SECURITY NOW!

Transcript of Episode #648

Post Spectre?

Description: This week we discuss continuing Spectre updates, how not to treat Tavis Ormandy, a popular dating app where you'd really hope for HTTPS but be surprised to find it missing, the unintended consequences of global posting of fitness tracking data, gearing up (or not) for this year's voting machine hack fest, another record broken by a cryptocurrency exchange heist, bad ads and fake ads, the unclear fate of the BSD operating systems, a caution about Dark Caracal's CrossRAT Trojan, another way to skin the Net Neutrality cat, a bit of errata and miscellany, one of the best SpinRite testimonials in a long time, and some closing-the-loop feedback from our terrific listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-648.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-648-lq.mp3

SHOW TEASE: It's time for Security Now!. A security roundup today, all sorts of stuff to talk about. The latest on Spectre. Steve hears from a programmer who's hurt by his thoughts. He will apologize. And why Net Neutrality may actually find a savior in the state legislatures. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 648, recorded Tuesday, January 30th, 2018: Post Spectre?

It's time for Security Now!, the show where we get together with this guy, this guy right here, Steve Gibson, and talk about security and privacy online and bugs and all sorts of stuff. It's the geekiest show we do, thanks to the geekiest guy I know. Hey, Steve.

Steve Gibson: Hey, Leo. Great to be with you again for Episode 648 as we wrap up January and head into February in two days. We're still trying to get the whole Spectre and Meltdown thing behind us. And I'm really wishing that it wasn't two different words. I wish there was like a nice combined name for this, just because it's sort of awkward to keep saying Spectre and Meltdown. But it's really Spectre which has turned out to pose the biggest problem. Although Meltdown poses the greatest performance hit, it's easier to fix. So I titled this week's podcast "Post Spectre?" sort of in the hopeful...

Leo: Question mark?

Steve: Hopeful, yes, sense that maybe finally - but no. We do have some additional news about Spectre that we have to talk about. But some other interesting stuff, too. No really massively dominant story, although a bunch of interesting stuff for us to talk about, among them how not to treat Tavis Ormandy when he's trying to help you.

Leo: Ooh, don't mess with the Tav.

Steve: Don't mess - he'll just go take a shower, and you'll regret it. A popular dating app where you'd really hope for HTTPS encryption, but be surprised to find it missing. The unintended consequences, and I'm sure you're up to speed on this story, of global posting of fitness tracking data.

Leo: Yes.

Steve: And how that can bite you. Gearing up or not for this year's voting machine hack fest during the August upcoming DefCon. It's turning out to be a bit of a problem this year. We have another record broken by a cryptocurrency exchange heist. Bad ads and fake ads. The unclear fate - which this story caught me by surprise, but sort of certainly interesting to our listeners - the unclear fate of the BSD operating systems.

Leo: What?

Steve: Yeah. They're not doing that well. We also have a caution about last week's discussion of the Dark Caracal, in this case the CrossRAT trojan. Another way to skin the Net Neutrality cat. And in fact, just while we were setting up, another piece of news broke on what states are doing on their own about Net Neutrality. We also have a bit of errata, some miscellany, one of the best SpinRite testimonials we've encountered in quite some time. Historically we've had some really fun ones. Haven't really had somebody who exercised his creative writing abilities for a while, but we got one this week. And then we'll wrap up with some closing-the-loop feedback from our terrific listeners. So I think an interesting, fun podcast.

So we've been having a lot of fun in recent weeks with our Pictures of the Week. And this occasion there were just too many. We will have an overage of Pictures of the Week for at least several weeks while we catch up. So it was difficult to choose which one. One of the things that has happened is that the Meltdown and Spectre vulnerabilities have prompted the creation of a number of interesting twists on the Intel Inside logo. And of course so we have Meltdown Inside and Spectre Inside for this week's picture. Next week, unless it's preempted by something even better, we have another take on the older Intel Inside logo. And I almost used that for this week. But I thought, well, who knows what's going to be in store for next week.

Leo: I don't remember the older Intel Inside.

Steve: You will when you see next week's Picture of the week. It brings back some fond memories. But anyway, so just some more fun about Intel and their logos.

A couple things have happened on that front, on the Spectre and Meltdown front. Actually, Meltdown, as I mentioned at the top of the show, that got resolved quickly, although at some performance cost. It was the most expensive in performance for older machines that didn't support the PCID and Invalidate PCID features which were added, as we corrected the record on it was Haswell and subsequent have the Invalidate PCID instruction which works with the PCID feature that was introduced earlier but never used. So as long as you have that, you are able to mitigate the Meltdown problem without much performance hit. Earlier machines did take a hit, but that pretty much resolved things.

What happened, though, as we have been discussing the last couple weeks, is that Intel stumbled in - and no doubt they were under tremendous pressure and a great hurry. Although, as we understood the coverage, there were months going by in the late summer where they knew there was a problem, yet that hadn't come out onto the surface. Maybe they weren't ready to release yet, or maybe they were testing. Who knows. But as a consequence of that, as we were discussing last week, they made mistakes in the release of the firmware which affected apparently a large subset of their processors, maybe all of them.

Unfortunately, the disclosure was sort of deliberately murky, and it was squeezed out through the PR funnel that left us with more questions than it did answers. Since then, Microsoft has formalized their withdrawal of the support for that firmware. In other words, last week I was talking about, okay, well, if you're not having any problems, then just probably holding your breath is good enough. The Spectre liability, the Spectre vulnerability is protected. It's mitigated. And if your system is not having what Intel sort of obtusely says "more frequent reboots than usual," whatever that means, then leave well enough alone.

If you are having a problem, as we discussed last week, you could back out to an earlier version of the firmware offered in an earlier version of the BIOS from your manufacturer, which would probably be around since you would have just been able to update recently. And of course Intel, we discussed last week, formally said to all their partners, don't give anybody else this firmware. We're working on, like we now understand what's wrong with the firmware in a couple cases. We're working on fixing all of this.

Well, Microsoft since has gone a step further. They have issued a Windows update to disable the mitigation against the Spectre Variant 2, which is the focus of all of this. So their update is literally titled "Update to Disable Mitigation Against Spectre Variant 2." They wrote in this: "Intel has reported issues with recently released microcode meant to address Spectre Variant 2. Specifically, Intel noted that this microcode can cause" - quote, and they're just quoting everybody down some chain - "'higher than expected reboots or other unpredictable system behavior' and then noted [says Microsoft quoting Intel] that situations like this may result in data loss or corruption.

"Our own experience," Microsoft says, "is that system instability can in some circumstances cause data loss or corruption. On January 22, Intel recommended that customers stop deploying the current microcode version on affected processors while they perform additional testing on the updated solution. We understand," says Microsoft, "that Intel is continuing to investigate the potential effect of the current microcode version, and we encourage customers to review their guidance on an ongoing basis to inform their decisions.

"While Intel tests, updates, and deploys new microcode, we are making available an out-of-band update today" - and this is their KB4078130 - "that specifically disables only the mitigation against" - and then we have the CVE number. And I've got these things memorized. I didn't ever think I was going to be memorizing CVEs. But there's three of them. This is the Variant 2 of Spectre ending in 5715. That's the bugaboo in all of this. And that's the branch target injection vulnerability.

Microsoft says: "In our testing, this update" - that is, this one they've just released a couple days ago out of band - "this update has been found to prevent the described behavior." Meaning the higher than expected reboots, which is a good thing. "For the full list of affected devices, see Intel's microcode revision guidance. This update," Microsoft says - that is, their just released out-of-band yet another update - "covers Windows 7 (SP1)" - that is, the most recent service pack of Windows 7, the only one you'll ever get - "Windows 8.1, and all versions of Windows 10 for client and server.

