy.

Steve: It's on his kitchen table.

Leo: Yeah.

Steve: Yeah. This makes Hillary's email server in an ISP's closet look good by comparison.

Leo: This is tongue-in-cheek, though. Steve. This must be somebody pointing out the ridiculousness of this.

Steve: It's so wonderful because organizational type is an individual. And then it says, parens, "(Achmed, and possibly his cousin Mustafa, who knows a bit about computers)." And then the primary market/customer base - and these are all the questions that are part of Mozilla's form.

Leo: Right, right.

Steve: And he says, "Absolutely anyone who will give us money." Impact to Mozilla users: "Achmed's business plan is to sell a sufficiently large number of certificates as quickly as possible in order to become too big to fail (see 'regulatory capture'), at which point most of the rest of this application will become irrelevant." And then, under technical information about each root certificate, the certificate name that this was being applied for was, of course, Honest Achmed's Used Cars and Certificates. The certificate issuer field, Honest Achmed's Used Cars and Certificates. Under certificate summary: "The purpose of this certificate is to allow Honest Achmed to sell bucketloads of other certificates and make a lot of money."

Leo: Yay.

Steve: And then remember how...

Leo: He's honest, you know? He's Honest Achmed.

Steve: Yeah. And that's been reinforced here. Notice how, as we've talked about it, certificates have a bit mass, essentially, a bit field of things that they are enabled for. For example, some certificates can be used to sign code. But a code-signing certificate cannot typically also be used to represent a domain because it's a different application. And some certs are intermediate certs, so they're established that way, but they're not able to sign other certs, whereas root certificates can, so forth. So anyway, under requested trust bits, which is another field in the Mozilla form, Honest Achmed has said: "All of them, of course. The more trust bits we get, the more certificates we can sell."

And finally, under CA hierarchy: "Honest Achmed plans to authorize certificate issuance by at least, but not limited to, his cousin Osman, his uncles Mehmet and Iskender, and possibly his cousin's friend Emin." So anyway, if anyone is curious, the link is in the show notes. There's more. I excerpted from it. But somebody had a lot of fun. And I got a big kick out of the fact that it was taken very seriously by Mozilla, who declined the

application. However, this bug had a huge trail of responses which are equally fun. So if anyone enjoys this kind of thing, it's there. Thought you should know.

Gizmodo reported on the story that our smartwatches can now determine what we type. And of course immediately upon knowing that, it would be obvious to anyone that the motion sensor in your smartwatch could detect what you're doing. And so this video on the Gizmodo page that Leo's showing right now is of someone entering a number on a 10-key pad, and the smartwatch, just from the relative motion, determining what they're entering.

And so of course this is yet another so-called "side channel attack." We've talked about these. And they occur in movies. For example, a famous one is someone reading lips at a distance through a window, where you can't hear what the person's saying, and they may be even under the cone of silence. But if you can see them, then essentially a side channel leakage is somebody who is a gifted lip reader can determine what they're saying. Or lifting a fingerprint - huh?

Leo: "I read your lips, Dave."

Steve: Right. Oh, yeah, that's a perfect example.

Leo: It was Hal; right?

Steve: Yes. Or lifting a fingerprint from a glass and then reusing that lifted fingerprint, dusting it with powder, making it optically visible, and then using it to gain entry somewhere. And we've talked about more high-tech approaches like the way encryption algorithms sometimes change - they don't have a linear path through the code. But if the key causes different jumps to be taken, then you can actually get bits of the key by looking at the power deviations caused by the processor taking jumps or not. I mean, wow.

But your first thought is, oh, yeah, but, you know, really? And it turns out, yeah. Grad students or master's thesis kids who have time on their hands try it, and it turns out it's able to work. So, and of course, and we've talked about how a smartphone lying next to a keyboard, the vibrations from typing on the keys, or even listening to keys being typed.

Leo: Remember Van Eck phreaking; right?

Steve: Yup. Yup, there's Kevin.

[VIDEO CLIP]

KEVIN: You're sitting at home, you know, you're doing a little web browsing, surfing around on the...

Leo: You're broadcasting.

