SECURITY NOW!

Transcript of Episode #560

Z-Wave Goodbye

Description: Leo and I catch up with a busy week of security happenings, including Steve's true feelings about Windows, the Oracle/Google Java API battle, the end of "burner" phones, public audio surveillance, more John McAfee entertainment, a Ring Doorbell glitch, a loony Kickstarter security product campaign, some miscellany, and a look at the closed proprietary Z-Wave IoT home automation system and some hidden problems with one of its door locks.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-560.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-560-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We're going to talk about yet another home automation protocol, Z-Wave. But we're also going to talk about lots of other stuff, including kind of a scammy Kickstarter he wants to warn you about. Lots of news about Windows and why Steve still is in love with that great operating system from Redmond. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 560, recorded Tuesday, May 17th, 2016: Z-Wave Goodbye.

It's time for Security Now!, the show where we protect you and your loved ones online. "We" not really so much. He is Steve Gibson, the security guru at GRC.com. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you. So we jumped on ZigBee and SmartThings.

Leo: Last week was anti-ZigBee week.

Steve: Yeah, with dumb SmartThings and anti-ZigBee. And I thought, you know, it's not fair not to take a look at the competition, which is Z-Wave, which is the other very popular protocol. By some counts, it is actually getting more uptake than ZigBee-based systems. So I found a good piece of research that had been done. And so the title for today's podcast is Z-Wave Goodbye.

Leo: Yes, let's offend equally all sectors of the IoT economy.

Steve: Well, we've got a whole bunch of fun stuff to talk about. And I'm glad that, I mean, I don't have that much to say about it except I want to, after last week's podcast and this week's, that'll give us some foundation to sort of talk about the direction I hope that home automation and the Internet of Things takes because it's sort of in its infancy. And if anything, I would counsel people, where they can, to wait because nothing that we've really seen so far seems to be right. And we really need an open consortium and spec.

And in fact, openness is one of the things we're going to talk about. We're going to talk about the Oracle and Google fight over the copyright ability of the Java API. I got a lot of tweets after last week. I guess I must have come down really hard on Windows because people were, like, saying, "Why do you hate Windows?" And so I wanted to correct the record on that and explain why I love Windows. We've got some pending legislation requiring the registration of burner phones, which is a little creepy. Surveillance microphones found outside of courthouses in San Francisco, hoping to pick up...

Leo: I know. That was amazing.

Steve: Yes. McAfee is providing us another round of entertainment. It's been so long since we've been able to have fun with somebody, like, inventing alien-strength cryptography. And anyway, there is a - oh.

Leo: Thank you.

Steve: I thought I was [indiscernible] speaker somewhere. Anyway, there's just a loony tunes Kickstarter that I keep expecting to disappear because it's just - but the good news is I don't think it's going to fund because enough people look a this and go, eh, this doesn't sound right. So we'll talk about that. A controversial feature being removed from Windows 10. A problem with the 7-Zip application that should cause everyone, if they're using 7-Zip, just to update it. It's not a huge, end-of-the-world thing, despite what The Register said. And then we're going to talk about, take a look at the Z-Wave home automation system. So I think a great podcast for everyone.

Leo: Jam-packed.

Steve: We'll see if we can fit it into two hours.

Leo: As usual, jam-packed goodness coming up.

Steve: It's funny, I learned a lesson when I was, like, maybe six. And understand, I've always been fanatically interested in engineering and technology. And there's a picture that my dad took of me when I was four, wiring up a little light and a dry cell and a knife switch and things. And I'll never forget going over to - my parents were going to another family's home for dinner, and they had kids around my age, and my sister and I went over. And I saw, like, this - I don't think it was a keypad, but it was something to do with, like, there was an alarm system at this home. And I asked the owner of the home, I don't remember his name - actually, I do, Chuck Snook. But I said, "Hey, you have an alarm system," and he said yes. And I said, "Tell me about it." And he said no. And I said, "What?" And he says, "It's not something that one speaks about."

Leo: One does not speak of one's canary.

Steve: You do not talk about one's alarm system. That's supposed to be...

Leo: It's really good, yeah.

Steve: And it just stuck with me, just like, wow. I mean, the essence of that, that there are some things that are not spoken about. And then I realized, yeah, I don't want to know because, if anything ever did happen, I would never want to be on the list of people who knew.

Leo: That's true, too, isn't it, yeah.

Steve: So it's just like - and it just stuck with me. It was like...

Leo: The bank doesn't announce what kind of safe it has. That would be foolish; right? I know that because I talked to Mikko Hypponen, the legendary security researcher for F-Secure. And I said, well, what do you - hey, you're like a security guru. What operating system do you use? He said, "I'm not going to tell you that." He says, "I don't want to give anybody any attack surface at all."

Steve: Right.

Leo: You just don't - I will not tell you. It's security through obscurity, but why give that stuff away?

Steve: Correct. Correct. Okay. So this week's photo on the first page of our show notes is an often-tweeted to me in the past week dialogue which explains what sort of the mysterious refresh two weeks ago of the 3035583 update. 3035583 is, of course, the Get Windows 10. And what Microsoft did was they refreshed it in order to move this from you kind of have a choice to, eh, really not so much. And in fact Paul Thurrott tweeted that this dialogue - he just sort of had his face in his hands. It's like the worst user experience imaginable. For somebody who doesn't want to upgrade, they're just not being given a choice.

And this is, you know, you have the big button that says "OK." So the dialogue says "Windows 10 is a Recommended Update for this PC." And frankly, I think some of the confusion comes from the fact that many users, I mean, for example, I don't mean to pick on Jenny. Actually, she's off on a Mac now, so she's safe. But this would come up, and she would think, okay. And, like, whatever Microsoft wants. And I think the problem is that Windows 10 is such a huge experience change, less from 8.1, but certainly from Windows 7, that people just sort of assume this is like security updates, and they're not going to see any difference. Instead of, like, everything they know going away or being moved somewhere.

So anyway, it was the update two weeks ago to this 3035583 that changed this behavior. And now what we're seeing is - and was it on The Tech Guy on the weekend, or maybe it was - I don't remember now what show it was. But somewhere I know that you had encountered someone that this had happened to.

Leo: Oh, yeah.

Steve: I think it was a photographer.

Leo: This is pretty similar to the old one. The point is that there's no, you know, typically you see an "OK" and "Cancel," or "OK" and "Not Now." But the choices are "OK" or "Upgrade Now," which is identical. That's the same choice. And only if you - but this has been on there for a while. There is a "Click here to change upgrade schedule or cancel scheduled upgrade." You know, that's your only out. But it's not apparent. In the fine print there's an out, but the buttons that normally users choose from, there's no "Cancel." But it's been that way for some time. They must have - this is maybe worse than it used to be, but it's...

Steve: Yeah, well, it's becoming apparently increasingly aggressive.

Leo: Yeah, yeah.

Steve: And so this is a good segue for me to talk a little bit about my relationship with Windows. I think people may have gotten the wrong idea. Sometimes I'm at fault for being a little too glib and sort of assuming...

Leo: Well, you did say Windows 10 was a turd.

Steve: A flying turd.

Leo: Oh, I'm sorry, a flying turd.

Steve: I did. I did early on.

Leo: That was Windows 10, not necessarily Windows in general.

Steve: Well, yeah. And so I want everyone to understand. I don't hate Windows. I love Windows. I have a multi-decade massive investment in Windows. And it is today, remains the majority operating system, with more than half of the market share, even when you include iOS and Android, the large mobile platforms. And if you look at only desktop, it's at 83.6%.

So, I mean, so my whole deal is that I want to be able to write software which helps people, is useful. And I'm able to do that for a greater percentage of all users if I'm writing for Windows. So even today I'm not regretting the investment that I made. I'm not wishing that I knew how to program one of the much lesser desktop operating system platforms. I'm 100% happy with my knowledge and understanding of Windows and my past with it.