"If you are running an affected device, this update can be applied by downloading it" - this is not going to be pushed to you, so this is the reason I'm bringing this all up is that our listeners have to go get it if they want it - "can be applied by downloading it from the Microsoft Update Catalog website. Application of this payload specifically disables only the mitigation against" - and then the CVE ending in 5715, that is, the branch target injection vulnerability. I have a link to it in the show notes. I'm sure, Leo, that the search for it will find it.

Now, what's interesting is Microsoft also goes on in this guidance to describe registry changes which will also do the same thing. And that is exactly what GRC's InSpectre utility does.

Leo: We should mention you probably shouldn't install this unless you're experiencing these issues, though; right? Or do you recommend people roll back even if you're not getting reboots?

Steve: Okay. So, I mean, this is why this is all somewhat controversial, that is, it isn't just cut and dried, black and white. There is still no known exploitation of any of this in the wild, even the Meltdown that was the easy one to do, that is, the easiest one to exploit. So these all remain theoretical vulnerabilities for which there is no reason to believe anyone is actively in danger from. So the biggest danger apparently is from turning on this feature with both the faulty Intel microcode and Microsoft's enabling this feature which causes some system instability. That's the biggest problem that has ever been seen from all of this is the mitigation of this problem.

So my Twitter feed has been full of feedback from people. I've seen some reports of people believing their system became less stable, who then disabled or backed out, and things seemed to be better. But it's all kind of like no one has been able to firmly find a test for the problem or invoke the instability and conclusively demonstrate that, oh, now it's gone again. So I think my advice is what it was last week, although now we have another piece. Last week was back yourself out of the microcode if it's causing a problem. Now, since then, Microsoft has said we'll back you out by giving you a link you can click to give you another "go get it if you want it" update which does the same thing as just turning it off. That is, even if it's in your microcode, if you turn it off, the instability goes away.

Now, that's news. I did not - I couldn't assert that last week because I always, as we know, I built that in to InSpectre from the beginning. There's cute little buttons down there at the bottom of the InSpectre app which you can just press, and it'll turn off the Spectre or the Meltdown, you've got a button for each, mitigation. So now Microsoft has confirmed that turning it off prevents the instability. So you could either download

Microsoft's thing that turns it off, and then I'm not sure how you turn it back on again, which is one problem. I mean, I guess maybe...

Leo: Presumably there's another update coming from Microsoft at some point that would fix it.

Steve: Where it's like, okay, everything's finally good.

Leo: Whenever.

Steve: Exactly. Whenever that happens, yeah. So you could use InSpectre to flip it off, and then you could flip it back on again. But arguably you would be waiting in any event for newer microcode which doesn't have this more frequent rebooting side effect. And then Microsoft, once everyone's sure we've got it this time, Microsoft will send us another update out of band or in band or some, you know, who knows what the band will be playing at that point. And then we could all move forward.

Also InSpectre got a revision because we found a bug in the Creators Update, not the Fall Creators Update, that is, the Fall Creators Update is 1709 of Windows 10. It turns out that 1703 had a bug. The 32-bit support in Windows turns out to be completely different than the 64-bit support. Back once upon a time, the Windows API was 16 bits. And then of course they went to 32. Those were very similar. That is, you were able, in fact, you could load 32-bit code into a 16-bit process and call it. But you can't do that with 32 and 64. They are completely different.

Well, it turns out that InSpectre, my code, is a 32-bit app. And the 32-bit app, as all 32-bit apps do, calls a 32-bit API. Well, there's a function in Windows, a DLL, ntdll.dll, which exists in both 32- and 64-bit flavors. And we discovered, actually it was a researcher in the GRC newsgroups, discovered that, because users were reporting who were using the Creators Update 1703 that InSpectre was saying they were not protected. But the 64-bit version was saying they were protected. Well, it turns out that there's a bug in Windows 32-bit implementation of ntdll in the Creators Update, which they fixed in the Fall Creators Update, but it persists in the Creators Update.

So I had to scramble around, and I wrote my first 64-bit assembly code last week. I created a 64-bit probe which is contained within the 32-bit InSpectre so that, if it sees it's on a 64-bit system, it launches this 64-bit probe into the system, which is the only way for it to get a view of reality in light of this buggy implementation of ntdll.dll in the Creators Update. So we're at Release 6. Oh, and Leo, while I was there, I also implemented the fix that we talked about last week which is inverting the sense of Yes and No in the presentation.

Leo: Oh, good. Nice. I'll download it right now.

Steve: So if you get a green Yes, that's good, instead of getting a green No, which was confusing. So now if you get Yes/Yes, that's the good news. And the no's with an exclamation point are red. So that's been fixed also. And we're at about 355,000 downloads. So we're trucking along and doing well and continuing to get good attention and coverage. And it's helping people. So now we know that, if you feel that your system is unstable, you don't have to back out of your microcode. You don't have to update and go out and get the out-of-band patch unless you want to.

And in fact, it may be that that thing only sets the registry. I don't know what it does. But they all - because Microsoft also said, "Or you can do this to the registry." Which InSpectre does for you, and safely, and reversibly. So lots of options for our users. And it's confusing. There's no known exploitation of these vulnerabilities. The ones that are causing the biggest problem would be the hardest to exploit, so we would expect to see them maybe taking longer to happen, if they even ever do.

The biggest problem, as I mentioned, is the cure is worse than the disease in this case for many people. All of our systems are running more slowly for apparently no good reason at the moment. But again, better safe than sorry, I think. In this case, certainly if you suspect that your system is misbehaving in any fashion, then turning off the Spectre mitigation until we get updated firmware from Intel certainly would make sense. And Microsoft is sort of saying, you know, data loss or corruption. Meaning that's kind of more scary. At least a reboot is like, ooh, whoops, we crashed. If it actually could cause, and I think that's what Microsoft is saying, data loss or corruption, I don't know if that's with the reboot or silently without it bothering to reboot, but that's of concern, too. So, yeah, I don't know.

Leo: Yeah. I'd heard the same thing.

Steve: Yeah. So anyway, that's an update on the gift that keeps on giving the industry. And certainly once - and I'm sure that Intel is working hard. They said they understand what's going on. They're not sharing it with us, which is really my only source of angst is it would be - we're just sort of dealing in a vacuum, and this podcast likes to have facts to deal with. And so, like, oh, it's worse than it used to be. More reboots than usual. What? You know, it's like, okay. Okay. So speaking...

Leo: We should mention that we were talking about this on MacBreak Weekly, and I knew you heard this.

Steve: Oh, good, what?

Leo: Apple had wisely avoided using the Intel fix. They did the calculus that we've kind of done which is, well, since there's nothing out in the wild, let's patch it on WebKit on our browser because that's the only exploitation vector that we really know about, and we'll wait until Intel gets it right or, I mean, it sounds like they kind of sensed there was something wrong with the Intel fix, and they didn't...

Steve: Well, and remember that Google was also very quick with their very clever Retpoline solution.

Leo: Right, right.

Steve: Which does require code recompilation, but Apple is able to recompile their code in order to implement that fix.

Leo: Yeah, so, hmm.

Steve: So Tavis, our great buddy at Google, who just everywhere he looks it's like with this amazing fine-tuned precision ability to find vulnerabilities and help the industry get smarter, has decided to take a look at highly popular online gaming, thinking, eh, nobody's looked over there with his level of expertise. It turns out that last month, last December, he took a look at Blizzard's company-wide, distribution-wide download and install and maintenance facility and found a significant problem. This affected World of Warcraft, Overwatch, Diablo III, StarCraft II, the entire catalog of extremely popular Blizzard online gaming.

He reached out to them as he does for full responsible disclosure, opened a dialogue, explained the problem that he found, provided them with a proof of concept which allowed - get this - any website to leverage the lack of strong authentication in Blizzard's entire suite of gaming to allow it to download and install and run arbitrary code on any gamer's machine. Whoops.

