Dumb SmartThings

Description: Leo and I discuss an interesting week packed with security news, including Microsoft's Mega Patch Tuesday; the final word from Dr. Craig Wright; Lenovo, Microsoft, and Qualcomm each in separate doghouses; more Curl Bashing; terrorist math; lots more - and a look at the insecurity of the most popular home automation system, Samsung's SmartThings.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-559.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-559-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We're going to talk about the week's security news. There's a big, big Windows Update today. He's got the details. And then later we'll look at the ZigBee protocol and potential security flaws that make it probably a pretty bad choice for home security monitoring. Steve will have the details, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 559, recorded Tuesday, May 10, 2016: Dumb SmartThings.

It's time for Security Now!, the show where we cover your security and privacy online with this guy right here, our Explainer in Chief, Mr. Steven Gibson.

Steve Gibson: Oh, and for those of you who missed the pre-show...

Leo: Oh.

Steve: ...my eyes are watering...

Leo: It was kind of a silly pre-show.

Steve: ...from crying.

Leo: We may duplicate it, however, as we get into the full content. This is going to be a good show today.

Steve: We have a lot to do. This is our smart, or, I'm sorry, our Dumb SmartThings episode, where we're going to take a look at some research that various people have done into the operation and architecture and, frankly, the profound failings of the number one most popular home automation Internet of Things system, which Samsung bought from its creator back in 2014 and just sort of added to their Samsung collection of stuff. It is by far, in terms of number of apps and number of devices, currently the leader, although there are a bunch of other companies, one huge consortium, the AllJoyn, J-O-Y-N. That's like the Who's Who. It's everybody except Samsung is a member of that. So it'll be interesting to see how this evolves over time. But we're going to end up talking about that.

But we've got a Mega Patch Tuesday. We've got, thank god, closing the chapter on Dr. Craig Wright. Lenovo, Microsoft, Qualcomm, all in their separate dog houses. A fun little piece of curl bashing, following up on the problem of piping the output of curl into bash that we've been talking about for the last couple weeks. A strange event in the world of terrorist math. An expensive but possibly useful gizmo that I ran across on Gizmodo. A bunch of miscellaneous stuff. The Temperfect Mug actually exists. I received it. Actually, I think it was the afternoon of last week's podcast, so I've had a chance to play with it and can review it.

Leo: Oh. I want mine. Okay.

Steve: I have a significant breakthrough in the Healthy Sleep Formula. You, my sister, and my best buddy are all receiving bottles of one ingredient which has changed, which dramatically improves its strength and will allow, I mean, I'm still recalibrating things, in fact. It's like, it's big.

Leo: Wow. I love it that I get little pill bottles in the mail from Steve. I pick up the package, and it's rattle, rattle, rattle. I go, "Oh, new ingredient."

Steve: No excuse for not trying it.

Leo: Oh, no. I love it. Keep 'em coming, thank you.

Steve: We have a little follow-up on last week's hit, The Sequence puzzle game. The new companion app for the Zeo is released and available. A few more tidbits, and then SmartThings. So tons of stuff to talk about this week. Well, so we are on May 10th, the second Tuesday of May, and it's...

Leo: Oh, there's a big one, I think; right?

Steve: Oh. In fact, I made this deliberately redundant because it's just sort of a joke at

this point. This is the Windows Patch Tuesday bonanza. And so as I was putting this together, I thought, oh, this is just a crackup because we have a critical remote code execution flaw in Internet Explorer, where Microsoft says: "This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted web page."

Critical remote code execution in Microsoft Edge: "This security update resolves vulnerabilities in Microsoft Edge. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted web page." Critical remote code execution in JScript and VBScript: "This security update resolves vulnerabilities in Jscript and VBScript scripting engines in Microsoft Windows. The vulnerabilities could allow remote code execution if a user visits a specially crafted website."

Critical remote code execution in Microsoft Office: "This security update resolves vulnerabilities in Microsoft Office. The vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file." Critical remote code execution in some generic Microsoft Graphics Component: "This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a specially crafted website."

And it goes on, including same thing for Windows Journal, Windows Shell, and then we have somewhat toned-down problems in IIS, Windows Media Center, Windows Kernel, Microsoft Remote Procedure Call (RPC), Kernel-Mode Drivers, Adobe Flash Player, .NET Framework, Virtual Secure Mode, and Volume Manager.

So update Windows. I did that on my various Windows 7 machines. And, boy, I've been seeing reports about Windows Update being sluggish. And I don't know what's going on. Some people have suggested maybe they're prioritizing Windows 10 updates over the down version updates, specifically Windows 7. But, I mean, it's not snappy anymore, that's for sure. I don't know, it's like - I don't know what's going on. But I had 16 patches on both of two different Windows 7 machines, and some optionals. They keep trying to give me Silverlight, and it's like, no, I'm never going to want Silverlight.