My complaint is that my needs are at odds with Microsoft's needs. And it's why I'm on XP still today and didn't move. It would be nice if I didn't have to completely rebuild a system from scratch in order to move. So certainly a compelling idea, a concept in Windows 10 is that it will now just evolve as it is, rather than you needing to just effectively start over. But it is a problem for me that it's Microsoft's closed source commercial profit center. And through the years they have needed to create new ones because we all know upgrade revenue was what fueled Microsoft historically.

And so the tension that exists with me is only that it's changing for Microsoft's purposes, not for mine. And this matters to me because it's not a toy. I don't just bounce around with it and use it for displaying social networking and Instagrams and things. I mean, it is a tool. I need it to work, and I need it to be reliable, and I need it to be stable. And so, for example, when Microsoft says, as they are with Windows 10, "the most secure Windows ever," well, that's complete nonsense.

They also said that about XP. And as we talked about at the time, it's impossible to declare a platform secure at its birth. You may want it to be secure, but it's up to history to prove that. And if XP is any example, it was the biggest security disaster we've ever known. Code Red and Nimda and the MSBlast worm and, I mean, it provided material for this podcast endlessly because it was a disaster. And Windows 10 will get fixed and patched. But as we know, with security, leaving things alone rather than constantly changing them is the way for them to be secure, rather than constantly adding stuff.

And then on top of that, there's my feeling that I've talked about before, that the role of an operating system is to provide a file system for managing files, manage memory, manage applications, create a foundation for applications to run on, and provide I/O and networking services. That's what it's for. But it's the way that Microsoft is evolving it in their desperation to move people to something new. None of those things are of use to me. So as Windows 10 acquires increasing market share, we'll continue covering it. There's nothing there that it offers me. And so I will be, as I've said, moving to Windows 7 at some point.

And again, I think that people want me to love the Windows they've chosen. And I'm not going to. I love Windows itself. But there's nothing that 10 or 8 or 8.1 have for me. And I'm moving to 7 because I do need 64 bits so that I can use a lot more RAM. And as protocols evolve, I do need to be able to be using the latest protocols and crypto suites and have those available. So there are things that push me. But in the case of an operating system platform, I'm definitely not in a hurry to be the first out there with arrows in my back because for me it's a tool. And what I just want is stability.

So anyway, I just - I wanted people to understand that I don't hate Windows 10 at all. You know, the fact that I created Never10 isn't a statement at all about Windows and

Windows 10. It was that Microsoft was pushing people. And we see instance after instance of this push that Microsoft has to move everyone to 10 not being about what's best for the user. It's what's best for Microsoft. And that's a problem. So Never10 just gives people some control over that.

Leo: Yeah. I'm the one who hates Windows. If you want to tweet at me, that's fine. Don't blame Steve for my aversion to it.

Steve: And I think...

Leo: And I don't have the same concerns you do. When I write programs, I write them for myself. I'm not writing for anybody else.

Steve: And I'm glad you mentioned that because I have no problem, Leo, with you feeling however you want to feel.

Leo: Well, I have the same feelings you do. But the point is I have no commercial reason to use Windows other than so I can talk - I have to, and I do use it all the time, and I have Windows machines because I have to for a variety of reasons, mostly involving reporting on Windows. But the way Microsoft - the road Microsoft's gone down, I agree with you, is not a good road for consumers. So for those of us who don't have to use it, why use it?

Steve: And I've heard you taking a broader view, which I completely agree with, which is in general this is happening across the entire industry.

Leo: Yeah, yeah. For a while we were talking about user-centric businesses, and that seems to have gone away. It's like, what's in it for me now for all of these companies.

Steve: Now it's all about us being leveraged in one way or another.

Leo: Yeah, yeah. And they use it against you, frankly.

Steve: Well, and someone tweeted that his Windows 10 was now pushing Office 386, or I'm...

Leo: 365, yeah.

Steve: Office 365. And it's like, oh. I just, you know, I don't want my operating system to be a marketing platform. That just isn't what I want.

Leo: There's ads now. They put ads in the Start Menu.

Steve: Yeah. I know.

Leo: The thing is, at the same time as that's been happening, I feel like desktop Linux has gotten better and better and better. You would be so much happier if you didn't have to use Windows. And we're going to talk about open versus closed. And I've always had a strong predisposition toward open platforms versus closed source platforms.

Steve: Yes, yes.

Leo: And I think that the point you're going to make later applies more broadly than just to security and to - but we'll talk about it.

Steve: Yeah. I completely agree.

Leo: You've kind of come around a little bit because I've always said crypto has got to be open source. I'd like some more open source hardware. That's a tougher challenge, frankly.

Steve: Yeah. And, I mean, for a true codesmith like myself, the idea of the source being available...

Leo: It's awesome, yeah.

Steve: ...is compelling. There have been times when I've been fighting with the Windows API. It just doesn't seem to be doing what I expect it to. And if I could open the source for it and look through it and go, oh, that's why, you know, and like there's a documentation error. So the good news is, for the large part, Microsoft has been very good about it working right, for which I thank my lucky stars. And historically their developer tools have been excellent. I mean, it was a very nice, compelling place that brought developers in because their tools are among the best in the industry. They're getting a little bloated and sluggish now, which is just not what you want in a tool. You don't want to click something and have to wait for the menu to respond because then the system begins getting in your way.

But anyway, so I just sort of wanted to explain that it is a problem that Microsoft's interests and mine don't align. Microsoft has historically been upgrading people for their reasons, not people's reasons, not providing any benefit that I could see in this march of operating systems. And if people want the newest and the latest, I think that's fine. But I'm driving a 2001 model car because it works, and it's got no Internet connection, and no magic keys, and it's unhackable, and it hauls my butt from one place to another just fine. I'm just not a person who thinks that "new" automatically means "better." That just isn't my style. But anyway, I just wanted to correct the record because people seemed really annoyed with me, as if I hated Windows. And I don't.

Leo: I've been getting a lot of tweets too because of Windows Weekly. And I don't remember saying anything particularly negative on Windows Weekly. Maybe just the pro-Windows forces have rallied. And I don't know why you would - I understand if you're a developer. There's lots of reasons to be pro Windows. I'm not saying that. That's still the largest install base of users. But I think it's a good - I think, you know, one of the things I say a lot, and I know you agree with this, is many users are buying more computing power than they need, more complexity than they need.

Steve: Oh, yes, exactly. I mean, the idea of using a Chromebook for what you'd need, I mean - and because the platform is becoming huge and fragile. And as we know, complexity is the enemy of security.

Leo: Yeah.

Steve: And so security is just - it's going to be a constant problem. And being able to just power wash your Chromebook and have it forgive anything that you may have done, that's wonderful.

Leo: Yeah, yeah. And there are plenty of people, I mean, look, I couldn't be using my HTC Vive or my Oculus Rift without a very nice powerful Windows 10 PC, and I was very happy to build one, and it's great. If you're a gamer, you should be running PCs. And the truth is the people who need to run PCs are sophisticated enough that they probably know how to keep them safe. It makes me sad to see people who don't need full-powered operating systems like Mac and Windows running it, especially since they often don't have the skills to maintain them and keep them safe. So it's a bad - but, gosh, most of the people listening to this show could use whatever they want because they know enough to keep themselves safe.

Steve: Well, because these systems have become incredibly complicated.

Leo: They're very complicated, yeah.

Steve: Yeah.

Leo: All right.

Steve: Okay. So...

Leo: Good. It's not your fault, man, it's my fault. Blame me, folks.

Steve: Well, no. And I just, I think, again, I think sometimes I'm a little too glib because

I just assume everyone has sort of been following along for the last 11 years.

Leo: Yeah, yeah. Me, too. I do the same thing, yeah.

Steve: No, I mean, I have...

Leo: People should know us better.

Steve: I have an unopened box of Microsoft Windows 3.1.

Leo: Right.

Steve: And I have, just above where the camera is, a beautiful sandblasted bottle of cabernet that was part of the Windows 3.0 launch that Microsoft gave me. I mean, I'm in all the way with Windows. I just - I don't follow along with, as everyone now knows, certainly, with the latest major change because I look at it, and I think, okay, what does that do that I need? Nothing.

Leo: Right.