KEVIN: You're broadcasting. Those frequencies are going outside of your monitor. Someone could potentially sit there and then pick up a mirror image of exactly what you're doing, just by picking up those frequencies and then reinterpreting them with [crosstalk].

[TALKING OVER CLIP]

Leo: I think he demonstrates this. This is an old Screen Savers episode.

[CONTINUE CLIP]

KEVIN: There have to be a lot of things in place to make that happen.

Leo: Now, before we make everybody paranoid and crazy and looking for [crosstalk].

[TALKING OVER CLIP]

Leo: So, and this is 2004.

[CONTINUE CLIP]

Leo: We should say we don't know that this is possible.

KEVIN: We don't know that this exists. But the government did have a top-secret program called Tempest.

Leo: Tempest. This is in the '60s or '70s, yeah.

KEVIN: In the '60s and '70s.

[END CLIP]

Leo: Yeah, to prevent Van Eck phreaking; right? Yeah.

Steve: Yup. And Snowden's documents had a lot to say about this, too.

Leo: Yeah, yeah.

Steve: There were a lot of little passive eavesdropping gadgets that we talked about that...

Leo: Bluetooth, or wireless keyboards. Remember we talked about how poorly encrypted those were.

Steve: Yes, like four bits of, quote, "key," unquote.

Leo: Yeah, yeah.

Steve: Yeah. So, and then of course we've also run across, more recently, a high-res photo of an old-school metal door key. It turns out there aren't that many positions, and you can get close enough, just taking a picture of the key that we all have dangling in our pockets, if you leave it out. So anyway, I thought, here is yet another one. Smartwatches are able to, you know, naturally. Although only on the hand where the watch is. And so my first thought was, wait a minute, people typically wear their watch on their non-dominant hand, yet they would enter on a keypad with their dominant hand.

Leo: Us lefties, though, often wear our watches on our dominant hand because the world has dictated that you should be able to wind your watch with your right hand.

Steve: It is annoying, too.

Leo: So, yeah. You're a lefty; right?

Steve: I'm a lefty, and I do wear my watch on my right hand.

Leo: Do you, yeah. A lot of people do, but you can't reach the stem.

Steve: Yeah. And Apple did address this; right? You're able to rotate the watch in order to have the stem high and on the outside.

Leo: That's right. Thank you, Apple, for thinking about lefties.

Steve: A new standard coming, it's actually been in the works, the chips exist, but it was just ratified. It will be called HaLow, H-A-L-O-W, so that's how we pronounce it, HaLow. And I heard you yesterday, I think, you were talking about microwaves interfering with WiFi.

Leo: Right.

Steve: And maybe it was IoT stuff because, as we know, microwave ovens use the same 2.5GHz band that WiFi does.

Leo: Every time Megan Morrone's husband would fire up the microwave to heat up a bun, she'd get knocked off her WiFi. And I deduced, maybe wrongly, I don't know, but I deduced, well, I think that's 2.4GHz interference coming out of the oven.

Steve: Yup, totally makes sense. So what we've done now, and this is 802.11ah, so they swapped the "ah" to make "ha" in order to - and then stretched it a little bit further to get "hay." And so now - and it's a low frequency, so it's HaLow.

Leo: HaLow, I get it.

Steve: Yes. So this is...

Leo: This is not a successor to "ac," which is the current standard.

Steve: Correct, this is not.

Leo: This is an adjunct to it.

Steve: And what they've done is this - you can sort of think of it as the Wi-Fi Alliance's refusal to give in to Bluetooth.

Leo: Of course.

Steve: So it's - yes. So it's lower speed. So it's also not multiple megabits, the way we have now in the high-frequency 802.11. This is a hundred kilobits, so much slower. But on the other hand, temperature thermometers, your light bulbs, your doorbells, all of the Internet of Things things, they're not typically media devices shooting, you know, that need high bandwidth. And what they need is low power.

So this is a very nice tradeoff between speed and power. It runs sub-gigahertz, down in the unlicensed or license-exempt 900MHz band. Being sub-gigahertz, in terms of the way radio frequency propagates, lower frequency has an easier time, for example, going through walls that would otherwise block the much higher frequencies. So this is longer range. And get this, up to a kilometer. So it's a kilometer range, low frequency, and a low data rate.