Leo: What?

Steve: Oh, yeah.

Leo: I'm telling you, Steve, sooner or later you're going to go to Linux or BSD.

Steve: I don't doubt it. I don't doubt it.

Leo: OpenBSD would probably be the right choice for you. But I just put Linux on my Chromebook Pixel, and it's gotten so easy. I thought this was going to be quite challenging.

Steve: Nice.

Leo: It's a snap. And this is UEFI and Secure Boot and everything. And it's just, you know, you can do it. You have to turn off Secure Boot. But it's so easy.

Steve: Oh, and we'll be talking about that in a few minutes.

Leo: Right, yeah, mm-hmm.

Steve: Because there was a glitch in a bizarre...

Leo: I don't want to use Windows anymore. I really don't.

Steve: Yeah, I know. It's like you really feel like Microsoft is now fighting their users. I mean, every week now there are problems, and we've got some more that we'll talk about in a second. But I did want to close this chapter on the good Dr. Craig Wright. Everyone will remember that a week ago, just before the podcast, I was just shaking my head, and I tweeted, "I sure hope this clown is not Satoshi. Get a load of this latest spew of nonsense." And I shared last week's spew.

So what he then posted, you just have to shake your head. It's like, okay, you know, thank goodness this case...

Leo: This is a classic conman. Classic.

Steve: It is.

Leo: Right?

Steve: So for people who don't know, just listen to this. It's short. And it's just - it is just screwball. So it starts out - this is all you get when you go to drcraigwright, W-R-I-G-H-T, you know, D-R-C-R-A-I-G-W-R-I-G-H-T dot net. That's all that's there. "I'm sorry," it starts. "I believed I could do this." Now, okay. So just for a little back story, if anyone has skipped any episodes of the podcast or has been under a rock somewhere, he was going to give us proof, and spoofed apparently proof, to Gavin, who he knows and cares about, for reasons that are beyond comprehension still, several weeks ago. So now here's the final chapter:

"I'm sorry. I believed I could do this. I believed that I could put the years of anonymity and hiding behind me. But as the events of this week unfolded, and I prepared to publish the proof of access to the earliest keys, I broke. I do not have the courage."

Leo: Oh, that's what happened. He broke.

Steve: "I do not have the courage. I cannot. When the rumors began, my qualifications

and character were attacked. When those allegations were proven false, new allegations have begun. I know now that I am not strong enough for this." Okay, well, let me finish. "I know that this weakness will cause great damage to those that have supported me, and particularly to Jon Matonis and Gavin Andresen. I can only hope that their honor and credibility is not irreparably tainted by my actions. They were not deceived, but I know that the world will never believe that now. I can only say I'm sorry, and goodbye."

Leo: So that's what a con man does when he gets caught, basically.

Steve: Yes. Yes. Some bizarre loony-tunes spin. You know, yeah, he painted himself into a corner and just came up with another bizarro spin. Anyway, the guy is...

Leo: Bye-bye.

Steve: We're done with him. So, wow.

Leo: Bye-bye. So long. See you later.

Steve: Yeah. Okay. Now, get this. ASUS motherboards for a long time have enabled Windows Secure Boot, or just generic, you know, UEFI Secure Boot, by default. Secure Boot support was introduced with Vista, so it's always been built into Vista and successor OSes from Microsoft, thus Windows 7. Consequently, when Windows 7 systems have been installed on ASUS motherboards, which had Secure Boot enabled, those Windows 7 OSes were configured by the setup system with Secure Boot, which the OS supported by default.

Then, like a week and a half ago, for reasons still not explained, Microsoft reclassified a previously optional Windows Update, which is KB3133977. They reclassified it from optional to recommended. What that of course did was install itself on Windows 7 machines. What does 3133977 do? It removes from Windows 7 its support for Secure Boot because it's no longer "supported," in quotes. So everybody who had Windows 7 installed on ASUS motherboards, last week, when they rebooted their systems after this recommended update had installed itself and removed Secure Boot, was greeted with a big red warning from the BIOS with the title "Secure Boot Violation. The system found unauthorized changes on the firmware, operating system, or UEFI drivers."

Leo: Oh, no.

Steve: "Press OK to run the next boot device" - meaning give up on booting your hard drive because of course you can't - "or enter directly to BIOS Setup if there are no other boot devices installed." And then it says, "Go to BIOS Setup > Advanced > Boot and change the current boot device into other secured boot devices." Anyway, this is just...

Leo: Wow. I mean, that's what we have - don't you have an ASUS motherboard, too, on your new one?

Steve: Oh, my new one was a...