Steve: And it seems like a big step backwards. So it's like, you know. So anyway, I've got, you know, I have a Windows 10 machine, an 8.1 machine. Of course the new mega box I built will be running 7. And so I'm here, but I'm just not a fanboy, unfortunately. I love it, and it's the platform that I develop for.

Leo: See, that's - I wouldn't say I love it. To me, I mean, you know, you can love your operating system. It doesn't love you.

Steve: I love XP. I love XP, and I'm liking 7. So this is really - you've been talking about this, and I just wanted to spend a little bit of time on this podcast, for those who aren't following this all very closely, and that is that for years there has been an ongoing battle between Oracle and Google over Oracle's contention that Google is violating Oracle's copyright in essentially using the Java APIs. And the EFF has a nice summary where they wrote:

"At issue in Oracle v. Google is whether Oracle can claim a copyright on Java APIs; and, if so, whether Google infringes these copyrights. When it implemented the Android OS, Google wrote its own version of Java. But in order to allow developers to write their own programs for Android, Google's implementation used the same names, organization, and functionality as the Java APIs. For non-developers out there, APIs (Application Programming Interfaces) are, generally speaking, specifications that allow programs to communicate with each other. So when you read an article online, and click on the icon to share that article via Twitter, for example, you are using a Twitter API that the site's developer got directly from Twitter."

In May of 2012, so exactly four years ago, "Judge William Alsup of the Northern District of California ruled that APIs are not subject to copyright. The court clearly understood that ruling otherwise," writes the EFF, "would have impermissibly and dangerously allowed Oracle to tie up 'a utilitarian'" - and this is the judge - "'a utilitarian and functional set of symbols,' which provides the basis for so much of the innovation and collaboration we all rely on today. Simply, where 'there is only'" - and this is the judge again - "'there is only one way to declare a given method functionality so that everyone using that function must write that specific line of code in the same way,' that coding language cannot be subject to copyright." I thought that was a beautiful piece of legal reasoning, that is, if there's only one way to do this, then it's not subject to copyright. It's a recipe that you are following in order to create the result you want.

"Oracle then appealed Judge Alsup's ruling to the U.S. Court of Appeals for the Federal Circuit. On May 30, 2013" - so that was one year later, one year after the May 2012 ruling that Judge Alsup gave - "EFF filed an amicus brief on behalf of many computer scientists asking the Federal Circuit to uphold that ruling" - that is, Alsup's ruling - "and hold that APIs should not be subject to copyright. On May 9, 2014" - again, one year later - "the Federal Circuit issued a disastrous decision, reversing Judge Alsup and finding that the Java APIs are copyrightable, but leaving open the possibility that Google might have a fair use defense."

Then on October 6, 2014, so about six months after that, "Google filed a petition asking the U.S. Supreme Court to review the Federal Circuit's decision," so basically saying, okay, we're not happy with this appellate court's overturning. Could the Supreme Court please look at it? And again, the next month, on November 7, 2014, "EFF filed an amicus brief on behalf of many computer scientists that asked the Supreme Court to grant Google's petition for review, reverse the Federal Circuit, and reinstate Judge Alsup's opinion. Unfortunately, in June of 2015" - so last summer - "the Supreme Court denied Google's petition." So saying, no, we're not going to take it up. "The case will now return to the district court for a trial on Google's fair use defense."

So that's the background summary from the EFF. Oracle has got some strange thinking. And I want to share it and quote it verbatim because it's interesting. Oracle has expanded the scope of their ongoing copyright battle against Android and accused - and get this wording - "accused Google of 'destroying' the market for Java. Oracle made a request last month to broaden its case against Android."

Leo: That's a little farfetched. I think they might have...

Steve: Oh, wait, it gets...

Leo: ...in fact done more to help Java than anybody.

Steve: Exactly.

Leo: With Minecraft, probably.

Steve: Exactly. "Oracle made a request last month to broaden its case against Android. Now, a supplemental complaint filed Wednesday in San Francisco district court encompasses the six new Android versions that have come out since Oracle originally filed its case back in 2010: Gingerbread, Honeycomb, Ice Cream Sandwich, Jelly Bean, Kit Kat, and Lollipop. Oracle charged: 'As with previous versions of Android, these six Android releases copy thousands of lines of source code from the Java platform, as well as the structure, sequence, and organization of that platform. This copying constitutes copyright infringement.'" Okay, now, that's okay.

Then they said: "Oracle also noted that Android has expanded beyond smartphones over the years" - Android has expanded - " to include wearable devices, TVs, cars, and various household appliances. Advertising on the mobile platform has increased dramatically as well, it said, thereby bolstering Google's core source of revenue and allowing the search giant to 'reap enormous profits from both its direct and indirect exploitation of the infringing code.'"

And finally: "As a result of all this, Oracle's Java business has been seriously harmed, it said." Oracle wrote: "Given the widespread dominance Android has achieved with its continued unauthorized use of the 37 Java API packages over the past few years, Android has now irreversibly destroyed Java's fundamental value proposition as a potential mobile device operating system." What?

Leo: No.

Steve: What?

Leo: No.

Steve: This is exact. This is from the legal complaint. Android and Google have destroyed Java's fundamental value proposition as a potential mobile device operating system. What does that even mean? Anyway...

Leo: Well, it has, if you're going to do copyright, there's four fair-use tests. And one of them is you don't get fair use if it damages the economic viability of the product, if you hurt sales. So when you read these pleadings, it's very clearly aimed at the four tenets of fair use, which is the only defense Google has because this is such a weird, bizarro world to begin with. That they even allowed copyrighting an API in the first place is bogus.

Steve: Yes. Well, and so I liked your analogy when you were - I think you were talking about this on TWiT.

Leo: No, it was The Tech Guy, with the brakes and the cars?

Steve: Yes.

Leo: Yeah.

Steve: It's driving a car. If we didn't have a single uniform car/driver interface, meaning brake and accelerator, and this is how the steering wheel works, it would be a disaster. And as I though about this more, I realized that this notion of standards is what this comes down to. And standards are such a part of our life that it's even - it's almost hard to appreciate the degree to which we depend upon them. I mean, think about even threads, you know, nuts and bolts with standard threading. If everyone just made up their own, so that screws were not interchangeable, it would just be a catastrophe.

And, I mean, so I guess my real complaint is that Oracle has historically benefited from the spread and the use of Java. And so because they allowed that to happen, it's done as well as it has. And suddenly now Google has capitalized on it, and they're wanting to take their marbles back and to say - or basically, essentially, this is a $9.3 billion lawsuit. So they're saying we want some of the revenue which Google is obtaining as a consequence of doing a far better job in commercializing and leveraging Java for profit than we ever could. Because all we're doing is telling everyone to get Java out of their computers.

Leo: Yes. I think you could make the case that Google singlehandedly kept Java alive.

Steve: Right, it's the only reason to use it today.

Leo: Millions of developers have learned Java just so they can write for Android apps. And by the way, if I were Google, I'd just change to Swift and say screw you, Oracle. Just screw you. Just, you know, just change it all.

Steve: Well, it is frightening precedent.

Leo: It's a terrible precedent, absolutely.

Steve: And, for example, Intel never tried to say that our instruction set is copyrighted, and thus their - is it Citrix? There have been several Intel clones, and of course AMD as the largest. And that kind of competitive environment has resulted in everybody getting better products.

Leo: Cyrix.

Steve: Cyrix, right.

Leo: Remember that chip? That wasn't a good chip. But it was compatible.

Steve: Yeah.

Leo: Couldn't have been without this.

Steve: Yeah. And so historically...

Leo: Phoenix BIOS, the Compaq computer, all of that.

Steve: Yes, yes.

Leo: And on and on.

Steve: The BIOS is another perfect example. The fact that IBM gave us an interface called the Basic I/O System allowed all kinds of programs to be written without regard for whether it was, for example, a color graphic display or a monochrome graphic display. They were completely different. They occupied different hardware regions. Yet the BIOS hid those differences so that a program didn't have to worry about what type of hardware you had. And that was an API, a standard. But just in general this kind of standardization, you can sort of imagine sort of a Mad Max post-cataclysm world where you no longer have standards, and everyone's thing is just made from scratch, and they're not - nothing's interoperable. And it would just be a bizarre place.