It's also a completely new network topology. What we've had, essentially the way WiFi works, and we've discussed this often, is it uses the same CDMA technology, the Collision Detection Multiple Access, that wired LAN uses. The way traditional Ethernet works is everybody who's hooked to the same wire is listening for a quiet period. And when it's quiet, they'll broadcast onto the shared connection. But that means two people could see silence at the same time and broadcast at the same time. Well, so while they're

broadcasting, they're also listening. And so the collision in their broadcast would cause what they sent to be garbled. In listening, they would say, oops, that didn't work. Then they back off a random amount of time.

So statistically, one of them will rebroadcast before the other, and their message will get through. Then there'll be silence again, and then the second guy will broadcast. So what happens is this all works as long as you're not really busy. And you can sort of imagine that, as long as the bandwidth of this shared medium is sufficiently higher than the bandwidth that the medium is trying to convey, this sort of ad hoc, hope for the best, is okay. But as the number of transmitters or the amount they're trying to transmit begins to get up near the capacity, the collision probability goes up. And so everybody spends much more of their time waiting for a turn and then recolliding with somebody else.

So this doesn't fail very well. But we have no real choice with the existing WiFi. The WiFi we're all using right now is the same model. It uses CDMA technology. What these guys, what the Wi-Fi Alliance has done with this next version is completely different. It's this 802.11ah uses contention minimization. In the spec is internode relaying to create mesh networks so that you can reach devices much further away because devices - in the protocol is the ability for an intermediate device to relay to a more distant device. It has explicit power management with waking and dozing built into the protocol.

It is possible for devices to negotiate for higher bandwidth bursts. For example, the Ring Doorbell might, if it were using this spec, in the normal case it could be running at a much lower power consumption. But when it does need to transmit video, it could negotiate for a chunk of bandwidth in the network and be able to receive it. Also in there is antenna segmentation and radio beam forming technology.

So this stuff is like next generation, but we have it now. Chips are on the way. And essentially the idea is that, I mean, they've deliberately made it competitive with Bluetooth in terms of power consumption, but with vastly larger coverage, and then state-of-the-art technology. I mean, all the things I just talked about that are in this "ah" spec would - they would have been impossible five years ago to do in a cost-effective way. Now it'll just be integrated in a little chip smaller than a thumbnail, and it won't cost anything. And it'll be in light bulbs and everything else.

Leo: Well, that's what we want; right? Because the more things that are Internet connected...

Steve: That's what we need.

Leo: That's, you know, what could possibly go wrong?

Steve: That's right. And before our final sponsorship and we get into miscellany, I wanted to mention that GRC did, as I had planned to, switch from SHA-1 certs to SHA-256, thanks to my beloved DigiCert certificate authority, who actually was kind enough to issue both kinds to me so that I would be able to switch when I wanted to. I did it a few days before the end of the year because I recognized, if anybody had their calendars or clocks off, they could think that it was already 2016, and these certs expired on December 31st at midnight - thank you, DigiCert - of the end of 2015. So I did that so that Chrome wouldn't have been complaining until now.

So I'm now up to SHA-256. I've noticed no difference. And I didn't expect to. But the advantage of my having dragged my heels as much as I did, despite all the people who were saying, Steve, what's wrong with you, you're still using SHA-1, is that all of those XP systems that are apparently still out there - unless they're using Firefox, which brings its own security suite along - if they were using IE or even Chrome, because Chrome uses the native OS crypto libraries, they would have been completely unable to get to GRC all of last year. Now they are unable to get to GRC, but they're unable to get to anything else that is still using SHA-1. I wonder how many people still are.

I guess, I mean, nothing prevents people from continuing to use it, with expirations obviously in 2016 or even 2017. But we know that the browsers are going to be really unhappy. And at some point browsers will just stop supporting them at all. I think, as we've covered, maybe around the middle of this year, around the middle of 2016, browsers are just going to say, uh, there's no excuse for still using it. And we do know that SHA-1 is no longer being issued as of New Year's.

So, okay. On This Week in Google, I got a kick out of your - you were lamenting the whole messaging platform problem.

Leo: Oh, my god, yes.

Steve: You said, "Everyone you know is on Facebook except for a few weird grumpy people."