Leo: Gigabyte, you bought Gigabyte.

Steve: Gigabyte, yeah.

Leo: We bought ASUS. So I guess I can't do Windows Update. Oh, my god.

Steve: Well, so what's crazy is, like, Microsoft seems to be doing things that are hard to explain. Of course the conspiracy theorists say, oh, here's yet one more thing Microsoft's doing to try to move you from Windows 7 up to Windows 10. It's like, make Windows 7 no longer boot on your ASUS motherboard.

Leo: Geez Louise.

Steve: Yeah. So the problem was there was no clear connection between just doing Windows Update, which doesn't normally, or isn't supposed to, render your systems unbootable, and then this big red BIOS warning saying "Secure Boot Violation." How would you put those things together? And it's funny because, as I was putting these notes together, I was reminded of my discovery of the very first spyware from that Aureate company.

Leo: Right, right.

Steve: That's where I created OptOut. And what happened back then was that freeware was surreptitiously installing this Aureate spyware which was designed to be a kind of a central server of ads for that freeware and of any other Aureate-enabled freeware. But because it was surreptitiously installed, one of the problems was the Aureate freeware was - somehow it hooked into IE, but it broke IE for many people. So they install the freeware and use it to check their shoe size or whatever the heck it was doing. And then they go to use IE, which is now broken. And so they think, oh, that's odd.

Well, first of all, there isn't a connection between the two events. It's obvious. But maybe they uninstall the thing that they installed, thinking that it might have some connection, except that the instructions were, because many different pieces of freeware might be using this central ad server which you had unknowingly just added to your system, the explicit instructions to developers who included this Aureate stuff was don't remove it because other software may still be in the system which uses it. So you would remove that bad stuff you had inadvertently downloaded, that is, you would uninstall the freeware. It would leave the Aureate stuff behind, still screwing up your system. And we only found out about this when I created OptOut to find it and remove it. And then people said, "Oh, my god, my browser works again." And I was thinking, what? How does OptOut fix your browser?

And so it was by reverse-engineering that, the whole tale was finally uncovered. But similarly, here is, you know, you're just installing Windows Updates, and suddenly you're getting a Secure Boot violation, which just seems crazy. Anyway, so ASUS has

responded. They've got a patch for the BIOS. Maybe users, presumably users, if they figure it out, can disable Secure Boot and tell the BIOS, okay, calm down. For whatever reason we no longer have a Secure Boot-capable OS because Microsoft just decided to take that away from Windows 7.

So, I mean, again, I'm becoming, I mean, I'm a Windows developer, Leo. Never10, it was important for me to be able to crank out Never10 quickly. We're at something like 335,000 downloads, and 5,000 a day, so it's been a huge, I mean, I get all this great feedback from people. So I'm glad I'm able to respond. And Windows still is the majority OS in the world. So it makes sense for me to be here. But, boy, I mean, Microsoft is just becoming hostile to their users. And I'm with you, that it just does not seem like the place I want to be.

Leo: I don't get it. I just don't get it, yeah. It's just a mistake. I mean, it can't be - it's not intentional. I can't buy that it would be intentional.

Steve: You're right. You have to imagine that somebody at Redmond is in trouble for not testing this, or not considering the consequences...

Leo: That's what's weird. How could you not - yeah.

Steve: ...of retroactively revoking Secure Boot capability on an OS that has it. It's like, what? Why?

Leo: Odd.

Steve: And based on the protocol of Secure Boot, perhaps, I mean, perhaps they have to do this. But, unfortunately, this is something that should have been better thought through.

Leo: Is it possible that - somebody in the chatroom was saying ASUS implemented their own Secure Boot, that is it possible ASUS did something nonstandard, and that's why they're - I mean, obviously they're different than anybody else.

Steve: Good question. All I encountered in digging into this was that they enable Secure Boot by default. It may well be that other motherboards...

Leo: Oh, everybody does. No, no, everybody does.

Steve: For example, my Gigabyte motherboard supports it, but it's disabled.

Leo: Oh, really. Oh, interesting.

Steve: Yeah. And so I think...

Leo: Well, if you build your own, that makes sense because you could then put Linux on it. But if you buy a Windows machine, Secure Boot is always on by default.

Steve: Right. In fact, that was a requirement up until 10. Well, up until 10 it had to be on by default, but you had to be able to disable it.

Leo: Right.

Steve: They've softened that a little bit, where it's now sort of unspecified. So far, all the systems we've seen, you are able to turn it off. And of course the industry is sort of in a quandary at the moment. Alternate OSes need to either know that systems can have it disabled, or be able to support it themselves. So it's not quite sure where we're going to go. But I think the future is Secure Boot, that because of problems with rootkits and just trying to tighten security up - to me this all feels a little bit backwards, though.