And I think one of the major things that the Industrial Revolution did was it taught us the power of interoperability. And here Oracle is trying to say, yeah, we're going to get a toll for you using something that we purchased and never figured out how to use. And lord knows, I mean, everyone - I was thinking of all the times in the past we've just been saying to people, if you don't know you need it, meaning Java, uninstall it because it's just bad.

Leo: I'm telling you, Steve, you're going to get to the end of this show, and you're going to say - the moral of this show is going to be open source software, open APIs, and GPL solves all these problems. And it's the only way going forward, frankly, because everybody's trying now to, you know, kill everybody else and make a buck. And it's too bad.

Steve: Well, yes, yes. And clearly, you know, we've talked about how increasingly more and more is sort of becoming generic, how once upon a time you could charge for a mouse that moved a pointer on the screen. I mean, that was like a big deal. You could get money for that. A GUI, oh my goodness. And now it's like, what? It's just sort of become the way things work, and no one is able to leverage that. And once upon a time an operating system was spooky and magical and sort of like, oh, my goodness. Now you just download however many you want in a day.

So this is Microsoft's problem, is that they built themselves around a proprietary, closed source technology which is becoming a commodity. There's a commoditization of operating systems and hardware such that none of this is as special as it once was. Yet they're desperate to somehow hold onto it. So, yeah, you and I are definitely on the same page.

Leo: And we should be clear, so you don't get tweets, you don't hate Java, per se. It's a perfectly good programming language, and the Java Runtime and the JVM is all a very clever way to make software write once, run everywhere. What you hate and I hate and everybody should hate and uninstall immediately is the plugin that makes Java run automatically in browsers.

Steve: Right, because we should have never - it should never have been that an extremely powerful programming environment was exposed to a web server that you visited.

Leo: Right, right.

Steve: I mean...

Leo: That's like ActiveX, same problem.

Steve: All of our listeners know. There's no way that's not going to end badly.

Leo: Yeah, it's just it's a security nightmare.

Steve: Yeah. I have Java on my system. I have several major applications written in Java that require me to have the JVM, the Java Virtual Machine. None of my browsers expose it. And, yes, it's a very useful tool. I completely agree with you.

Leo: Yeah. Minecraft's written in Java. That's why it runs everywhere. But it doesn't mean you have to let the browser do it.

Steve: On Friday the 13th I tweeted something that someone sent me, and I tweeted: "Wow. A new law proposed in the U.S. House of Representatives requiring legal identification for the purchase of 'burner' phones." This is H.R. 4886. If anyone is curious, I created a jump link, j.mp/HR4886. And the legislation reads: "To require purchasers of prepaid mobile devices or SIM cards to provide identification, and for other purposes."

And then it says: "This Act may be cited as the 'Closing the Pre-Paid Mobile Device Security Gap Act of 2016.'" And so it was interesting, a lot of people responded that, oh, yeah, that's the way it's always been in this or that country. So I guess we're, at this point, it sounds like the U.S. has been lax and open and unconcerned, relatively, about the security implications of selling somebody a pre-paid mobile phone. And now suddenly Congress is going to fix that oversight.

So Section 2 of this act - Section 2 is Identification Requirement - reads: "Prior to the completion of any sale of a prepaid mobile device or SIM card to a purchaser, an authorized reseller shall require the purchaser" to provide the following information: their full name, their complete home address, and the date of birth of the purchaser.

And then under Section 3, which is Identification Verification, there's either in-person sales or not. They call it "other sales." For in-person sales, "An authorized reseller making a sale to a purchaser in person shall verify the purchaser information provided under Section 2 by requiring the purchaser to display either of the following." First, a photographic identification card issued by the federal government or a state government, or a document considered acceptable for purposes of identification of the Immigration & Nationality Act, or any two of the following: a W-2 wage and tax statement received from the IRS, a Form 1099 Social Security benefit statement received from the Social Security Administration, a 1099 received from another agency of the federal government, or any document containing personal identifying information that the Attorney General finds by regulation to be acceptable for purposes of this section.

And then, if it's not in person, then for other sales, "An authorized reseller making a sale to a purchaser not in person shall verify the purchaser information provided under Section 2 by requiring the purchaser to submit the following information: Valid credit or debit card account information, their Social Security number, their driver's license number, and any other personal identifying information that the Attorney General finds by regulation to be necessary for purposes of this section." So again, it's not law, but it gives us some indication for where the wind is blowing.

Leo: Fortunately, there's a gun show exception. So you'll be able to buy your burner phone at a gun show. And that's the good news.

Steve: Is that true?

Leo: No. But there ought to be. Get your gun and your burner phone.

Steve: Because I was wondering, you know, I'm not a gun owner, and I watch all of this go by, all of the gun rights legislation stuff. But I was wondering how this compares to buying a gun. Is it now more difficult to buy a cell phone than it is to purchase a firearm? I'm not, you know, I don't know.

Leo: Yeah, you can go to a gun show, much easier.

Steve: Wow. CBS in San Francisco uncovered the fact that hidden microphones were placed in bus stops and pedestrian walkway lighting by agents of the FBI to secretly surveil the environ around the courthouse for any, I guess you'd call it "ex parte" conversation that a client might be having with their defense attorney.

Leo: That's terrible. That's terrible. Although, I mean, look, you're in public.

Steve: Yes.

Leo: I don't think it's against the law. I don't think a judge would allow you to use any ex parte conversations with your attorney.

Steve: Correct. So it is not against the law. An attorney was contacted by the reporter doing the story and said, and I quoted these in the show notes: "Speaking in a public place does not mean that the individual has no reasonable expectation of privacy." And "A private communication in a public place qualifies as a protected 'oral communication' under Title III, and therefore may not be intercepted without judicial authorization."

Leo: Right.

Steve: And so, yes, I think - and so what may be happening is the FBI is hoping to gather some information that would give them some clues into other people that they should get formal surveillance warrants for and so forth. But still, just a little bit creepy that in a place where you would not expect to be surveilled, that's going on. On the other hand, there's video cameras pointing in every direction these days.

Leo: Well, I guess that's the point is we're being surveilled all the time, and it isn't illegal to do so.

Steve: Yeah.

Leo: It reminds me of the Philly police who had the car with the Google Maps logo on it because they wanted to hide the fact that they had all this machinery to scan license plates.

Steve: Right.

Leo: And it feels wrong to me because it's like a fishing expedition. They're just looking for stuff. But it's not because you're in public.

Steve: Yeah.

Leo: You know? I mean, Google might have a problem with it.

Steve: I forgot to mention that Denise Howell, who was on - was she on TWiT?

Leo: Yes, she was on TWiT. She was great.

Steve: She was great and had some really good additional input on the Google/Oracle fight, explaining that, as I remember what she said, explaining that some of what the Supreme Court said was that enough of this had not been resolved in the earlier arguments. And so it's not that the Supreme Court was never going to hear this, and that they might not reconsider taking it up, but that it was sort of done prematurely. It was pushed to them before - and I don't remember any of the legal jargon that Denise used. But she understood that we have a ways to go, and that all is not lost yet.

And I am glad that Oracle has decided to fight Google and not some much smaller fry that wouldn't be able to defend themselves because certainly Google can. Although, boy, some of what the attorneys were apparently saying didn't sound very compelling. Like the judge was more confused after the attorneys got through explaining it to him.

Leo: This is the judge, by the way, we mentioned when this happened, who taught himself Java so he could - because I guess he went to - his undergraduate degree is in math.

Steve: You're right, we did talk about it four years ago.

Leo: Yeah. He taught himself Java.

Steve: And were very impressed that he learned what this meant.

Leo: And his ruling originally was you couldn't copyright an API.

Steve: Correct. He came to the right decision.

Leo: Yeah. But then it was overturned.

Steve: Yeah.

Leo: So it's just, yeah, oy. It just shows, you know, really the truth, what I take away from this, is if you can afford lawyers for years upon years, you can do anything. You need to have enough of a bankroll to just pay the lawyers.

Steve: Right.

Leo: And they can just tie things up forever.