Leo: Like you; right? Are you? Yeah, okay, you're not on Facebook.

Steve: Exactly. I made the jump to Twitter, but that pretty much is all I have [crosstalk].

Leo: We're working on him. You'll get there. You'll get there.

Steve: Well, and the thought I had was what you guys - and this was already in the show notes and everything before you were talking about it at the end of MacBreak Weekly. What occurred to me, because I've heard you lamenting that there's this fragmentation in the messaging world...

Leo: Yes.

Steve: So that, for example, in my case, everybody I know is an iOS user. And so iMessage gives me a hundred percent coverage. But you've got a lot of people, because you're in a sort of a younger, more techie environment, who are Android adopters.

Leo: Right.

Steve: And then of course there was Telegram and WhatsApp and Facebook Messenger

and iMessage and on and on and on. And so what had occurred to me was something that you did mention at the end of the MacBreak Weekly podcast, was this notion of a messaging bridge. Because that's, to me, of course, no vendor wants to create a bridge to other people's messaging apps because they all want to be fully siloed and use the pressure that you're lamenting of fragmentation in order to force people all onto their platform.

Leo: Right.

Steve: Unfortunately, it's not going to happen. People are going to stay pretty much where they are and grumble that they can't get there from here.

Leo: Or they'll have, as many of us do, you heard us talking about it on MacBreak Weekly...

Steve: Multiple.

Leo: ...a folder on our front page of our phone with every messaging system known to man because Aunt Maude uses WhatsApp and Cousin Bernie uses Messenger and like that.

Steve: Yeah. So it would be nice, I don't know, because Apple's iMessage is closed, they won't allow anybody in. But it would be nice if there was a bridge system, like some sort of a bridge solution.

Leo: Well, you remember Trillian and Pidgin and all of the -- and this is how we kind of technologically solved these siloed IM solutions. You have one client.

Steve: It's using a multiprotocol client.

Leo: Right. And that was very helpful because Google, when it started Google Talk, used Jabber, used XMPP, which was an open standard. Then they abandoned it. But had they continued and maybe encouraged others to do that, then we wouldn't - this would be a snap. But nobody wants that. And Google kind of fumbled Hangouts because they have a fully cross-platform solution, but they've kind of let it lie fallow. The rumor is they're going to add smart agents to it, which might increase adoption. But the problem is then I have to tell Aunt Maude, could you please get Google Hangouts on your phone. Whereas I'm pretty sure Aunt Maude already has Facebook Messenger. Everybody but you.

Steve: Yeah. And that's fine. Don't call me.

Leo: And you know what? You watch. Yeah. You don't want - but you watch.

Because I think that there is a subtle, and it will be a mounting pressure from the people you talk to, to adopt this. And Facebook is just kind of the no-brainer. I wish there were some unified solution. There isn't. And I hate to give in to Facebook.

Steve: Yeah, well, because you were holding out with Telegram for quite a while.

Leo: Yeah, yeah. Thing about Facebook is it has a lot of nice features, including the ability to send money, including they're going to add these smart human agents called "M." Google's going to do search agents. So instead of searching, you'll talk to your messenger client and do it that way. But I think Facebook is way ahead of the curve. And the real key is the network effect.

Steve: Yes.

Leo: You've got to have that. And without that, you don't have anything. So unless you do something so amazing - it's possible somebody'll come up with something brilliant that everybody says, oh, I've got to have that.

Steve: Yeah, I kind of think we're past that point. Messaging is messaging, and so, like, you know...

Leo: I don't know. You haven't really experienced messaging until you have the ability to send animated GIFs to friends and family.

Steve: As you keep saying.

Leo: Oh, it's awesome. It's better than stickers. So we start with emojis, little tiny [raspberry]. Stickers, big, you know, varied, user installable. But the animated GIFs...

Steve: You want to be able to see the expression on the cat hanging from a wire.

Leo: It is, you know what it is, it's nonverbal communication. And there's a subtlety to it that we miss in not being person to person; right?

Steve: Yes.

Leo: And we need to supplement it. And emojis and emoticons were the first way we did that.

Steve: And I have to, I confess, I'm a big emoji user. I love my little emojis. I just, you

know, I often sprinkle my stuff with them.