Look at the list of fixes that we just had today in Windows in terms of anyone - basically, touch the Internet, and you can have malicious code run on your system. Okay, and we're worried about something affecting the boot? I mean, yes, that's a problem. We should fix that, too. But, boy, look at the inconvenience that that brings to the rest of the ecosystem. No inconvenience to Microsoft. They're able just to say, oh, you know, we're going to have Secure Boot, and we're going to make everybody else do it, too.

Leo: Right. Well, a lot of Linux users were upset about that because, again, the conspiracy theory was, oh, well, Microsoft doesn't want you to put Linux on your Windows machine. And you do in fact have to disable it to use Linux.

Steve: Right.

Leo: But you can disable it, so it's not the end of the world; right?

Steve: So Lenovo, back in the doghouse. The so-called "Lenovo Solutions Center" has both a userland or user mode app and a kernel mode backend server thing. And it turns out that they didn't code it correctly. There is an arbitrary code execution vulnerability which allows either a remote attacker or a local user to execute arbitrary code with full system privileges. So, once again, a problem with Lenovo. They've scurried around and fixed it. So if you do have Lenovo Solutions Center installed, you may want to ask it for a solution to itself, and have it supply that.

Leo: That's a little recursive. Solve yourself.

Steve: Meanwhile, Qualcomm, it turns out, five years ago, back in 2011, they provided some updates to the core Android system, adding a bunch of network features, including tethering capabilities. That required that they update the netd daemon in Android. And it

has just come to light that there are some serious problems with that. Now, the good news is not remote code execution, so not as bad as the Stagefright problems, where just receiving an MMS message can take over your machine. But this is a local privilege elevation flaw which does allow apps to get up to mischief that they shouldn't be able to. They're able to obtain access to the users' private data, including SMS and call history; to change system settings, disable the lock screen, and more.

Now, this has already been patched in the May Day Android security patch that we talked about last week. So it's been fixed. The concern, though, is that because this is old, this is back in 2011, that it's most worrisome on devices running Android 4.3 Jellybean and previous, which are unlikely to ever get patched. So I just sort of wanted to give our listeners a heads-up that, I mean, this is a problem that's been fixed in newer Android versions. It isn't known to be exploited. But over time, if you're running older Android, this may not get fixed. I mean, it's probably not going to get fixed. And so it'll be a known vulnerability that some mischievous developers could consider leveraging in order to get access, to basically break out of the app sandbox and get access to the OS-level features.

And in sort of a side note, both the FCC and the FTC are beginning to wake up to the whole question of mobile security and the obligation of carriers and vendors to patch this stuff. They're asking Apple, Google, and others for clarification of their policies for the factors that they consider in deciding whether to patch vulnerabilities on a particular mobile device. So that's good.

As we've been saying on the podcast now for quite some while, these are computers in our pockets. And we now have a long history of understanding that consumer devices need to be patched. First it's desktop computers. Then it's our mobile devices. And of course now we recognize that embedded devices like this whole IoT, the Internet of Things world, are going to be needing the same kind of ongoing patch maintenance. There just is, you know, all of our history and experience says that all of these systems are going to have weaknesses and flaws that need to get fixed.

There was also, remember I mentioned last week that the infamous 3035583 update, I saw that sort of like came back last week. And that's the one, that's the Get Windows 10, the GWX update. And there was some anecdotal report, like the day after I mentioned that, that the GWX icon had reappeared, and that people were being offered Windows 10 again. Now, the good news is not a single user of Never10 reported that. I did see one person who said he was going to be reinstalling the big GWX utility thing. I can't remember the name of it.

Leo: The Control Panel.

Steve: Oh, the Windows Control Panel, GWX Control Panel.

Leo: Right.

Steve: Then in a follow-up of some of the - it was Windows ITPro that initially reported it, I think on May 5th. Then on the 6th they updated their story, saying that this issue has only been, or may only be responsible - I'm sorry. This issue has - okay, the English. I did copy it right from the story. "This issue has only be reproducible," they wrote, so whatever they meant.

Leo: I've noticed lately, blogs no longer have anybody copy checking or proofreading. Even big blogs, frequent typos. You can see where - obviously the guy wrote "been" and then accidentally deleted the "en" or something like that. But you would catch that immediately if you looked at your copy before you filed it.

Steve: Yeah.

Leo: The standards have just collapsed for this stuff.

Steve: It's funny you mention that because I was also quoting, in the next story, the top of a blog post, and it was just full of spelling errors. And I thought...

Leo: And on, like, well-known, like The Verge and stuff. I mean, it's kind of - I guess they have to file so fast, so many stories, I mean, they really have to do many, many stories a day, that they don't have time to check it. Which makes you wonder about the facts.