Unfortunately - and who knows what the politics is behind this. But I don't think whoever it was he talked to at Blizzard knew who he was because they stopped communicating with him. They went silent, cut him off, and then implemented a fix that didn't work, without any further interaction. They then went public with their great ballyhooing, we care about security, we fix things. And Tavis said, uh, no, you didn't. That's not a good fix.

And the bottom line is, after a little bit of embarrassment and backpedaling, somebody more mature or more aware of what's going on in the industry said, oh, shoot, yes, Tavis knows what he's talking about. Apologies were made. Dialogue was reestablished. Blizzard then said that what they put out was something that they had around for a while, and it wasn't really meant to be the permanent fix, but they're doing one now, and they'll have it online soon. And Tavis said, well, okay, good. And so they've reestablished communication with him. And with any luck they will involve him in their proposed solution this time, and he can take a look at it and say, yes, that looks good. And this is of interest to all other major online gaming companies because Tavis has since decided that he's going to look at the other ones.

So if you're not Blizzard, and you have been watching this happen, make sure Tavis has a way of getting a hold of you, and listen when he tells you that he's found a problem. Don't be embarrassed. Don't suddenly pull the rug in over yourself and hide. Just work with him, fix the problem, and that'll be the path to least resistance. So those of us in the security industry, and we talk about this all the time, have learned that - certainly, for example, the guys at LastPass respond within minutes of Tavis contacting them and saying, whoops, I found a problem here, as does everybody in the security industry. So Blizzard probably now understands that Tavis and Google and Project Zero are valuable components of this industry that should be taken advantage of when offered freely, as they are.

Some researchers at a security firm in Tel Aviv named Checkmarx took a look at Tinder's iOS and Android mobile apps and were surprised to find that it lacked HTTPS encryption, if you can believe it or not. Anyone sharing the same WiFi as an iOS or Android mobile Tinder device or Tinder app user can see your Tinder photos, add their own into the photo stream, and track what you do on Tinder. They're not using encryption to keep the photos safe from anybody who wants to eavesdrop. And although apparently they are using encryption for encrypting the actions of a Tinder user, the encryption is spotty. And it turns out that even looking at the encrypted stream it is possible to ascertain what the user is doing.

So Checkmarx produced a proof-of-concept app called TinderDrift which is demoed on YouTube which reconstructs any Tinder user's online session of what they see and the way they respond to what they see, essentially unmasking any person's behavior who is using Tinder on a shared Ethernet medium like WiFi. So although, again, the swipes and matches are encrypted, Checkmarx explained, and approved, hackers sharing the same WiFi are able, essentially, to completely unmask everything that is being done. It turns out that the specific patterns of bytes that represent a left swipe, a right swipe, a super like, whatever that is, and a match, are all clear.

Even though technically they're encrypted, nobody at Tinder really gave the security of their application much thought, apparently, or any real concern over protecting the privacy of their users. The Verge in their coverage asked Tinder to respond to this. And so Tinder did respond, saying that the unencrypted photos are profile pictures, and Tinder is a free global platform, so the pictures are "available to anyone swiping on the app anyway." Of course, what isn't free and global are the individual Tinder users' choices and reactions to those unencrypted, unprotected photos which this research demonstrates was poorly concealed.

So I'm glad, again, this is, I mean, we just keep seeing example after example. I mean, we just talked about it with Tavis and Blizzard, and here now Checkmarx in Tel Aviv and Tinder, where we have to have oversight. We have to have an environment where security firms and researchers are able to examine these things. And I'm thankful that they're willing to volunteer their time and do so. They bring some beneficial positive press to themselves for doing so, and in the process it's benefiting the users of these applications for which it's clear not enough attention has been given to security.

Which is the perfect segue to, Leo, this was - for a while I kept trying to sort of ignore this story because I thought, really, this is bad? This is a story? Finally I was just overwhelmed by it. It was without a doubt the most tweeted news item this week. And that is the unintended consequences of globally connecting your fitness tracking devices, and what happens when arguably position-sensitive personnel are tracking their fitness with them, specifically U.S. military personnel.

Turns out that the Pentagon, I mean, military personnel are probably already fitness-oriented, and they're going to be using Fitbits and similar tracking devices. Turns out that the U.S. Armed Services has even taken to giving personnel these devices to encourage them and their fitness. And what came to light was that there is a firm that had been collecting all of this data and aggregating it globally and pushing it through mapping software. What it turns out you're able to do is essentially it creates a heat map of where people are all over the world who are using fitness tracking devices. And so my first thought was, okay, well, yeah, duh. So what?

But it turns out there are many places where our military would not want confirmation of their personnel. And although this, I mean, this doesn't deanonymize these people, you can't use it to prove what is going on somewhere, any bad guy can pinch and zoom and pan around and wonder, okay, wait a minute, what is going on here, and what is going on here, and what is going on here, and what is going on there? So it certainly does clearly represent a leakage of information of the potential position of people which you would not otherwise have. You might presume to be maintaining radio silence where unfortunately your fitness tracking device knows, is receiving GPS coordinates, storing it, and then uploading it somewhere where it's being aggregated.

And so this sort of creates an end-around disclosure of the position of these things which may be worn by military personnel, maybe in locations where we would rather not have, or, I mean, anybody would rather not have any disclosure that people are running along a certain trail in a certain location in the world. And yet now it's all public.

Leo: I wonder if you can fault Strava for releasing this data. The other question we had is - because Strava you can turn on private so that you're not sharing. But it's not clear whether this data released - it's private because it's not any individual. But if it's in aggregate, including private information, in other words, if it would be enough for the military to set private and then go for a run, and but still Strava has a heat map. It sounds like that's what happened. And that they released it is to me, like, come on, guys. Nevertheless, the military has changed their procedure, and they will be strongly encouraging people not to do that anymore.

Steve: Well, and I'm sure, no doubt, that military minds are themselves pinching and zooming and looking to see what is now in the public domain. I mean, now...

Leo: Well, all this satellite data was already out there; right?

Steve: Right.

Leo: So they know, I think they know where the bases are. The one weird use case was if a base was pretending that it was closed, and then you saw people running around...

Steve: Like deliberately being dark.

Leo: Yeah. But like, if you look at, on the Strava heat map, if you look at the Pentagon, it's actually quite interesting. We showed it yesterday on TWiT.

Steve: Oh, cool.

Leo: And you could see people running around the Pentagon, but it's completely dark inside the ring. And at first I thought, well, nobody's getting exercise inside the ring. But really it's not that. It's that that's radio hardened. Nothing's getting out of the ring. Of course.

Steve: So no device that is in there knows where it is, yup.

Leo: Doesn't matter if you're wearing your Fitbit. Yeah, of course not. And I bet you if you looked at the same thing, if you looked at the White House or anyplace they're trying to keep it secure; right?

Steve: Yeah. And at the same time, black zones are information, too.

Leo: That tells you something, too, yeah.

Steve: Yeah.

Leo: That's interesting, yeah. Leave it at home, kids.

Steve: So anyway, I mean, this is the consequence of a world where everything is connected to everything else, and we're still learning how to handle the power of this kind of information. Speaking of which, voting machine makers...

Leo: Oh, this is - 2018 is nine, 10 months away; right?

Steve: Yes, are telling - yeah. Voting machine makers are trying to stifle the sales of decommissioned and resold voting machines by threatening eBay sellers with litigation if they sell these machines, telling them that it is illegal to do so, which it is absolutely not. So we all remember all the fun we had last year, after last year's DefCon, which was the largest of the Voting Village - DefCon hosts this Voting Village competition where they collect just a completely heterogeneous assortment of voting machines and tell the hackers, okay, have at it, kids. Let's see what you can do.