Leo: Better than emojis is sticker. Better than stickers, GIFs. I'm telling you. Plus with Facebook Messenger, just like with Apple's messages, you could send audio and video. You know what, today, for instance, I found some keys, and my son had been over with about 18 of his friends. And I figured, well, it's one of them. So at first I was going to message him, a text message: "I found these keys, they're blue, and they have...." And I said, what am I doing? I took a picture of it, sent him the picture saying somebody left their keys here. He sent it to all his friends. It was so efficient.

Steve: Got them identified, yup.

Leo: It was so efficient. It was so efficient. And I'm thinking, yes, this is the new era. Instantaneous, efficient communication. And you are going to be left out, my friend.

Steve: I'll let you know how it feels.

Leo: No, you won't, because you never talk to me.

Steve: Okay. So I'm not suggesting this to anyone. I'm only wanting to make sure people who care don't miss it. And that is that on the 14th, which is a week from Thursday - so that's, what, 10 days from now, yeah, today's the 5th - USA Network is premiering a new sci-fi series called "Colony," which is a post-alien invasion Los Angeles where you've sort of got your standard tension between the collaborators, the alien collaborators, and the resistance that's fighting them. And so I don't know what it's going to be like. I'm not suggesting it, recommending it. But I'm going to see if it's any good because, who knows, maybe we'll get lucky. "Colony" on USA Network, premiering on January 14th.

Leo: And "Mr. Robot" is coming back.

Steve: Yes, yes. They had a marathon. My TiVo caught one of them, for some reason, I don't know why. And it sort of got me overexcited. But it was Episode 3 of Season 1.

Leo: Change your OnePass to new shows plus replays.

Steve: Ah.

Leo: There's a setting for that.

Steve: Yes. I know about that.

Leo: I would have sent it to you via Messenger had you...

Steve: If I were only on Facebook.

Leo: If you were only on Facebook.

Steve: You could shoot me a picture of the settings screen.

Leo: Exactly.

Steve: And we have not talked about "The Expanse" on Syfy. As of tonight I'll be three episodes behind, so I just haven't been watching it. I will catch up. But so far it looks hopeful. So who knows. And I did just want - I talked briefly about the Vitamin D podcast at the top of the show. Many people want more health stuff. And after SpinRite is done, after 6 is finished, I'm going to try to make some time. It's just a matter of time. My head is all full of fun supplement stuff, but I just don't have time to do it. So, and I'm not going to steal the time before SpinRite's done because SpinRite people would be even more mad at me than they are for having taken the time away for SQRL.

I got a tweet from Nick Lozano, who said: "Steve, I was listening to a" - or actually a DM because it's long. "I was listening to a podcast" - oh, wait, Leo, did I hear you correctly? Tweets are going to have...

Leo: This is the Journal apparently published an article saying 10,000 characters would be the new tweet limit. But now there's some people saying, no, no, no, they just misunderstood, they're talking about DMs. Because DMs already are 10,000.

Steve: Right. And I and my followers are having a great time with that. We're sending long messages to each other. And then I thought, oh, no, not if they're just, I mean, tweets. Well, that would break - I think that would break too much of the existing infrastructure.

Leo: Yeah.

Steve: Anyway, Nick says: "Steve, I was listening to the podcast a few weeks back and heard some people would like to follow you on Twitter, but they don't want to create an account." And they also probably don't have Facebook Messenger. Anyway: "There is an iOS and Android app called Hooks that lets you follow a Twitter user and sends you a push notification when the person you select to follow sends a tweet. You then click on the push alert, and it opens a web version of Twitter right in the app. No account needed. There's also a bunch of other neat things you can do with it. Just thought some other listeners might find the app useful for following you on Twitter without having a Twitter account. Love the podcast. Listen every week."

And so I checked. It's called Hooks, H-O-O-K-S. It is iPhone only. That is, if iTunes is set

for iPad only, it doesn't come up. Boy, Apple needs to fix this annoyance. But it's from Hooks Technology. And for what it's worth, it looks like it does a whole bunch of other things, as Nick noted, in addition to allowing you to get notified from people you follow without needing a Twitter account. So my note about that before generated a lot of interest, and I wanted to share this with people who might be iOS or Android users. And it's free. And it didn't look like there were any in-app purchases, so it looks like it was really free, which is refreshing.