Steve: It's also part of the culture now, isn't it.

Leo: Right.

Steve: It's this, oh, my goodness, we have to be first out with this. I mean, I will say, on the flipside, I was stunned but pleased by the rate at which Never10 was, like, found. And it was like, one site finds it, and they're all of course looking at each other's Twitter feed.

Leo: Well, that's - you can manipulate this, exactly, because there's such a huge need for content, if they're factories, that they will totally do that. Everybody will pick up everybody else's story, and it just goes. Everything's a wildfire now.

Steve: Or nothing.

Leo: And you miss that day, it's over.

Steve: Yeah.

Leo: What's sad is that we can be manipulated, and that's why we have the candidate for President we have. It's so easy to manipulate that technique, as well.

Steve: So whatever they meant, they said: "This issue has only been reproducible in a few reported instances and does not seem to be widespread. If you are experiencing this

problem, let us know so we can help determine if it's" - okay, and there should be an apostrophe there. Anyway, "if it's environment or configuration specific." So for what it's worth, something happened, and it doesn't look like, I mean, I immediately was worried when I saw this. It's like, I was just so sure that Microsoft would never think of violating their own group policy enforcement to prevent this, which of course is what Never10 uses is the fully normal sanctioned Microsoft-blessed way of not, you know...

Leo: Yeah. Yeah. That should do it.

Steve: Yeah. And so I was like, I was thinking, oh, my lord, you know, is Never10 going to be broken? And it's like, no. It's not clear what it was. What I think must have happened is various, you know, early on there were other wacky ways of semi-blocking this. And so those people who adopted earlier previous solutions, like maybe they installed the GWX Control Panel, then removed it, thinking it was no longer necessary, or who knows. And it did other things than what Never10 does. But the good news is we all appear to be fine. And I guess, is it the presumption, Leo, that in July, when the...

Leo: July 29th.

Steve: When the deadline - the deadline.

Leo: The deadline for free is over.

Steve: Update by now, or you're going to have to pay $129.

Leo: Yeah. Yup, that's July 29th.

Steve: To be further abused.

Leo: So presumably this will all go away then.

Steve: Oh, yes, nice, yeah. Wow. Okay.

Leo: By the way, important point. Probably everybody should do this. Turn off recommended updates. It is on by default in Windows 10, anyway. Just do critical updates. That's the ones you have to do. Recommended updates are the ones that bring along all of these problems, including the ASUS motherboard problem.

Steve: Right.

Leo: Just don't do the recommended updates.

Steve: Right, right. So we've talked for a couple weeks now, starting with the - I'm trying to think of the name of it, the Raspberry Pi...

Leo: I'm usually very good at guessing your intent.

Steve: ...VPN.

Leo: I don't know where you're going with this. Oh, yeah, yeah, that script.

Steve: Yeah, yeah, yeah, the script. But there was a fun name for it, and I'm blanking on it now.

Leo: I can't remember, either.

Steve: The chatroom will figure it out. Anyway, the idea was, what was fun was that you could plug a Raspberry Pi into your router, bring up its terminal window, and pipe the output of curl into bash. Curl is C-U-R-L, simply retrieves from a URL something on the Internet and spews it out. Well, when you pipe that into bash, the spew goes into the bash shell, so bash interprets those lines as commands. And basically, so it's an automated - it's a cool way, but dangerous, as we talked about last week, of basically turning your little Raspberry Pi over to a server on the Internet, to in this case install the OpenVPN. Okay. I think this will be the final comment on that. But I got a kick out of this. Phil, whose last name I couldn't find, he has a blog at IDontPlayDarts.com.

Leo: A good name.

Steve: And so he said: "Installing software by piping from curl to bash is obviously a bad idea, and a knowledgeable user will most likely check the content first." Which we talked about last week. "So wouldn't it be great if a malicious payload would only render when piped to bash?" So essentially we're escalating this as an attack vector.

He said: "A few people have tried this before by checking for the curl user agent, which is by no means failsafe," meaning that - remember that whenever you ask a server for something by URL, part of the query, the so-called metadata, the query headers, there's a user agent. You know, Internet Explorer declares itself, but they always say Mozilla for some deeply historical reason, and Chrome and Firefox and so forth. You're able to tell who's asking. You know, spiders that crawl the 'Net, they identify themselves as a spider. And so that allows the server to manage them however it wants to.

So the point is that, similarly, curl will declare something. And maybe there's some way of determining from the metadata, from the query headers, that it's being piped to bash. So he says: "A few people have tried this before by checking for the curl user agent, which is by no means failsafe. The user may simply curl the URL on the command line, revealing your malicious code. Luckily," he writes, "the behavior of curl and wget," which is actually - that's the tool that I often use on Windows - "changes subtly when piped into bash. This allows an attacker to present two different versions of their script, depending upon the context."