And last year's was the biggest by far. It had been going on quietly at DefCon, but it sort of really got a lot of attention last year. And what we learned and had fun with on this podcast was the horrifically poor security that the machines actually had. Well, we had fun with it. Of course the voting machine manufacturers did not. They are not happy. And as I said, they've been actively threatening sellers of used and retired machines with legal action should their machines be resold, even though doing so is completely legal.

So remember last year we talked about this. I mean, there were machines that all had, I think it was Sequoia machines all had the same hard-coded password across, I mean, like, all of them had it.

Leo: Well, that's for convenience, you see.

Steve: Correct. You wouldn't have to write all those pesky passwords down.

Leo: Just put it in the manual.

Steve: Yeah, yeah. Some lack any security, apparently, at all. Some could be penetrated without physical contact to the device. In some cases a USB thumb drive had to be inserted, but not all. Some just offered you the convenience of WiFi. Many had software that was riddled with well-known vulnerabilities that have been documented for years, if not decades, that had never been patched or updated. Most machines had never been wiped. And in some cases there were machines that had - there was one case had a 600,000 voter registration database still present in it that was available for exfiltration from this machine. I mean, so it was an embarrassing catastrophe for voting machine companies and voting machine security in general.

Well, in preparation for this year's upcoming DefCon, the Voting Village organizers indicated during their own talk at Shmoocon, they told attendees at the Shmoocon hacking conference that they were having a surprisingly difficult time preparing for this year's upcoming DefCon Voting Village event because they were having a hard time acquiring machines after what happened last year. And what they learned when trying to buy machines was that the, as I have said now, the manufacturers were threatening one of the most popular sources of these machines for resale, which was eBay, eBay resellers receiving notices threatening them with legal action should they sell those machines.

So for what it's worth, if we have any eBay resellers within earshot of this podcast, there is nothing illegal about reselling these machines. It is perfectly legal, as is their hacking. And I will say again, this is the only way we're going to get security. I mean, until recently, these electronic voting machines have been allowed, I mean, even from well-known companies like Diebold have been able to say, you know, we're a security company. Trust us, these machines are secure. Turns out absolutely not true. Remember, there was not a single machine that withstood attack last year. Not one. Some of them collapsed within minutes. Some took maybe an hour or two. Not a single one survived attack, which is just - should be just beyond embarrassing for these companies.

And so my feeling, of course, is that no machine should be allowed to be used that hasn't had full, well, first of all, they ought to be open source. They ought to be fully scrutinized. They ought to have academia looking at them, saying yes, we find no problems with these. And then that machine should be produced. So this notion of proprietary software in voting machines for something like U.S. elections, that absolutely has to end. It is the wrong way for this to have been done. And these chickens are coming home to roost.

So we have broken a record again on the largest heist in a cryptocurrency exchange. We all recall when, four years ago, back in 2014, Mt. Gox, which at the time was one of the largest bitcoin exchanges, ended up filing for bankruptcy after admitting that it had lost $450 million worth of bitcoins. Well, it turns out that now, just a few days ago, Coincheck, which is a Tokyo-based cryptocurrency exchange, has suffered what appears to be the largest hack of cryptocurrency loss in history, totaling what would be $532 million in digital assets.

In a blog posting, they acknowledged or confirmed the cyber heist. However, they did not explain how the tokens were stolen, and then froze most of the assets and their services, including deposits, withdrawals, and trade, because no doubt they want to figure out what it was that happened. Interestingly, though, they did not freeze their trading of bitcoin, which did take a 5% hit in its market valuation on this news. So anyway, I mean, I guess this is the problem with - it's an acknowledged problem, even though this is a huge, more than half a billion dollar loss. We're seeing people having problems maintaining the security of their cryptocurrency constantly.

We have often said that it is incredibly difficult, if not arguably impossible in a complex enough environment to have true security, and that you only have security to the degree to which nobody is trying to penetrate the barriers that you have erected to protect yourself. And so money is money, and where there's money there's going to be pressure to penetrate security. So it looks like, I'm sure, that other exchanges are taking lessons from these massive losses and doing everything they can to protect themselves. Individuals need to do the same.

Those individuals who have substantial assets in cyber currency need to really, I mean, the only thing you can do, I think, is to store it offline. And that's a common refrain of mine when, for example, I've talked about the QR codes that I use for registering new devices' authenticators. I understand it's inconvenient to have them offline, but it's the only way to be safe. And the same is certainly true of cryptocurrency wallets. You want to keep them offline when they're not in use because, if it's online, it's vulnerable. So certainly these guys, Coincheck, have learned that lesson, or presumably learned that lesson. I hope other exchanges have.

In I guess what would be foreseeable, it came to light from an advertising security company - and I didn't know there was an advertising security company, but I'm glad there is advertising security. Confiant is the name of this company that discovered the existence of a very large and malicious advertising operation which they named Zirconium, which I thought was kind of a fun name for a fake advertising, I mean, a huge fake advertising effort.

This Zirconium operation created 28 completely fraudulent fake advertising agencies and established them with full-blown apparent credentials, Facebook pages, LinkedIn accounts. They created fake people to populate them and created fake personas for them, basically erecting an entire 28 separate agencies in order to funnel and mask their advertising. It was so large that Confiant determined during the peak of their activity the group was purchasing 62% of ad-monetized websites on a weekly basis. So just a large machine.

Confiant believes that about 2.5 million users who encountered Zirconium's malicious ads were redirected to a malicious site, with about 95% of those 2.5 million users being based in the U.S. Essentially they purchased over a billion ad views last year in 2017 and used these malicious ads to redirect users to tech support scams and malicious pages peddling malware-laden software updates and software installers.

So unfortunately what was done was, and this is the technology we've talked about often, is that the ads have the ability to run JavaScript. And they used something that they described as JavaScript code executing a forced redirection to hijack visitors' browsers' queries that were trying to just display an ad on an ad that was on some website. The browser was redirected in a series of bounces, first to a server, an intermediary domain that would fingerprint and classify the incoming traffic, then redirect the user to another domain operated by Zirconium where they would then be sent to a third domain which was an affiliate traffic jumping-off point which allowed others to buy traffic which had been hijacked from legitimate sites.

So essentially this was, I mean, this was arguably not the fault of the websites hosting the ads. They thought they were hosting legitimate ads. But essentially 28 full-blown fake ad agencies were created specifically for the creation of malicious advertising. And they were often offering fake malware-laced Flash Player updates, which as we know has been historically and is still not completely gone away, a means of getting malicious code into people's machines.

So anyway, I thought this was interesting because this gives us a better sense of the scale to which malicious advertising is being deployed. And during the same period of time, well, actually not all of 2017, but just in the last couple weeks, YouTube was hit with Coinhive cryptocurrency mining advertising. It turns out the good news is that antivirus software is now up to speed about Coinhive. And so what set off alarms is that visitors to YouTube were having their antivirus tools firing off warnings that cryptocurrency mining was going on. And sure enough, 80% of their processor was being used, leaving just enough unused to play videos. So essentially, while people were watching YouTube videos, the rest of their system was being commandeered for Monero cryptocurrency mining with Coinhive. Trend Micro, that of course is one of the major AV monitoring folks, providers and monitors, said that the ads drove a more than threefold spike, that is, the YouTube ads, the ads appearing on YouTube, more than a threefold spike in web miner detections during this period of time.

A Google representative who was asked about the incident by Ars Technica, that was one of the outlets reporting on this, told Ars Technica that mining cryptocurrency - this is Google, the owners of YouTube - "Mining cryptocurrency through ads," they wrote, "is a relatively new form of abuse that violates our policies, and one that we've been monitoring actively." They wrote: "We enforce our policies through a multilayer detection system across our platforms which we update as new threats emerge. In this case," they wrote, "the ads were blocked in less than two hours, and the malicious actors were quickly removed from our platforms."