Something to consider for the New Year: It was interesting because this happened before today's announcement of a solution, or a potential solution. So a DMer requesting anonymity sent me: "I've been thinking for a long time about giving my LastPass password to a trusted individual, such as a friend." Very trusted. "In the event of my death, I'd like for them to be able to access my accounts without having to go through the rigmarole of proving my death to each site. However, while I'm still alive I would like to keep my LastPass account secure. I've been pondering using Shamir's Secret Sharing algorithm and giving parts to five different trusted people where four of them would be required to successfully recombine my LastPass password. Note I'm presuming my phone would still be intact, so the two-factor authentication part of my LastPass account would be simple to access. What do you think about this proposition? What are the downsides I'm not seeing? What are the upsides of this tactic? Instead of going on this complex route, what might be a simpler way to ensure my LastPass legacy lives on?"

So what was just announced this morning was a major update to LastPass, taking us to v4.0. And among the new features, basically it looks like there's a completely revamped user interface on the web interface, they also have what they call an Emergency Recovery feature. Joe tweeted, I think it was in response to a question that Simon Zerafa had, and he also mentioned SGgrc, so I saw it, that basically they were doing the same thing they were already doing using RSA public key crypto in order to make this TNO. I have not had a chance to dig into it, and I will, so I'll have a detailed readout for next week.

Shamir's Secret Sharing is something we've talked about long ago, a very clever approach where using some - there are two ways to do it. One is the heavy-duty math approach, which is what Shamir - he's the "S" of RSA, by the way - designed, where you could designate how many people are in the group, and how many of those people in the group are required in order to recreate a secret. And the idea being that - so, for example, you might have five people in the group, and any three of them are required to recreate the secret.

Now, there are some sort of simple-minded ways that you could do it, too. You could, for example, create a very long password and physically divide the password, for example, into sixths, into six equal-sized pieces. So say that it was 30 characters, for example, and you divide it into six five-character pieces, and then you numbered them one, two, three, four, five, six. Well, if you think about it, you could give each person a different set of three of them, or two of them, for example, or it's possible to work it out so that you would need a certain minimum of them to guarantee that, among that group, that subset of the whole, they would each have, of the pieces that have been given, all six, and thus able to recreate the entire password. That's sort of a simple way of thinking through what Shamir does with some serious crypto math. So that's secret sharing.

What it looks like LastPass has done is the typical, let's come up with a deliberate, but clear, softening of Trust No One in order to add a feature. So the idea is it looks like you can assign somebody sort of a provisional access to your account with a time delay so that they apply for access, and they can't get it for, for example, 48 hours, or presumably a delay that you specify, during which time you are notified of their

application and have an opportunity to deny it. So the idea being that, if you're dead, you know, we're not looking for this as a proof of concept, but if you didn't respond, then that time elapses, and LastPass makes your account available to them after that elapsed time. I think that's what Joe has done.

And I have no doubt that the implementation is solid and does what they say it does in a way that isn't making it any less secure than that protocol itself is. Clearly, this isn't foolproof because something could happen to you. You're stuck at the bottom of a mineshaft, during which time people think you're dead, but then you get pulled up out of the mineshaft.

Leo: I hate it when that happens.

Steve: Lo and behold, you're alive, but you were unable to deny this friend of yours and so forth.

Leo: Dead man switch.

Steve: So anyway, I think that's what it is. And I mention this as a New Year resolution kind of thing because this is increasingly important. If you think about it, for example, I might, to what degree the world uses SQRL, write down my rescue code and put it in an envelope and give it to my attorney, who I trust with other things like that, so that if something should happen to me, and people need access to my resources, there's a way to make that happen. But as more of our life goes online, this is something very much like a will, where it's neat that this person is reminding us, so, you know, we need to think about this. What happens if our family, after something should happen, needs to get to our stuff?

Leo: LastPass's password sharing is such a good solution. I use that, and that seems to be the way to do it, I think.