Now, okay. I did last week handle that by suggesting that you curl to a file, browse the file, see what the command stream is, then pipe that file into bash, meaning pipe what you have audited and looked at into the bash command prompt. But anyway, what's clever is, and his point is, that bash is an interpreter that is interpreting line by line what it receives. So if the first line of the script that is coming from the server is a statement like "sleep 10," "sleep 10" puts a 10-second pause into the interpretation of the script for whatever reason. Sometimes it's to allow something else to happen asynchronously. You just sort of want to pause the bash script. Maybe you want to put up a notice that the user will see when stuff's crazily scrolling by.

You want to just, like, pause so the user can look at something, and then you continue. The point is, that will create a pause in the pull from bash through the TCP connection that the remote server could sense. So if the server wanted to be malicious, that is, if it wanted to deliver different content to a terminal window versus bash, it could put a little pause at the beginning, notice if there was no pause in the pull.

Then it would say, oh, that sleep statement wasn't interpreted, it was simply displayed by the command window, and that would tell it to follow that with benign content so the user surveying it would go, oh, yeah, look at that, it looks all fine. Then when they issue the same command, but with bash, there would be a pause because bash would interpret the "sleep 10" statement, and that would then allow the malicious content to be swapped in its place, and you wouldn't know any wiser. So interesting sort of security lesson there, which is...

Leo: But I have to say that this kind of piping a script, downloading and piping is done all the time to save people steps and to simplify. I'm looking at this is something that a lot of people install on their Macintosh called Homebrew, allows you to install Linux packages. And you can see that the command is a one-liner that curls a script and runs it through Ruby. And that's very common. And, I mean, you see this all the time.

Steve: Well, and again, that's what was so elegant about this was that...

Leo: It's simple, yeah.

Steve: ...here's, like, one line. And, bang, you've got OpenVPN installed and configured on your Raspberry Pi. It's very cool. But from this podcast's standpoint, there is a security implication.

Leo: Oh, yes, absolutely. But anytime you install software from an unknown source, especially somebody named Inphektion, you should be careful. This is Oh My ZSH, which is a really nice shell utility. You see sh-c, and there's a curl command. You curl a script and run it, and it's a one-liner, and it just runs it. And so you see this all the time. And if you don't trust these people, they could screw you in many other ways, too. They don't have to run the one-liner.

Steve: Right, right. And again, I think that's - yes. That is an important point, and it's been one of the themes that we've been highlighting recently, which is just how much of

the whole system...

Leo: It's all trust.

Steve: ...is in fact out of our control.

Leo: Right.

Steve: And we know that security has to be soup to nuts. If you skip a course, there's an opportunity for someone to do a little man in the middle anywhere between the sand coming off the beach to create the silicon for the chips, all the way to you explaining to your mother-in-law why all of her files have been encrypted.

Leo: Sorry.

Steve: Sorry about that. What did you click on? Yeah. Okay. So...

Leo: Well, it was just a one-liner, a Perl one-liner. I don't understand why...

Steve: Okay. So this, I didn't know how I was going to cover this because this was interesting. But the Washington Post covered this event in such a wonderful narrative style that I wanted to just share it as it was written. So this was last week, Thursday evening, two days after last week's podcast. The writer says: "On Thursday evening, a 40-year-old man - with dark, curly hair, olive skin and an exotic foreign accent" - and I have a picture of him in the show notes - "boarded a plane. It was a regional jet making a short, uneventful hop from Philadelphia to nearby Syracuse. Or so dozens of unsuspecting passengers thought."

Leo: Clearly a terrorist. He's using al-gebra.

Steve: Oh. "The curly-haired man tried to keep to himself, intently if inscrutably scribbling on a notepad he'd brought aboard." A notepad, Leo.

Leo: Ooh.

Steve: "His seatmate, a blond-haired, 30-something woman sporting flip-flops and a red tote bag" - we still don't know her name, by the way...

Leo: No, she escaped.

Steve: "...looked him over." She gave him, you know, the once over. "He was wearing

navy Diesel jeans and a red Lacoste sweater - a look he would later describe as 'simple elegance' - but something about him didn't seem right to her." So she decided to try out a little small talk.

"'Is Syracuse home?' she asked. 'No,' he replied curtly." He simply "deflected further questions. He appeared laser-focused" - perhaps too laser-focused, Leo - "on the task at hand, those strange scribblings. Rebuffed, the woman began reading her book. Or pretending to read, anyway. Shortly after boarding had finished, she flagged down a flight attendant and handed that crew member a note of her own.