Well, unfortunately, Ars observed that it wasn't clear what the representative meant when saying the ads were blocked in less than two hours. Evidence supplied by Trend Micro, and on other social media where there was an outcry about that, demonstrated that the ads containing substantially the same JavaScript ran for as long as a week on YouTube. And then, when queried about that, the Google representative did not respond to Ars' follow-up questions looking for a timeline of when the abusive ads started and ended.

So again, this is a moving target. Nobody has found a way to be completely clear of these sorts of attacks. All you can do is respond to them as quickly as possible. And as we've talked about here, because it's necessary for users' browsers to go obtain the script from Coinhive, blocking the Coinhive domain, as we covered several weeks ago, or using some add-on such as uBlock Origin or one of the good monitors of these sorts of domain queries, should keep at least your own machine from being commandeered for this. But of course it's an industry-wide problem.

CSO magazine had an interesting piece that caught my attention, which was brought to me thanks to one of our listeners, posing the question whether the BSD versions of the open source Linuxes are dying. And apparently some researchers believe...

Leo: Wait a minute. BSD versions of open source Linux, those are two different things.

Steve: Well, okay. Well, BSD, like OpenBSD, FreeBSD, and NetBSD.

Leo: Yeah, those are not Linux, yeah.

Steve: Oh, god, I'm sorry, I meant Unix. Thank you for catching me.

Leo: You scared me.

Steve: Just purely misspoke.

Leo: No, but I think it is the success of Linux that's starting to make these other versions go away.

Steve: Correct.

Leo: You and I both are BSD fans.

Steve: Correct. And I have been forever. But ultimately I suspect that the open source ecosystem may not need nor be able to support more than one, like one winning open source solution. And I think it's very clear that that solution is going to be Linux.

Leo: In a way that's too bad. Somebody said, I have a quote in my blog, and I'll go look and see who said that, that Linux is a POSIX-compliant Unix designed by PC users. Let me see if I can find the quote because it's a great quote. And BSD is designed by Unix users. And PCs are kind of secondary to the whole point; right?

Steve: Yeah. So while you look, I'll just provide a little bit of background here. So we have three of them.

Leo: There's many, actually.

Steve: Yeah. The top are OpenBSD, FreeBSD, and NetBSD.

Leo: There's also PCBSD, which is now TrueOS, which is a very popular version, as well. So there's a lot of them.

Steve: Didn't that branch from FreeBSD?

Leo: TrueOS. I mean, many of them have been branches. But at this point...

Steve: Yeah.

Leo: This is Matthew D. Fuller: "BSD is what you get when a bunch of Unix hackers sit down to try to port a Unix system to the PC. Linux is what you get when a bunch of PC hackers sit down and try to write a Unix system for the PC." That's the difference. It's more pure Unix-y. Right?

Steve: Yes, yes. And frankly that's been my affection for it. OpenBSD is regarded to have the highest security because security has been its primary focus from the start. And in terms of like bugs found in the kernel, it supports that, I mean, it's living up to its promise. FreeBSD is regarded as the most advanced and feature-rich, though that has come at some cost in security because, if you let your guard down, as we know, bugs are going to creep in. NetBSD is regarded as being the least secure because its focus has been upon having the widest run-on-anything profile, supporting any device and any platform.

And again, there's going to be a security consequence of just having a lot more legacy driver code so you can continue to run on really old hardware which is not being supported, and nobody is really scrutinizing very much anymore. And so the argument has been that, as a consequence of just a lack of eyeballs - and that's really what it boils down to, a lack of eyeballs looking at the kernels of these BSD operating systems. They don't have as many people looking at them. In some cases vulnerabilities that are reported are not fixed in a timely manner, where they are with Linux.

And again, FreeBSD has been my non-Windows Unix OS of choice. And I wouldn't be surprised to find that if in time these alternative OSes just sort of - they just slow down and stop being developed because there just isn't enough steam behind them. And I do wonder if, fundamentally, there is enough interest to support more than one primary, nonproprietary, open source alternative. And we know what that would be. That would be Linux.

Leo: I don't know.

Steve: Kind of probably inevitable.

Leo: Yeah, I think it is. Hardware support is a real issue in the PC universe. That takes a lot of people banging on it. And then frankly the presentation layer on BSDs are just - it's not as elegant looking.

Steve: No.

Leo: And so I don't - and that's somewhat related to hardware support, I guess. But anyway...

Steve: Yeah, yeah. And the other thing is that a lot of them are beginning, and we're seeing this, they're beginning to cross-borrow chunks of technology because they can't afford to just redevelop the same thing independently. So it's like, oh, well, yes, we borrowed this from that. We like the network stack from this OS, and we're compatible with these graphics drivers because they just can't afford to have them all rewritten from scratch.

Leo: Yeah.

Steve: But again, I just thought that was an interesting little tidbit is what we're seeing is we're seeing them, some of the fervor dying off. Also you really have to be a serious hardcore developer to be mucking around in the kernel of one of these operating systems and not create more trouble, like more problems than you solve. So you can have the best of intentions, but it's a little bit like how the U.S. space shuttle system began having a problem at NASA because all the engineers that designed it and knew how it worked had retired.

And so that knowledge, they took the knowledge of how the shuttle systems functioned with them. And so you could have really freshly minted, energized young people wanting to come in, but they were looking at this stuff saying, "Uh, okay, why exactly is there bubblegum stuck over here? Is that important?" And the old guys would say, "Oh, yeah, yeah, yeah, don't touch that. That rebalances the kravistat, and we need that." That was carefully calibrated bubblegum, but the new guys wouldn't know.

So I got a kick out of some of the reporting of this, talking about undetected CrossRAT malware. And I thought, well, okay. Or undetectable. The headlines were saying, and this is, remember, the CrossRAT is the trojan which the Dark Caracal is using, written in Java, cross-platform, runs on Windows, Linux, and macOS. And some of the coverage said that it was undetectable. No. It is currently undetected, but there's nothing about it that is fundamentally undetectable. At the moment, and this is the useful cautionary about this, only two out of the 55 AV scanners at VirusTotal are detecting the Dark Caracal's CrossRAT trojan, the remote access trojan, as malicious. Which that is certainly a concern.

On the other hand, this all just became public a week ago, and I'm sure that a week or two from now the detection count will have jumped up to nearly all of the AV scanners. As we've seen, today's AV uses patterns and heuristics. And there are certainly features in Dark Caracal, that is, in this CrossRAT trojan, that any AV could lock onto. For example, there is a very well-known domain which CrossRAT currently uses for its command-and-control server. All anyone would have to do is scan for the presence of that domain. The problem is that, as soon as that was unmasked, it was changed. So what we need is we need a more mature analysis of CrossRAT in order to come up with some signatures that will reliably detect it, even when it changes.

Now that it's on everybody's map, I'm sure that all of the AV tools will be getting samples of it and will be adding detection of it to their suite. And of course, as our listeners know, the first version of InSpectre set off just about every alarm that there was across the AV industry for no reason except that I had used a registry key that was regarded as "sensitive" because it's the one that I use for flipping the protection on and off. And it wasn't that I was using that key for that purpose. It's just that it is a sensitive access key.

And so unfortunately all I had to do was obscure my use of the key. Once I saw what was happening, I figured out what it was that was probably the problem, and I encrypted the key, and then I decrypted on the fly. So this sort of demonstrates that it is, I mean, this is the cat-and-mouse game that malware and antimalware go through is that, as soon as a piece of malware is detected, if it's able to determine what it is that it's doing that's setting off the alarms, it can hide itself. And thus the cat-and-mouse game that is going on constantly.