Steve: And it's not like it's inexpensive. It's like, you know, all of your money goes down the drain. I remember someone talking about patents and was asking me why I didn't patent things. And I said, well, you know, I guess there's a little bit of ego benefit. It's like, oh, I have 14 patents. I said, but on the other hand, you have to enforce them. And enforcing a patent is incredibly expensive. And as I said, I used to be an expert witness. I used to agree to be an expert witness. And I watched several technology decisions come down absolutely on the wrong side. And I just thought, oh, boy, you know, this is - I don't want to be associated with this. It's just too frustrating.

Leo: Yeah.

Steve: Speaking of not being associated, John McAfee. So McAfee is back in the news.

Leo: What's he up to this time? The last we heard of him - by the way, John McAfee, inventor of the McAfee Antivirus. Which he sold, we should say, to - who did he sell - not Symantec, Intel. Intel owns it.

Steve: Yeah.

Leo: And so it's not...

Steve: You've got to wonder whether they're sort of wishing they'd changed their name.

Leo: Oh, they should change their name, yeah.

Steve: Really, because McAfee Antivirus is just like, wait a minute, is that the John McAfee Antivirus? Well...

Leo: And then he went - he took the money and went to Belize. Kind of had a crazy lifestyle. There was a murder charge.

Steve: Someone killed his dog.

Leo: It was a thing. He escaped. And then the last we heard of him he said, "Oh, I can crack the Apple iPhone. If I can't, I'll eat my shoes." And then he said, "Well, I was lying. I couldn't really. But I'm not going to eat my shoes."

Steve: Right. So now he decides - well, okay. So the press covers this with "WhatsApp Message Hacked by John McAfee and Crew." MSN reports: "John McAfee claims to have cracked secure WhatsApp messages."

Leo: My god. Why do they still fall for this stuff?

Steve: Engadget: "John McAfee claims he can read encrypted messages on Android." And Gizmodo: "John McAfee Apparently Tried to Trick Reporters into Thinking He Hacked WhatsApp."

So here's what actually happened: "It appears that McAfee has tried to trick reporters again, by sending them phones precooked with malware containing a keylogger..."

Leo: Oh, lord.

Steve: "...and convincing them he somehow cracked the encryption on WhatsApp. According to cybersecurity expert Dan Guido, who was contacted by a reporter trying to verify McAfee's claims, McAfee planned to send this reporter two Samsung phones in sealed boxes. Then, experts working for McAfee would take the phones out of the boxes in front of the reporters, and McAfee would read the messages being sent over WhatsApp over a Skype call. McAfee offered this story to at least the International Business Times and Russia Today, and one additional source said he also shopped the story to Business Insider."

So this security researcher, Dan Guido, said: "John McAfee was offering a couple of news organizations to mail them some phones, have people show up, and then demonstrate with those two phones that McAfee, located in the remote mountains of Colorado, would be able to read the message as it was sent between the phones." Dan wrote: "I advised the reporter to go out and buy their own phones because, even though they come in a sealed box, it's very easy to get some Saran wrap and a hair dryer to rebox them."

Leo: What kind of idiot would just take the phone and go, okay, and not say, well, okay, John, I have my own phone. Why don't we try it on this one?

Steve: And of course this bubbled up to Moxie...

Leo: Oh, boy.

Steve: ...because WhatsApp uses Signal. And we talked about Signal a few weeks back, and for me it was a love affair because I was so impressed with, I mean, the protocol and the technology and the cleverness of the solutions they had come up with. So "Moxie Marlinspike, who of course developed the encryption protocol used in WhatsApp and assisted in implementing it, told Gizmodo that McAfee also admitted his plan to him." Moxie said: "Some reporters that had been contacted by McAfee about a demo got in touch with me" - contacted by John McAfee, not McAfee AV - "by John McAfee about a demo got in touch with me. I talked," says Moxie, to McAfee on the phone. He reluctantly told me that it was a malware thing with precooked phones, and all the outlets he'd contacted decided not to cover it after he gave them details about how it would work."

So remember in the case of the San Bernardino phone, he later said, yeah, I don't really have any way to do that. And actually the phase he used was "I just thought it would generate" - and I'm sorry to say this word, but he used the term - "a shitload of press."

Leo: Yeah, yeah.

Steve: And so he was doing it purely...

Leo: What's bizarre is he's not - he isn't selling anything.

Steve: No. No.

Leo: What does he want the press for?

Steve: It's ego.

Leo: Ego.

Steve: It's just he needs, you know, I mean, Washington has Donald Trump, and our industry has John McAfee.

Leo: Yeah.

Steve: And both are providing a lot of interesting times and entertainment for the press. So, wow.

There was a problem that was misreported by a lot of the media, the tech media, because there were some reports of users of one of our favorite products, the Ring Doorbell, seeing other people's video. And I was very impressed with The Verge and their reporting. And so I'll just share it because they did a beautiful job of explaining it. And Ring's response was nice, too.

So The Verge wrote: "Sometimes the wheels can just come off this whole Internet of Things thing. When cameras are talking to the cloud, there's room for them to make mistakes, and these devices are filming pieces of your private life so that can be a little worrisome. Unfortunately, some owners of the Ring Doorbell Pro recently experienced just this sort of mix-up when the 'smart' system showed them video of visitors outside only it wasn't their own home that the feed was coming from. They were getting video from other Ring users.

"Now, this isn't the worst thing," writes The Verge, "to have happen, securitywise. It's pretty hard to tell someone's address from a doorbell camera, so once you come to the realization that you're not seeing your house, all you're left with is a video of a total stranger. And for what it's worth, Ring claims that there were only 10 instances of this problem out of over millions of calls that its doorbells make each day. Still, it's the sort of problem that absolutely can't happen if we're going to invite smart home gadgets into our everyday lives 24/7. To that end, the company says it's taken steps so that this weird and," they wrote, "semicreepy bug won't repeat itself in the future."

And then Ring explained it. They said: "We use random numbers to" - and I should mention, some outlets said that they were - they got the story wrong, and they said that the random numbers lacked enough entropy so that there weren't collisions. That wasn't it at all. Ring said: "We use random numbers to generate a call ID from Ring products. We did a very robust beta test of the new Ring Video Doorbell Pro on experimental software; and, when we moved it out of beta for the commercial launch, some customers' numbers were in two different databases." That is, they were still in the beta database, but then they were also in the commercial launch database.

So Ring says: "As a result, those call ID numbers were overwritten. We believe, based on all the data we've analyzed, that this caused less than 10 instances out of more than four million calls per day and over 84 million calls total where video recordings overlapped for

Ring Video Doorbell Pro users only. We're in the process of merging those databases so this will no longer occur. This issue only affected Ring Video Doorbell Pro users, not users of our other products, Ring Video Doorbell and Ring Stick Up Cam."

So again, I'm impressed. We talked about a problem that was found by some researchers on the Ring doorbell months ago. And then, in following that up, we learned that the doorbell immediately updates itself the first time it comes online, so no one would ever have been in any risk, even if they had one that they bought off the shelf that still had that firmware. The doorbell updates itself autonomously. And in fact that led me to say that, you know, this has to be standard operating procedure for Internet of Things devices. If they're going to be little operating systems running firmware, everything we know says that they're going to have security problems.

So much like routers that are connected to the Internet, the idea that Internet routers have old firmware is crazy because their nature is to be on the Internet. They ought to be periodically reaching out and repairing themselves. And so anyway, that's what that was about. It was well contained. Ring understood the problem and took care of it quickly.

Leo: And we should mention Ring is a sponsor of this show, in fact of this episode of this show.

Steve: Right.

Leo: And I did it on the air, and I hope people heard it. For the people hearing it ahead of time I said, "Please, Steve, don't let that in any way affect your coverage of this story." I didn't know ahead of time what his coverage was. But there you go. They are a sponsor.

Steve: Yeah. And I actually own one. I haven't yet installed it.

Leo: Oh, you do? Oh, good.

Steve: Yeah, yeah.

Leo: I hope you enjoy it.

Steve: I completely think it's the right thing.

Leo: Yeah.