"Then the passengers waited, and waited, and waited for the flight to take off. After they'd sat on the tarmac for about half an hour, the flight attendant approached the female passenger again and asked if she now felt okay to fly, or if she was 'too sick.' 'I'm okay to fly,' the woman responded. She must not have sounded convincing, though. American Airlines Flight 3950 remained grounded.

"Then, for unknown reasons, the plane turned around and headed back to the gate. The woman was soon escorted off the plane. On the intercom a crew member announced that there was paperwork to fill out, or fuel to refill, or some other flimsy excuse; the curly-haired passenger could not later recall exactly what it was. The wait continued. Finally the pilot came by and approached the real culprit behind the delay: that darkly complected foreign man. He was now escorted off the plane, too, and taken to meet some sort of agent, though he wasn't entirely sure of the agent's affiliation, he would later say.

"'What do you know about your seatmate?' the agent asked the foreign-sounding man. 'Well, she acted a bit funny,' he replied, 'but she didn't seem visibly ill.' Maybe, he thought, they wanted his help in piecing together what was wrong with her. And the big reveal: The woman wasn't really sick at all. Instead this quick-thinking traveler had 'seen something,' so she had 'said something.' That 'something' she'd seen had been her seatmate's cryptic notes, scrawled in a script she didn't recognize. Maybe it was code, or some foreign lettering, possibly the details of a plot to destroy the dozens of innocent lives aboard American Airlines Flight 3950. She may have felt it her duty to alert the authorities just to be safe. The curly-haired man was, the agent informed him politely, suspected of terrorism.

"The curly-haired man laughed. He laughed because those scribbles weren't Arabic, or another foreign language, or even secret terrorist code. They were math. Yes, math. A differential equation, to be exact. Had the crew or security members perhaps quickly googled this good-natured, bespectacled passenger before waylaying everyone for several hours, they would have learned that Guido Menzio is a young but decorated Ivy League economist, and he's best known for his relatively technical work on search theory, which helped earn him a tenured associate professorship at the University of Pennsylvania, as well as stints at Princeton and Stanford's Hoover Institution."

Anyway, yes. See something, say something. But maybe - who knows what was going on during these hours of tarmac stall and then return to the gate. But no one bothered to figure out who he was. And they do seem to maybe have overreacted a bit, since this was just some math scrawled on a notepad, not formulas for explosives. Wow. The story generated 4,700 comments, which I did not have time or any further need to read.

Leo: I think you get the gist after the first few, I'm sure.

Steve: Wow. Wow.

Leo: Sad that we celebrate ignorance in this country, it really is. It's just sad.

Steve: Okay. Now, at first blush, this seemed crazy to me. But upon further digging I thought, well, there are some applications, perhaps, for this. Gizmodo had the story, and they titled it: "When Your Internet Goes Out, This Smart Plug Resets Your Router Until It Works Again." And I thought, what? So get this. It's a cute little thing, Leo. It's ResetPlug.com. Bring that up, a big, pretty picture of it. ResetPlug.com. Gizmodo wrote:

"When your Internet goes out, resetting your WiFi router and cable modem often seems to fix the problem. Instead of getting up from the couch to fiddle with power cords, why not let a tiny outlet..."

Leo: This is actually a great idea.

Steve: Except that it's $60.

Leo: I know. Because the cats knock off our Internet all the time, and it would really be...

Steve: "Why not let a tiny outlet router power cycle your hardware for you?" Now they write: "You might balk at the ResetPlug's $60 price tag, but it's not an awful idea for people who hate having to get up when the Internet goes out. You plug the device into an outlet, then plug your WiFi router, modem, or both, into the ResetPlug itself." It only has one outlet, so you need a Y adapter. "It constantly monitors your home's Internet connection; and, when it detects a problem, it automatically cycles power to your router and modem until the Internet returns." So again, ResetPlug.com.

Leo: I wonder how much of a delay it puts in there.

Steve: Yeah, there would be some.

Leo: It takes a while; right?

Steve: Yeah. Well, it takes, my god, a cable modem takes about an hour to come back online.

Leo: Right.

Steve: Now, I was thinking, okay, take that same $60 and just buy a real router because, frankly...

Leo: One that works, you mean?

Steve: Yeah, one that doesn't hang. I've never had that happen once. And, yeah, I buy high-end routers.

Leo: Right.

Steve: Now I have a little PC running pfSense, and it's just bulletproof.

Leo: Right.

Steve: But really, come on. Yes, you can drive with a tank of gas and jumper cables in your beat-up car that won't hold a charge, or you can just get a good battery. I would just say, $60? Get a real router, and you're probably fine. However, when I looked at their page, they did bring up some interesting points because, when you're not home, you're not there to reset anything.