Steve: So someone else asked, he said: "Hey, Steve. Just wondering if you consider the NSA to be U.S. law enforcement. I ask because you refer to law enforcement when mentioning the Snowden revelations." And actually, even more broadly than that, I use the term a little bit loosely. I responded, saying: "I agree. I'm using that term loosely to mean entities with governmental powers. While the NSA doesn't have enforcement powers, it certainly has investigatory powers." So I said: "Yeah, I do mean to include them, as well." And a couple other people had said, hey, you know, NSA isn't law enforcement.

Leo: What do you call them? Okay, but what do you call them, if not law enforcement?

Steve: Yeah, I know. So I'm going to keep saying "law enforcement." For the record, I also mean the CIA, NSA.

Leo: Spooks.

Steve: People who typically don't, I mean, more than the DEA and the FBI.

Leo: NSA has an enforcement arm. It's called the U.S. Army. Strategic Air Command.

Steve: Yeah. Although that can't be deployed on the homeland, can it.

Leo: Well, nor can NSA.

Steve: Right.

Leo: Right?

Steve: Right.

Leo: NSA is, in theory...

Steve: Extraterritorial.

Leo: Extraterritorial.

Steve: Yup.

Leo: The CIA just uses whoever's got a gun.

Steve: So on the fifth, I'm sorry, the 50th, this is the 50th anniversary of the creation of Star Trek. And I thought, wow, was I 11? I guess I was. I got my start early. Of course, I'd already read Asimov's stuff, so I was...

Leo: Did you watch it in first run?

Steve: Yeah, oh, yeah.

Leo: I don't think I did.

Steve: And remember "Lost in Space"?

Leo: I loved "Lost in Space." "Danger, Will Robinson, danger."

Steve: Yes. And the salad monster? I remember my sister and I, like burying our heads in a pillow. We were terrified at the salad monster.

Leo: [Making terrified sounds]

Steve: Yeah. Yeah. Anyway...

Leo: Fiftieth anniversary, there's going to be a lot, I'm sure, to celebrate.

Steve: It turns out that Gene Roddenberry used some funky, nonstandard computers way back in the day.

Leo: Word processor, probably; right?

Steve: Yes, exactly, the very - and of course naturally he would be a techno leader because of course he created Star Trek and was a sci-fi author before that. So Ars Technica covered the story, with the headline "Files on nearly 200 floppy disks belonging to Star Trek creator recovered."

Leo: Wow.

Steve: And I think it was Dan Goodin...

Leo: I think Jerry Pournelle used the same computer. It's a Wang.

Steve: And Ars, I think it was Dan...

Leo: It's a Wang. It's a Wang.

Steve: Yeah, it may have been.

Leo: Yeah, I think it is. See, Wang diskettes. A Wang writer.

Steve: Oh, look at the colored key tops, yes.

Leo: Yeah, yeah.

Steve: Custom key tops. So I think it was Dan Goodin who wrote: "According to a press release from DriveSavers data recovery, information on nearly 200 floppy disks that belonged to Star Trek creator Gene Roddenberry has been recovered. The information on the disks belongs to Roddenberry's estate and has not been disclosed to the general public. DriveSavers notes, however, that Roddenberry used the disks to store his work and 'to capture story ideas, write scripts and take notes.' VentureBeat reports that the disks, containing 160KB of data each, were likely used and written in the '80s.

"The circumstances of the information recovery are particularly interesting, however. Several years after the death of Roddenberry, his estate discovered the 5.25-inch floppy disks. Although the Star Trek creator originally typed his scripts on typewriters, he later moved his writing to two custom-built computers with custom-made operating systems before purchasing more mainstream computers in advance of his death in 1991. The floppy disks were used with the custom computers, but unfortunately one of those computers had been auctioned off, and the other one was no longer operational. Roddenberry's estate sent the floppies to DriveSavers, which spent three months writing software that could read the disks in the absence of any documentation or manuals for the custom-built OS."

So not only were they from long gone computers, they were a format, they were not any format that is in use now. So they had to look at them, look at the flux reversal patterns. I'm sure they were FMs, frequency modulation recordings, so it's actually trivial to recover the binary. But then they'd have to look at it and figure out what kind of file system it had, reverse-engineer the file system - that would have been a project I would have loved to tackle. But anyway, it was done. And so it wasn't so much data recovery as it was format recovery.