Steve: Okay. Now, this is just too wonderful. The Kickstarter campaign is called DataGateKeeper.

Leo: Oh, boy.

Steve: Yeah. So the subhead is "DataGateKeeper: The First Encryption Software Engineered to Defeat Hacking." So no other encryption software that we're aware of, and apparently that they're aware of, has been engineered to defeat hacking. Theirs is...

Leo: It's the first one.

Steve: Theirs is the first.

Leo: Nobody's ever done this before.

Steve: We can start feeling good right away.

Leo: Damn, already.

Steve: They say: "Every day you use flawed data protection, not by choice. Due to these flaws, cybercriminals and hackers steal and profit from your stored and transmitted personal and business data every day." Then they explain that "Designed before the turn of the century, AES, the Advanced Encryption Standard, is older than most of the cars on the road today."

Leo: Wow.

Steve: Like the wheels are falling off, Leo. "However, it forms the basis" - this older than the turn of the century - "forms the basis of our global data security protection. And," they say, "It's failing.

"AES hacking solutions are readily available for sale on the dark web."

Leo: What?

Steve: "In the late 1990s" - who even remembers back then - "AES, while under well-intentioned government oversight, somehow a backdoor found its way into this 'approved' data security solution, and has been widely reported." What? What? Not here. But apparently everywhere else. Widely. "The unintended consequences of this backdoor in AES allows for complete access to your data..."

Leo: Oh, my god.

Steve: "...without your permission, to data monitoring, data mining and active eavesdropping, effectively voiding your right to privacy and confidently." Okay, they meant confidentiality, but that word had too many syllables. "So common is this practice, it has a name." They named it, Leo, "active snooping." Now they go on to explain: "SSL is a myth."

Leo: Oh, no.

Steve: Doesn't exist, Leo. SSL, we wish we had it. But, you know, it's just a myth. "Cybercriminals know about these flaws and backdoor." Because of course they hang out on the dark web, where this is all available. "They are stealing, compromising, and profiting from your data every day." Okay. This is just too fun.

"The commitment to build an impenetrable data encryption solution, free of outside influence" - because that would be bad, of course - "began nearly three years ago," well after the 1990s that no one can remember. "At the same time we were developing the DataGateKeeper, codenamed Deterrence, unfortunately over 150 million personal and confidential files were compromised, stolen, or hacked in the U.S. alone." So, you know, while they were developing this amazing new technology, Leo, it was happening. So clearly there's a big need for this. "And those were just the ones," they write, "that were reported." And then, "See the timeline." They have a very nice timeline where they show all of this happening.

They write: "We knew we needed to be successful. To accomplish our goal of building an impenetrable data security solution, we first had to be able to beat hackers at their own game, using their own tools. To do this, we reverse-engineered several commercially available automated password cracking programs, and two which are not, to understand these programs' methodologies." Ooh, they used a long word. "Following the decompile and disassembly procedure, we designed and built our own cracking program, and then we set about defeating our own new super hybrid. Goal met.

"The DataGateKeeper Total Data Protection Software" - oh, and I should mention there's just little TMs all over this stuff - "is the first data protection software specifically designed and engineered to defeat automated hacking and code cracking programs. Exclusively, the DataGateKeeper contains no backdoor." Unlike AES, which they have already explained has a backdoor that you can find on the dark web, "DataGateKeeper contains no backdoor, exclusively. And it disallows automated repetitions" - oh, why didn't we think of that? - "the core method used in brute-force attacks." They just disallow that, so we can't have any brute-force attacks. "We built an exploit that destroys their exploit." And this goes on. I won't belabor...

Leo: My favorite line is "You don't have to be 007 to use the DataGateKeeper encryption software."

Steve: No. One-click protection. One click.

Leo: And then they throw in stuff like "our pledge to those who serve to protect us, active duty and first responders" is completely gratuitous. It's very weird.

Steve: Oh, it is.

Leo: So it's not - and by the way, not cheap. It's 99 bucks for a 64GB flash drive with the DataGateKeeper software preinstalled.

Steve: Oh, and they have a very nice full-chested woman animated there who shows the cap being removed from the USB thumb drive, just in case you weren't sure how to take the cap off of it.

Leo: It both encrypts and decrypts.

Steve: Which is handy, you know. Oh.

Leo: I don't know how this stuff gets by the Kickstarter people.

Steve: That's why I kept worrying they were going to take it down. Oh, there she is. Look at that. See how that cap comes off?

Leo: Comes off? But, you know, it looks like it screws on and off. Ooh.

Steve: Oh, well, you know, it is good to a hundred meters under water. So you'd want to have it, you know, maybe it screws into a nice rubber O-ring so that it protects it from...

Leo: You know, they need to change her T-shirt, though. It says "MyDataAngelFloom."

Steve: Oh, no, we've got Data Angels, too.

Leo: Oh, okay.

Steve: I didn't get to the Data Angel part.

Leo: Oh, there's more. Oh.

Steve: Oh, yeah. Well, I'll just say that it's not exactly clear from their chart. That chart, if you go down a little further...

Leo: He's [crosstalk] Mr. Wizard. That must be for you.

Steve: Yeah, see, now they're going to get technical because you have 512kb, and I'm not sure what that is. But apparently it's six million times stronger. The "exploit the exploit," they said: "Following months of research, decompiling, and disassembly, we had a baseline for Deterrence" - remember that's the code name - "and developed our cipher utilizing cryptanalysis." So they're just not screwing around here, Leo. They're using cryptanalysis to develop their own cipher.

Leo: Oh, here's the math.

Steve: Oh, yeah. Yes. Watch out.

Leo: That's an animated GIF with the math.

Steve: Oh, goodness.

Leo: Formula C(n,r) = n!/r!(n-r)!). There you go.

Steve: I know.

Leo: There you go.

Steve: And they say: "We created a cipher that is six million times stronger than current data security."

Leo: Sorry, that was factorial, not not.

Steve: Right.

Leo: N factorial.

Steve: As proven by algorithmic mathematics, Leo.

Leo: Ooh.

Steve: They employed algorithmic mathematics in order to determine that their cipher, which they developed with cryptanalysis, is six million times stronger than that crap from 1990 that we're all using by mistake. So, yeah. And somehow, with the 512kb level, you get 50 years of protection, and that's for civilians. With the 768kb, you get 75 years of protection, which is for use by first responders, police, retired and active duty military. But if you really want to go big, that's the 1024kb encryption, which gives you 100 years of protection, and that's for enterprise. So, boy.

Leo: Wow. Oh, here comes Vinny in his car. Oh, Finito Brothers.

MALE VOICE: Jack needs a job done, Mona. We hear you're the best hacker on the East Coast.

FEMALE VOICE: AES, DES, Twofish, Blowfish. Not a challenge.

Leo: What's Bluefish? Twofish Bluefish? Made it sound like a Dr. Seuss story. Obviously she means Blowfish; but, you know, okay, fine. Okay. Wow. Okay. But they have raised a little bit of money, I've got to point out.

Steve: Well, you know, it's the Internet, Leo. And what was it that Barnum said, famously?

Leo: Yeah.

Steve: Yeah, unfortunately.

Leo: There's a sucker born every minute.

Steve: Oh, goodness.

Leo: So nobody who listens to this show will be fooled by that.

Steve: No. And many people were giving them a dollar, just to be able to post...

Leo: To laugh.

Steve: Like, what a crock this is. And then for a while they were rebutting them. And then finally they shut down the $1 donation because people were just using it, they were willing to pay a dollar just for the opportunity to say, oh, come on. Yeah, so we haven't had any fun like that in weeks.

Leo: That was a fun one.

Steve: The problem is we did this 10 years ago, back when people were still creating their - but, you know, that was after 1990s, Leo. It's like, people were still - they hadn't given up on creating their own cipher that they were absolutely sure was unbreakable.

Leo: You know what's really old? Math. Man, that's, like, thousands of years old. It's time we had something new.

Steve: Yeah, new math. They tried to teach that to me in high school.

Leo: Oh, yeah, we had to study that.