In this case there's nothing, there's no real concern about this CrossRAT trojan being undetectable. It's just currently not detected. What I would remind our listeners, the takeaway is that it's written in Java. And I understand that there are valid uses, especially within enterprise, for using Java. The advantage of Java is that it is cross-platform, and there are legitimate uses and applications for Java. But they're not super mainstream. So most users do not need Java installed on their systems. It is not by default installed in systems, so it needs to get added for some reason. So as long as you do not have Java in your Windows, Mac, or Linux machine, then this Java-dependent trojan cannot run on your system.

So I would say be aware of whether you have the Java Runtime present. If you do, and you don't need it, remove it. And be aware of anything that installs it because it itself is not dangerous. But we are seeing instances, I mean, traditionally when Java was exposed to the browser, that was a source of constant problems. We solved that problem, and Java now by default finally is not available to the browser, thank goodness. Not having it around at all is even better. And if you don't need it, make sure you don't have it because it can be used for mischief.

And in a last bit of news, just as I was - literally, like minutes before we began recording the podcast, I got the news that the California Senate had approved a similar action, actually this one had more teeth in it, than what Montana, that was first, and then two days later, just recently, New York State's governor both signed into orders. There is state-level pushback on Net Neutrality, that is, on what Ajit Pai has done with essentially overturning the existing legislation, as we've covered and as been covered throughout the TWiT network recently.

What the states are doing is sort of clever. They're using their purse, the power of the purse, or their purchasing power, in order to effectively enforce Net Neutrality within their states. These governors are signing executive orders, and we can add California to this list. It's got to go to the State Assembly for ratification, but it's virtually assured to pass. Unfortunately, this is ending up being political and partisan. And so what we're seeing is votes are falling down along Republican and Democratic party lines, but the Assembly in California, something like 58 to 23 Democrat majority. So given that that same party line vote occurs on this issue, it's virtually certain to pass in California.

So we'll have a number of major states who are saying that no state-funded organization or facility can purchase Internet services from any provider that does not honor neutral handling of bandwidth, that is, Net Neutrality. So New York is a massive consumer of Internet, that is, New York state services and facilities, and certainly that's the case in California, as well. The providers, of course, are now asking for legislation to outlaw this kind of state-level action.

So this is all not done yet. But for now states are exercising their independent rights, saying, okay, fine, if there's no federal policy to prevent this, then we're not going to allow any purchasing of bandwidth from providers at the state level, and we'll take it from there. And certainly no provider would be willing to give up all of the access to the amount of money that large states are spending on bandwidth in order to play games with their bandwidth.

I didn't know where to put this. I put this under Errata only because it was kind of harsh. But I thought, well, it's an opinion I wanted to examine. Someone named Ryan Dey tweeted: "I didn't appreciate the flippant nature of your coverage of Intel's Spectre mitigation work," he wrote. He said: "Speculative Execution has been a business-as-usual feature for a long time" - no argument there - "and there are a lot of people working very, very hard to reengineer the microcode and change everything on a dime.

Your disrespectful remarks on their less-than-perfect first efforts doesn't help anything, and likely insults many young coders who view you as a role model."

So that kind of caught me by surprise, but I thought, okay. If there was any confusion, I just wanted to say that, I mean, I understand how difficult this is. And I'm impressed by the idea that microcode can be flexible enough to surface these sorts of features which were not intended and designed in from the beginning. So by no means am I intended to demean, or did I intend to demean the efforts or to make light of the difficulty that doing this presents.

What I expressed my dismay over was Intel's presentation of this. They apparently know exactly what's going on. This is not a security issue any longer since we've had full disclosure of exactly what the vulnerabilities are with demonstrations and proofs of concept of these problems. What annoys me is that we're getting a lot of hand-waving from Intel. They're saying, oh, well, describing this as "more reboots than usual." Well, tell us what's going on. Tell us what the problem is. Tell us what you know, Intel. And Intel is not doing that.

And so, again, everyone who listened to this podcast knows how well I understand that anybody can make a mistake. Mistakes get made. What matters is the way you deal with them. And dealing with them is about communication as much as it is about engineering in this day and age. So what I took exception to and still take exception to is the PR spin and the obfuscating that Intel is subjecting us to. They could tell us, as apparently they know, exactly what is going on. If we had that, I would have no complaint with Intel. So it's not the engineering. It's not the coding. It's not the work of the people who I'm sure are scrambling around like crazy. It's that we're not having useful communication about something that I would argue is incredibly important. This is incredibly important.

As Ryan, you write, speculative execution is business as usual. And I have never faulted Intel for ending up in this place. It is the case that this has gone on for decades. And I have said that I object to the idea of class action suits being filed against any of these companies. I don't see fault in the fact that there are these defects which can be leveraged, and I never have. The fault I find is in Intel's communication. And that's the only complaint that I have.

Leo: I wonder if Ryan wrote this tweet before Intel pulled back on all of its fixes because it caused spontaneous rebooting.

Steve: Actually, I think not. And based on his location, I think he is at Intel in their - they have a facility up in the Pacific Northwest, I think, which I think is [crosstalk].

Leo: I don't think it insulted anybody.

Steve: Yeah. And Leo, Friday.

Leo: See, I like this book. You know me and science fiction, televised or filmed.

Steve: I know. And I wanted to give all of our listeners a heads-up, those who have access to Netflix, that it's probably going to be binge time. Starting on this Friday, February 2nd, is the release of the first 10 episodes, that is, the first season of "Altered Carbon." "Altered Carbon" is a term sci-fi readers know well. It's a fabulous title for a book I think written in 2002? It's been a while. It was a cyberpunk novel. And, boy, the preview just looks wonderful. So just a heads-up. Again, "Altered Carbon" is released on Friday. And the good news is I think you and I both have mates, Leo, who are as into this as we are. So I have no doubt that by this time next week Lorie and I, at least, and I would imagine you and Lisa, will have absorbed the first 10 episodes of this very, very interesting-looking new series.

And as I said at the top of the show, probably one of the most fun SpinRite testimonials we've run across in a long time. Of course it starts off with a subject that got my attention, "SpinRite Is Great," and then continues with: "Hi Steve, if that is your real name." Clete Boyce wrote this. He said: "I purchased a copy of SpinRite about a hundred years ago, you know, when dinosaurs ruled the Earth, and I am amazed at how many times SpinRite has saved the day.

"I am," he writes, "a hacker, penetration tester" - so he's probably a listener to the podcast - "penetration tester, software engineer, super genius who enjoys torturing hard drives on the weekends. I really enjoy doing things like playing around with Linux kernel code; and, since I am a super genius, I can feel free to ignore any and all warnings on the various forums. However, every once in a while I will be exploring the frontiers of ignorance and write some code that seems to completely destroy the hard drive itself. I will make one innocent change to the kernel code, reboot the PC, and all of a sudden I hear the PC beeping for mercy, see smoke shooting out the back, and see a tear in the space-time continuum forming in the middle of my living room. I check to see what the problem is; and, sure enough, my PC can no longer read the hard drive.

"That's okay, though. Since I am a Level 14 Hacker Elf, probably, and a super genius, I know that I can easily fix the problem. I reach into my satchel and pull out my Magic SpinRite disk" - oh, and speak of the devil - "pop it into the CD drive, and wait while SpinRite does some stuff that is probably very technical. I walk away, praying to the computer gods that they may forgive me, and most of all hope that SpinRite can fix the problem yet again.

"I've done these terrible things to poor defenseless hard drives many, many, many times; and, every time, SpinRite manages to fix the problem. The best part is I can happily continue to torture poor defenseless hard drives on the weekends without fear of completely destroying them because I know that SpinRite can apparently fix anything. While it might be true that hyperbole is my best friend, the underlying theme of this testimony is true. Steve, thank you for using your powers for good and not evil. And SpinRite works pretty well, too. Clete Boyce."

Leo: Yay.