Leo: I'm telling you. Just go - they should have called Jerry Pournelle, said, "What is, this, Jerry?" "Oh, I have one of those over here." No problem.

Steve: Yeah.

Leo: I guarantee you.

Steve: You're probably right.

Leo: Oh, of course. Jerry would look at it and say, oh, I know what that is.

Steve: Or, yeah, Gene got that one from me.

Leo: Yeah, I bet he did. I guarantee you he did.

Steve: And last of all, but not least, I got a tweet from Chris Ramsey. And I titled this

"Elaine above and beyond." Chris tweeted: "Elaine Farris at edigitaltranscription.com corrected my Hebrew when she transcribed my sermon." He says, "The.Best."

Leo: Wow.

Steve: And of course Elaine is transcribing these transcripts, and although they're not in Hebrew - in some cases for some people they may seem that way - she fixes all of the things that are questionable in what I say. So Elaine, thank you, and on to 2016.

Leo: Even if you say "Baruch atah Adonai Eloheinu," whatever. Watch, she's going to get that right. She's going to fix it.

Steve: She just got that right. Now we know. Leo, you can be fully off your leash.

Leo: I can do it in Hebrew. Hey, I've got a final note because, as I mentioned, I got the Tiny Hardware Firewall that I was talking about earlier. I haven't really configured it yet, but this is...

Steve: And it's got the built in - there's a VPN gateway, so it just VPNs you without doing anything.

Leo: Yeah. So you start the configuration by turning off the WiFi in your laptop, plugging this into the Ethernet port - I had to use an adapter because no laptop has Ethernet ports anymore - and then joining the WiFi on this device. And then you can configure it, change the password and everything. One of the things they say right away is change the default password. After the password has been changed, the THF - Tiny Hardware Firewall - asks you to log in with your new password. "Your username is still admin. Your password is now known only to you. Please do not write it on the bottom of the unit with a Sharpie." Good advice. That's in the docs.

Steve: Actually, I would write it on the bottom.

Leo: That's exactly where I'm going to write it.

Steve: Yeah. Yeah, because you're not [crosstalk]...

Leo: You'd have to have physical access to the hardware.

Steve: ...physical access, exactly. If someone's got physical access, the game is over. What you want is to have it handy and for no one to be able to get to it electronically.

Leo: And they say, "And don't forget it because we can't recover it. You're going to have to send this back and have the firmware rewritten because there's no way to recover this with a reset or anything."

Steve: I like their style.

Leo: I do, too. I'll have a report for you. So far it's worked exactly as described. I haven't yet started the VPN, so I don't know what the speed will be on that. That's always the downside of a VPN is the overhead. But I'll let you know next week. Next week a Q&A?

Steve: Yes, let's do it.

Leo: All right. Easiest way to do that, you can tweet him - by "him" I mean him, Steve Gibson - @SGgrc on the Twitter, 10,000 letters or less, please.

Steve: Oh, please.

Leo: You can also go to the website, GRC.com/feedback, and leave a question there. We'll pick 10 and answer them next week. That's a great place to go. And anyway, GRC.com is where you find SpinRite, the world's best hard drive maintenance and recovery utility. It's fantastic. Also all the freebies. You'll find out more about SQRL. There's a Vitamin D section there. There's a Health section with lots of good information. There are a lot of free utilities. Steve gives it all away. And you can even get this show there. And not only that, but Elaine Farris's fabulous, handwritten, beautifully transcribed Hebrew transcriptions.

Steve: Apparently in any language.

Leo: From right to left. And it's beautiful. No, she writes them in English. As long as the show's in English. Writes in whatever language we speak, apparently. That's all at GRC.com. We have audio and video, crazy enough, of the show at TWiT.tv/sn. But you can also subscribe, and I recommend you do, each and every episode available at all the traditional podcast sources. Just find one, look for Security Now! and subscribe, you'll get it every week. And you should because this is one show you do not want to miss. Steve, thank you. Happy New Year.

Steve: Leo, great to see you. Glad you had a nice trip. I had a nice vacation. And we're back on it for 2016. Here we go.