Steve: So a couple little last points here. We did note that in the Windows 10 Insider Preview Build which was announced, 14342, way down at the bottom of Microsoft's blog at Windows.com, they noted: "We've removed the WiFi Sense feature that allows you to share WiFi networks with your contacts and to be automatically connected to networks shared by your contacts. The cost of updating the code to keep this feature working, combined with low usage and low demand, made this not worth further investment. WiFi Sense, if enabled, will continue to get you connected to open WiFi hotspots that it knows about through crowdsourcing." So I don't know how to read that, really.

Leo: They're just turning off that thing, you know, that...

Steve: Yeah, and then...

Leo: It never really was as bad as everybody was talking about.

Steve: No, because you really did have to go through, jump through some hoops to turn it on.

Leo: That's why nobody uses it, probably.

Steve: Yeah. Yeah. But, I mean, I guess I don't really understand. This seems a little strange that they're taking things away because there are people who are not happy that they're taking it away.

Leo: Well, it happens all the time where a company doesn't want to support a feature that nobody used. And they know who uses it because they've got all that telemetry.

Steve: I was going to say, I think that's probably the way Windows 10 will roll moving forward is that they'll add things and remove things and just sort of, you know, things that work and people like stay, and things that don't, they go away.

Leo: Right, right.

Steve: People using 7-Zip, TheRegister.co.uk reported this as, you know, basically the end of the world as we know it. In fact, it's far less concern than that. The Talos security division of Cisco did find a couple heap overflow problems with the version of 7-Zip that was current at the time. So the idea would be, if someone created a malicious zip file, and they were targeting you, and they knew you were going to use 7-Zip, then maybe there was a way for them to execute code in your computer with the privileges of your logged-on session. And so that's the sum and total of it. So if you're a 7-Zip user, there's a new version. Go get it, and you should be fine.

Mary Jo Foley tweeted this morning, Paul retweeted and I retweeted, something that will be of serious interest for a subset of our listeners. Many people in the last few weeks have been, for whatever reason, installing Windows 7 fresh and having huge problems with Windows Update. And it has seemed to be going very slowly. What Mary Jo just tweeted was that Microsoft - her tweet reads: "Microsoft comes through with its promised 'convenience rollup,'" as they call it, "of updates and fixes for Windows 7." So it's not technically Service Pack 2, but you could think of it as Service Pack 2. So, and I got all three of them because I will be probably setting up versions of Windows 7 in the future.

The thing to remember is KB3125574. KB3125574. So what that takes you to is - oh, it's interesting, too, because you need a version of IE to run their whatever it is thing that they use. I had Windows 7 rolling. I fired up my Windows 7 box that I run Skype on, specifically to be able to do it, because I tried to get it on my XP system, and it just laughed at me. But there's three versions of this, and they're, like, 374MB to 474MB. And they are - it's a massive update rollup. So you would install Windows 7 with SP1, that is, the version that includes SP1. Then you would download or probably, either on that system download or have previously downloaded, this three to 400MB rollup. And it's a single executable that just brings you current. And so, yay, you know, thank you, Microsoft, for providing that.

Leo: I was talking to somebody, said it took him a week to apply all the updates with all the reboots and everything. So a rollup is really much appreciated.

Steve: Yes. And something seems to have gone wrong. Actually, maybe it's over because, when I turned my system on this morning, I had a couple little things it wanted to update, but it knew about them quickly. And last week it took, like, hours for that to happen.

Leo: You have to think that this could also be part of Microsoft's attempt to move you to Windows 10. Let's just make the experience, I mean, they've already taken stuff out of 7, and they don't seem to be patching it as quickly. And I just - I wonder if they're just - this is part of the whole thing to get you to go to 10.

Steve: And we did hear even that some of their telemetry stuff was being pushed back into Windows 7.

Leo: Right, it's in 7, yeah.

Steve: Which is a little annoying. Well, I have a nice report from somebody who is not annoyed, and that's Brad in New South Wales, Australia. His subject line caught my eye because it's "SpinRite success on iMac SSD." This was dated May 14th, so just a couple days ago. He said: "Hi, Steve and Leo. I've been listening to your show for about three years and really enjoy it. I need to give a bit of background to this story as there is a lot involved." And he actually gave me permission to cut it down, which I did a little bit.

He said: "I have a 2009 iMac that hasn't missed a beat since I purchased it. A year ago, it started to slow down somewhat. Not wanting to fork out a few grand just yet for a new machine, I managed to pull the machine apart and upgrade the optical drive and 3.5-inch mechanical drive to two new hard drives." Actually he says HDDs. He says: "One a higher capacity spinning drive, the other an SSD." And he made the SD his boot device.

He says: "The SSD was installed by a built-for-purpose blanking plate in the shape of the optical drive and was installed in the optical drive's original location." So basically he took out the optical drive and put the SSD in in its place. "Once the SSD was in place, the machine ran like new.

"Recently, the SSD was showing signs of failure and was no longer booting properly." So it was beginning to die. "Not wanting to pull the iMac apart again, I researched a solution. I came across a video I think you mentioned in a previous episode where it was possible to run SpinRite from within Mac OS X. I installed OS X onto an external hard drive and booted to it. I then downloaded VirtualBox and ran up a DOS virtual machine. I attached the dying SSD managed to the DOS virtual machine, then booted SpinRite with its ISO file. I ran Level 2 on the iMac's SSD, and after rebooting she now runs just like new again. Thanks for a great podcast. Cheers, Brad."

Leo: Woohoo.

Steve: So he came up with a nice solution. In the future, with SpinRite 6.1, I will be making that all a lot easier. But basically he had an SSD that he had installed into his iMac. It was dying. He arranged to run SpinRite on it, and it brought his SSD back to full speed. So yet another instance of SpinRite doing its same goodness on a solid state drive as on one that spins. Thus lots of future for SpinRite.

Leo: Yay. We continue on with Security Now!, Steve Gibson.

Steve: So in our talking about Dumb SmartThings last week, and the ZigBee wireless protocol, the alternative, which is by some measures even more popular than ZigBee, is Z-Wave. And I thought, you know, having been rough on ZigBee, I ought to take a look at Z-Wave and just see how it measures up. And what I found was that it is sort of a mixed blessing.

My biggest complaint with it is that it is utterly single-source closed and proprietary. And I just don't think that is fitting for something that is going to be IoT. I mean, if the Internet were that, we wouldn't have the Internet today. And I think the things we connect to the Internet need interoperability, but also we need to be able to have people looking at them who want to. So there is a very nice analysis of its security which was really difficult to do. I mean, it was impeded deliberately by Sigma Designs that is the owner of Z-Wave, not wanting anyone to take a look at this, which is just, you know, that raises all kinds of, as our listeners know, security red flags.

In the abstract of their paper, they wrote: "The ZWave wireless communication protocol has been widely used in home automation and wireless sensors networks. ZWave is based on a proprietary design and a sole chip vendor. There have been a number of academic and practical security researches on home automation systems based on ZigBee and X10 protocols; however, no public vulnerability research on ZWave could be found prior to this work.

"In this paper, we analyze the ZWave protocol stack layers and design a radio packet capture device and related software, which we named ZForce, to intercept ZWave communications. This device enables us to decode different layers of the ZWave protocol and study the implementation of encryption and data origin authentication in the application layer. We then present the details of a vulnerability discovered using ZForce tool in AES-encrypted" - it's too bad they don't have the Data Angel encryption because that would be six million times more difficult. Anyway, "...AES-encrypted ZWave door locks that can be remotely exploited to unlock doors without the knowledge of the encryption keys."

So basically the system is completely closed. The Z-Wave protocol is proprietary, developed by Sigma Designs. They are the sole source of the chips that are in any Z-Wave-enabled devices. The SDK is only available to OEM manufacturers after signing a non-disclosure agreement where the manufacturer promises never to make this available publicly. So, I mean, this is as bad as it gets. This is completely closed. Researchers are forced to use, as these guys did, they used a Texas Instruments SDR, a Software-Defined Radio kit operating at the frequency of Z-Wave to do raw packet capture and pull the stuff out of the air.