Steve: Well, Clete, thank you very much for a fun testimonial. And a couple of closing-the-loop bits of feedback from our listeners. Neil Gardner said: "Thank you for Security Now!. Learn a lot each week. How does one stop a Win10 machine from updating to Creator Edition?" And, you know, I meant to get the exact language. Maybe you can, Leo, if you have a Win10 machine running in front of you.

Leo: I do, yes.

Steve: In the Advanced Settings there are two dropdown list boxes containing numbers of days. And one of them you're able to ask Windows 10 to defer updating for fixes for some number of days. And the other one allows you to ask it to defer updating feature improvements for some number of days. And in fact I was just visiting that because I was setting up a new machine because I had to play with this 1703/1709 question, the Creators Update versus the Fall Creators Update, which is the 1709 newer one. And I noted that it was immediately getting ready, it was like, there it was, it was updating to Windows 10 1709.

So I thought, agh, and I quickly went over to Advanced Settings and dialed down the feature update to 365 days. It will let you push it back one year is the maximum on that little dropdown. And then immediately I was very pleased to see it honored that setting and immediately stopped trying to move me to 1709 because I specifically needed that machine to stay at 1703 because that was the one that had this glitch that I talked about at the top of the podcast where there was a bug in that particular version. So I was able to do that by using those two settings. And what exactly is the language?

Leo: I'm not finding the place you're pointing to.

Steve: Ah. So it was under Updates in Win10. And there's like Advanced Settings, which takes you to another level, and there's two different things you can change.

Leo: Yeah. Neither of these seem to have - remember, this may depend on the version of Windows you're using and so forth. And you may have other limits on what you can...

Steve: I realize that I do have one in front of me. Maybe I can bring it up.

Leo: Monthly upload. I don't know [crosstalk]...

Steve: Update and Security.

Leo: Is it in the main control panel?

Steve: So Windows Update. Advanced Options under Windows Update. And delivery optimization, is that where it was?

Leo: Yeah, it's not there.

Steve: No, you're right, I'm not seeing that. I wonder if they took that away.

Leo: Microsoft giveth, and Microsoft taketh away.

Steve: How interesting. Because I have it in 1703. And you're right, I'm not - delivery optimization is not it. That's the thing for getting it from your neighborhood or others. Weird.

Leo: I'm in the Advanced System Properties. Performance, User Profile, Startup and Recovery.

Steve: How funny. I did, I sure saw that and dialed it down and it stopped bothering me. So, gee, Neil, we'll have the detailed answer for you next week. Or I'm sure - get help with your updates? How weird.

Leo: Tell me, Burke, where is it? Back here; right?

BURKE: That one looks different than mine.

Leo: Yeah, see, that's the problem. I think that - oh, now, I already have the Fall Creators Update.

BURKE: Right there on the right, if you go down...

Leo: Advanced Options?

Steve: Hey, you know, Leo, maybe if you're up to date it doesn't give them to you. Because I'm on 1709 on the machine I'm looking.

Leo: Maybe that's it. We're up to date now.

Steve: Yeah. So if there is something to defer, then it lets you defer. If there's nothing to be deferred, then maybe it just doesn't give you the option.

Leo: Yeah.

Steve: So we'll go with that.

Leo: Yeah, because I'm not seeing it. This is one for - we'll ask Paul and Mary Jo. Yeah, see, it's not. Burke keeps saying, no, no, it's there. But it's not.

Steve: No. And I think maybe it's only there for people who have something to be deferred.

Leo: Yeah.

Steve: And in this case, on the machine - I just was checking on the machine I'm using because I'm talking to you through a Win10 machine, and I'm not seeing it. But I certainly was on the 1703 machine.

Leo: Now, somebody on 1709 build 16 says it does have the option. So who even freaking knows?

Steve: Anyway, Neil, it's there somewhere. Sorry we couldn't be more specific.

Leo: You know, I had this problem on the radio show, and I felt like an idiot because I couldn't find the setting. The problem is Microsoft seems to change stuff randomly from update to update. And so it really depends not even just what version of Windows you're running, but really what update you have.

Steve: Or what mood they were in.

Leo: What mood they were in. It's very confusing.

Steve: Anyway, Neil, it's there somewhere maybe. And maybe we'll get - I'm sure, the good news is, this podcast is heard by so many people who know the answer, Leo and I will both be flooded with the answer, and we will have a definitive response.

Leo: Yeah, so this is interesting because Burke's showing me his screen, which does have this, exactly where mine doesn't. So I don't - you got me.

Steve: That is bizarre. That is so disturbing.

Leo: I know. Imagine how dumb I felt during the radio show, thumpering around with this, saying, "Well, it used to be here. Where is it? What is it? Wah wah wah."

Steve: Yeah, well, add me to that club, Leo, because I just stuck my foot in it, too.

Leo: Well, I don't know. Okay.

Steve: We'll have an answer.

Leo: I am up to date. Maybe that has something to do with it. I don't know.

Steve: But Burke must be, too; right? I mean...

Leo: Well, who knows what Burke's doing?

Steve: Okay, don't know if Burke's...

Leo: It may have something to do with the version of the operating system. This is Windows Pro, I'm pretty sure.

Steve: Yeah, and mine was, too. And I'm sure this one is. Oh, wait. This might be Home because this one came with this little machine. It was already preinstalled.

Leo: I'm running, let me see real quickly. Oh, I'm on Home, too. You know what, that's probably what it is.

Steve: Ah.

Leo: It's probably - you would think this Lenovo T470s would be Windows Pro. But maybe I realized I didn't need it. So maybe that's what it is. You might have to have Windows Pro.

Steve: Yeah, and I haven't wanted to mess with this because this is working perfectly for the podcast. And what is it...

Leo: So that's an issue, by the way, because...

Steve: Yup, it's Windows 10 Home, Leo, the one that doesn't have it.

Leo: It's unpredictable what version you'll have. Now, you could go into GP Edit. You can download the - I guess you can. I don't know. You could download General Policy Editor and change this. Microsoft's also said, if you accepted the 7 to 10 upgrade, you can only defer for so long. A year seems long enough.

Steve: Yeah, yeah, yeah. I was happy to see it let me set it to 365. It wasn't clear that the thing scrolled down into the basement because it came up and it said, like, one to seven or something. And I thought, really? But then I, like, set it to seven, then I opened it again, now it went from seven to 14. And I said oh. So I just kept - I went all the way to the bottom, and it was 365. And we know where they got that number. Okay. So that answers the mystery is Home does not let you defer.

Leo: I'm not going to pay the $100 to upgrade to Pro to find out, either, by the way.

Steve: Good luck. And Pro does, yeah. So Neil, that's your answer. If you've got Pro, you can do it. But maybe you don't, and so that would explain why.

Leo: I think Home doesn't - that's probably the biggest difference is you can't defer.

Steve: Yeah. Anyway, I had a comment, but I'm just going to bite my tongue because we know how I feel.

Leo: Yes.

Steve: So a person whose name I didn't capture on Twitter asked: "Will InSpectre" - my little freeware - "work on Macs if run in a Windows VM?" And that's significant because a VM is different than WINE. And I wanted just to highlight that for our listeners. WINE is a sort of a thin Windows emulation layer, so InSpectre will run under WINE and be able to show you the truth about the processor, that is, the firmware.

The problem with a Windows VM, if you mean a full virtual machine, is that it is virtualizing the chip, which means that it's a function of what the VM's chip virtualization is choosing to show its hosted OS. And that's not clear. So InSpectre will work inasmuch as it will run. But you will not be able to, I can't guarantee you, depending upon what the virtual machine is doing, that it will, I mean, it will not, if it's a true virtual machine, it will not be seeing the actual chip. The VM could be showing its client systems, its hosted OS, the same as what is on the chip, or not, depending. So you really wouldn't know for sure. But the good news is WINE is pretty easy to run now on a Mac, so you're able to host InSpectre on WINE and then, yes, you'll be able to see what's really going on.

My comments about battery charging stirred up a lot of debate and question, as they always do. And I'm going to share two tweets and then try to clarify. Richard Bailey said, he wrote: "@SGgrc About battery health, the AccuBattery app recommends only charging your phone to 80% to also preserve its longevity. It gives me a tone when it gets to the percent I set, and I have to disconnect it from the charger." Opher Banarie wrote: "Re babying batteries, what about overcharging? I've been unplugging the device within 10 seconds of 100%. Is this no longer necessary?"

Okay. So to everyone, it is absolutely the case that it's the endpoints, the fully discharged, the fully charged, that are problematical. That's why I referred to being so impressed with my Lenovo laptop that noted after a few weeks that it was always plugged in and said, hey, how about if I run this down to 50% and hold it there? That's absolutely ideal, though it does, as I said, require me to plan, if I'm going to be running on battery and want to for a long time, to run her back up to 100 or near 100 before leaving the house.

So to Richard, who has an app that gives him a chime when it hits 80, yes, that would be better than running all the way up to 100. Also, if you have a battery management system which isn't good about keeping the battery from being overcharged, well, then that's a problem. And so I guess what I'm trying to say is that this is inherently a tradeoff. If you don't go to 100%, that's better for your battery. But obviously then you have less available when you're out running around, and you don't want to go too low because that's bad, too.

So if you're a person for whom it is worth giving a lot of your attention to keeping your battery between, for example, the 80% and the 30% high and low point, then great. That's going to be better for the battery, requiring more of your attention. If you don't want to invest that much, for me, I've sort of reached a compromise. I assume that Apple, the builder of my iOS devices, and I'm sure that, well, I was going to say that Samsung knows how not to overcharge except they're rather famous for having a problem with some of their batteries.

For me it's a compromise. I'm going to leave my devices plugged in when I'm not using them, and I'm not going to discharge them much because of my own life habits. When they're off of the charger, they never have a chance to go down much below 70%, and then they get plugged in again. Consequently, I've never had a battery life noticeably shortened. On the other hand, I'm not using them very much. They're mostly tethered to power.

So I hope that clarifies it. It is really bad to run them to the bottom. They really don't like that. It's better not to run them all the way to the top. If your device allows you to run them to 80% or 90%, that's probably better than running them to 100%. It's dangerous to overcharge them. So if you keep them away from the danger zone, that's better, but at the cost of having them not having as much run around time when they're off of the wall.

So that's, I think, the best way to sum this all up is don't let them run down too low. Try not to cycle them to extremes often. If your device lets you not charge them all the way up, take advantage of that. If you want to take responsibility, great. And I think everyone probably falls somewhere within that spectrum.

And lastly, Peter Kirby noted from our Picture of the Week last week - you remember, Leo, that that was the one we had fun with where sort of the philosophical approach to entering your password was, ooh, ooh, you're close. You're only off by one character. And we made fun of it, saying, yes, it's very clear why that's not the proper wisdom for dealing with a password. Anyway, Peter noted that, he says: "I was showing someone the Pic of the Week from 647, and it occurred to me, if the backend knows you're only one character off, then they aren't hashing the password like they should be, or they wouldn't be able to know that." And actually that's a very good point, Peter.

So I just got a kick out of that observation, yes. Not only are they doing the wrong thing philosophically, but the fact that they're able to do that philosophically means they are also really not doing the right thing technically because they're able to compare the password you gave them versus your in-the-clear password and go, "Oh, cool, he was really close. Let's let him know. Try changing the punctuation a little bit, and maybe you'll get there." So anyway, great feedback from our listeners, thank you. And that's our podcast, 648, for the week.

Leo: Nice. Well done. A job well done. We can put this one in the bank. You can get it now, as soon as we finish editing it and chopping it up, at Steve's site.

Steve: Massaging it a little bit.

Leo: Massage, just minor.

Steve: Oh, and I did want to mention to anyone who looks for these transcripts, Elaine's schedule is a little bit impacted this week and next week. So she begged me, she said, "Steve, Steve, Steve, would it be a problem if I'm a few days late?" And I said our listeners love you. They love having the transcripts. A little bit late is not a problem.

Leo: No, yeah.

Steve: So I'll put up a notice to that effect for people who don't hear this. But this week and next. The good news is she's busy. And she said, you know, it would really help me if you let me put you off a little bit so I can get another project finished. And I said absolutely. She's been so wonderful for 12-plus years, I have no problem with that.

Leo: Oh, absolutely. And I think, yeah, the transcript's really as much for archival purposes and search purposes. Although I know some of you like to read while you listen. But you'll just have to defer a little bit longer. You can get the transcripts and the audio versions at GRC.com. While you're there, check out SpinRite, the world's best hard drive recovery and maintenance utility even today, even for SSDs.

Steve: Even if you're an evil super genius, if you still need it then.

Leo: Even if you're - especially if you're an evil super genius. You'll also find lots of free stuff. Steve's very generous. And including InSpectre to inspect the status of your device. Now, I did want to - I forgot to get this in while you were talking about it. WINE recently updated to WINE 3, and for some reason the latest version of InSpectre and WINE 3 on my Mac do not like each other.

Steve: Ah.

Leo: So WINE hangs. Don't know. Don't know what it means. I'll try it on some other Macs. For what it's worth.

Steve: Interesting. I will end up addressing that because we have been taking pains to get SQRL working under WINE. So it would be available under Linux. And apparently it's now running under Android on WINE, WINE for Android. So that's good. So I'll have to figure out what's going on, and I will address it.

Leo: WINE had a big update with WINE 3 this week.

Steve: Yes, WINE 3, yup.

Leo: I was using it under WINE, an earlier version of WINE, before. Anyway, get InSpectre. If you have a PC especially. I think people on Macs with - if you're running High Sierra you probably just can relax. It's the older operating systems on the Mac that you've got to worry a little bit about because Apple's been slow to get those fixed.

Let's see. What else? We have the show as well on our website, TWiT.tv/sn for Security Now!. Video, as well, if you'd like to see Steve gesticulate. He's a fine gesticulator.

Steve: Yes.

Leo: TWiT.tv/sn. You can also find subscription links there, or just look in your favorite podcast application and subscribe. That way you'll get every episode as soon as it comes out. We only keep, you know, the way a podcast works, it's an RSS feed, and we only keep the 10 most recent episodes in there. If we had all 648 the RSS feed would be hundreds and hundreds of megabytes, which would kill your bandwidth, kill our bandwidth, it'd be terrible. You'd be downloading that five times a day. No, you don't want to do that. So just the last 10 episodes. However, you can go to the website and get all 648 there, TWiT.tv/sn or GRC.com.

We invite you to take the TWiT survey. We do this every year, beginning of the year, just try to get a better handle on who's listening. And there are a lot of new listeners to Security Now!, so it would be very helpful if you go to TWiT.tv/survey. We are not collecting in any way. We're not collecting your email. We're not collecting personal information. This is to be used in aggregate.

Two different groups: One is us because we like to know more about how you listen and what you listen to, and the other is advertisers. Because we don't collect information in any other way about you, this is the one time a year we get to know a little bit more about our audience. And advertisers would like to know that. We don't give them any information about you personally, I promise. And even the in-aggregate is really general broad strokes. It just makes them feel better. TWiT.tv/survey if you would like to help us out.

If you want to visit the studio, you can. No surprises, though. Let us know ahead of time: tickets@twit.tv. Just as you prize your security online, we prize our physical security here in the studio. So email us first: tickets@twit.tv. Thanks for being here. Thank you, Steve. Enjoy "Altered Carbon." We'll compare notes.

Steve: Ooh, yes.

Leo: Next week on Security Now!. Bye-bye.

Steve: Bye-bye.