They also found, and they didn't indicate which one, but they found a Z-Wave device whose firmware they were able to read out. And so they reverse-engineered the firmware in order to obtain some details of the crypto algorithm that was not otherwise obvious from just looking at the data, so to speak, on the wire, in this case over the air. And in doing that, they realized that a mistake had been made. And they then developed the technology to unlock a door lock that they had examined without having any knowledge or access to the system.

It turns out that the main controllers have a factory-burned 32-bit essentially Home ID. And so since only a single manufacturer makes these chips, that gives them 4.3 billion homes that would each have a unique Home ID. And then nodes on the network, there's an eight-bit byte for node ID. So you can have up to 200, and it wasn't quite 56, like 252, I think, because there were some reserved values. But, you know, so plenty of nodes. It forms a mesh network where nodes are able to be repeaters.

And in digging through this and reading all of the paper, on one hand I was impressed by the technology, and depressed by the fact that it was completely proprietary and locked up. And it would have been deliberately made as difficult as possible for any security analysis to be made of the system. And so it required them overcoming all these hurdles. And so the point is it doesn't matter if NDAs are in place. It doesn't matter if you try to hide this and protect it. All of our experience says that's a fool's errand. You can't do it.

And in fact these researchers demonstrated that they're able to reverse-engineer an endpoint, figure out everything that they need to know. And when they did, they found a flaw. So of course this raises the specter of who else knows about these flaws that are able then to, simply by sniffing the traffic - what they did was they sniffed the traffic, which is very active in the Z-Wave network. That allowed them to determine the 32-bit Home ID and the eight-bit node ID of the door lock. And then using a protocol mistake which they found, they unlocked the door, all from outside the house and wirelessly.

So overall my take is, as I said at the beginning of the show, what we need is, and I didn't have a chance to look at this big consortium of, as I described it last week, essentially everybody else. I mean, it's like it was the Who's Who of everybody except Samsung and Sigma. It has a different protocol that they're working on. That's what we need. It needs to be open. It needs to be multisourced. And ultimately, that's going to end up being the solution that I hope to see win.

So for what it's worth, this echoes what we said last week, which is that the systems today need to be regarded as sort of first-round IoT deployments. For early adopters, that's fine. I would say in the long term, since the eventual winning open system will require replacement of all of the existing investment, you may want to minimize your investment. That is, rather than going out and just completely setting up your whole system this way, ultimately I expect the winner is going to be the open, well-analyzed, truly secure, you know, there's just no way that that kind of group, with all the understanding we have of how to do this right, there's no way we're going to get a system that isn't designed with the kind of security we want.

It may not be that light bulbs, you know, light bulbs you may be able to screw in, and they'll discover themselves and then be on the network. But there will be, for example, high security links where you have to go through, you have to jump through some more hoops in order to authenticate the device to its home base. But that makes sense if it's your front door lock or your burglar alarm system. And also we have to look at the whole question, as we talked about last week, Leo, of using radio. I mean, there are technologies, there's frequency-hopping and there's spread spectrum, neither of which these current systems use, which are far more jam-proof than fixed-carrier frequency solutions, which are trivially jammed.

So anyway, I think, I have no doubt that in the fullness of time the podcast is going to keep going. And I imagine that at some point this large consortium of people working on the ultimate open standard for home automation, they'll have something. And then I'll be able to really dig in and tell everybody how it works.

Leo: And of course anything they do has to be patchable, has to be remote-patchable over-the-air updates, you know, so that when we do discover the flaws - because nothing, just because it's a consortium, and it's open, doesn't mean it won't be flawed.

Steve: Correct.

Leo: But when we do discover flaws, there have to be procedures.

Steve: Oh, yeah. Look at OpenSSL and Linux.

Leo: Yeah, right.

Steve: I mean, we're finding problems in all of these things all the time because they're just so complicated. So, yes, everything's going to have problems. We just need a means of fixing them.

Leo: And, you know, tomorrow I expect Google to announce some home automation stuff.

Steve: Yeah.

Leo: They're one of the companies that's...

Steve: Is it Cricket? No.

Leo: Well, Chirp is a thing that they're going to do - it's an Amazon Echo device. That's the rumor. But of course they have Weave and Thread. They have home automation protocols which are primarily open.

Steve: And that Hub thing that...

Leo: The OnHub supports those, although it does nothing yet with them.

Steve: Fancy antennas, but, you know...

Leo: Yeah, fancy antennas in there. And by the way, I think it has the 802 dot, oh, I can't remember, is it 15? There's a spec...

Steve: 15.

Leo: Yeah. And is that Z-Wave, or is that ZigBee, or...

Steve: ZigBee.

Leo: ZigBee. So it has a ZigBee antenna in support, although it doesn't do anything with it. So it's going to, you know, I think, yeah, you're right, I mean, this has been early days for a decade. At some point it's somehow going to be figured out, but...

Steve: Oh, I think we're seeing it now.

Leo: Yeah, it has to be.

Steve: I mean, with everybody's light bulbs and alarm systems and, you know, it's going exponential. It's a good market opportunity.

Leo: Well, the smartphone has really helped because the smartphone gave everybody a control device.

Steve: Yes.

Leo: And at this point we're in a situation where everything, like Ring, like Hue lights, they all have their own app. And so SmartThings was an attempt to, and still is an attempt to make one app that can talk to everything. That's why it supports both ZigBee and Z-Wave.

Steve: Right, and an app ecosystem, too, because they have an open programming environment.

Leo: That's right. But so does Apple. Apple has Home Kit.

Steve: Right. It's this, then that sort of interface.

Leo: Right, yeah. And Google and Apple are doing that, as well. So, you know. And I think tomorrow we're going to be doing a live broadcast of the keynote tomorrow at 10:00 a.m. Pacific, 1:00 p.m. Eastern time, 17:00 UTC. Andy will join me, and Ron Amadeo from Ars Technica.

Steve: Great.

Leo: And so, yeah, we're going to - Russell Holly. So we're going to cover the keynote, and I think there'll be a lot to say there about home automation. And I think Google will do the right thing, if anybody does.

Steve: Oh, and I know it's a huge interest of our listeners.

Leo: Oh, yeah.

Steve: And the security of it is obviously important.

Leo: Oh, yeah. And it seems prudent at this point not to use it for home security.

Steve: Yes, yes.

Leo: That would seem to be a wise idea.

Steve: Yes.

Leo: That's why actually most home security, good home security systems, don't they use - they don't use cell phones, they use landlines.

Steve: Yeah, mine does.

Leo: We had to install a landline because...

Steve: Mine does, yeah.

Leo: Because of the jamming.

Steve: Yeah.

Leo: Steve does this show every Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC. You can watch it live, participate. I guess Q&A next week?

Steve: Yes, let's do a Q&A next week.

Leo: Okay. So go to GRC.com/feedback, if you want to leave a question. Or Steve will take DMs on Twitter, or I guess regular open messages on Twitter. @SGgrc is his handle, @SGgrc. As you're traveling the web, do stop by GRC.com and pick up a copy of SpinRite. If you've got a hard drive, you've got to have some SpinRite. Get some SpinRite in your life, the world's best hard drive maintenance and recovery utility, even for SSDs. You can also find lots of other stuff, including - people were asking about Steve's latest Healthy Sleep Formula. It's in there. He doesn't make any money on that. He's not selling pills. It's not a vitamin shop. He also...

Steve: No, in fact I've had people asking for me to use affiliate links. And I said no. I just...

Leo: Good for you.

Steve: It's just too creepy. I just - I don't want there to be anyone who says, oh, yeah, you're just doing this so that you get affiliate credit. It's like, no, I don't want any credit. If everybody is sleeping better, that's great for everybody.

Leo: You'll be wide awake for this show.

Steve: That's right.

Leo: Coffee is not a substitute for a good night's sleep, my friends. You can get audio and video, as well, of this show on our site, TWiT.tv/sn. And the best thing probably is to subscribe. That way you get it each and every week. And you know what, it doesn't matter to us how you get it, just get it. We just want you to get it every week because there's always something good on Security Now!.

Steve: So far.

Leo: See you next week, Steve.

Steve: Thanks, my friend.