Leo: Right.

Steve: And if you're depending upon, as people, as we'll be discussing here when we get to the content at the back half of this, the Internet of Things stuff, and you do have, for whatever reason, a tendency for your home to go off the Internet, then this makes a lot of sense.

Leo: Lee Hutchinson in Ars Technica wrote about this. He said: "ResetPlug is a $60 device to keep you trapped in crappy WiFi hell." It's a Band-Aid. But it's true that, if your burglar alarm is on WiFi, or you know my Ring Video Doorbell. When the WiFi's out, the doorbell's not going to work.

Steve: Right. Exactly. And so on the ResetPlug page they say security cameras, thermostats, smart appliances, smoke alarms, carbon monoxide alarms, Smart TV or DVR, remote computers, sensors, security alarms, smart lighting, file servers, other IoT devices - the point being, yes, I mean, what is actually happening is our homes have to be on the 'Net even when we're not there, for exactly the example you'd give, Leo, with the Ring Doorbell, but all these other things, too. And so, yeah.

Now, what we'd like to see is a router that's smart enough to, like, reset itself when it realizes it's lost connectivity. I guess if it hangs, though, it can't. Okay. But embedded devices have always had - I'm blanking on the term - a dead man feature, where there's a hardware counter. And what it does is it's in hardware, and it counts up. And if it ever overflows, it pulls the hardware reset line - I'm sorry, watchdog timer, that's the term, a watchdog timer. And it's been part of embedded technology forever.

So the idea is that, in the software loop, the event loop, for example, the main event loop for the software, every so often it has a software timer which expires, and that

software timer pulls an interrupt that tells the watchdog, which causes the watchdog timer to be reset. And so the point is, every second or so, while the OS is running, it's resetting the watchdog. And if the OS ever hangs for any reason at the hardware level, that it stops being reset, that hardware counter overflows, a hardware reset is performed in order to basically reboot the router. It'd be nice if we had that. Apparently we don't in our consumer blue plastic routers.

But anyway, I wanted to share this because, frankly, though it seems a little pricey, you could do this for 20 bucks, and I'm sure there will be some for 20 bucks, although patent pending because it's an invention. And so maybe not. Maybe you've got to go - but still, I wanted to share it with our listeners because I thought, okay, there will be people for whom this provides an answer that they've been looking for.

Leo: All right, Steve. Onward.

Steve: So catching up on a bunch of loose ends and previous news, the much-discussed, oft-discussed Temperfect Mug arrived.

Leo: Oh, I'm so excited. Yay. Now, that's the titanium edition.

Steve: This is, yes, this is the ridiculous, I'm embarrassed now that I...

Leo: Powder-coated titanium.

Steve: ...spent this much money. Although it'll be interesting to see how it weathers over time. It's a titanium oxide, which, I mean, apparently you can't scratch it. It is, like, way too hard. It's sputter deposited at 3,500 degrees through some process. And I have to say, I mean, it is gorgeous. It has sort of a fine-grain sandpaper feel, which is nice because you'd like, if it's not going to be a rubber grip, you'd like it to be a little grippy. And so this provides that.

But mostly what intrigued us three years ago when this project began on Kickstarter was the concept that, as coffee drinkers, we, was the concept that it had a phase-change inner lining which - and by that I mean it actually is changed from a solid to a liquid. And that changing, it's a waxy-like nontoxic substance which, anyway, it's not, like, exposed to the coffee. It's behind actually three layers of aluminum. And so there's a sandwich.

And the layer closest to the coffee is this stuff which rapidly, in about two minutes, absorbs the initial heat of the coffee, which is initially too hot to drink, bringing it down to drinkable temperature. And so the idea is that inner lining has a large thermal inertia. So it holds - it takes the heat out of the coffee, but then puts it back in over time. Yeah, there is this crazy titanium. You're showing the video of it being sputter deposited.

Leo: Kind of plasma spraying it, yeah.

Steve: Yeah, it's crazy. So the idea is that it pulls the heat out, but then returns it as the coffee cools. And then the next layer is a vacuum layer. And in fact, I mean, these guys,

there has been constant email flow from them as they've gone through the trials and tribulations.

Leo: Did you get a serial number on yours?

Steve: Yes.

Leo: You're one of the first 10.

Steve: Number two.

Leo: Oh, my god.

Steve: You could see him etching it.

Leo: Wow.

Steve: And so I got a very nice note from Dean, one of the guys. He says: "Hi, Steve." First, I mean, the way it looked, I thought it was just printed to all of the early adopters. But he say: "Hi, Steve. I don't remember exactly how it happened. It's been a long time!"

Leo: They raised a quarter of a million dollars for this thing.

Steve: He says: "But somehow my nephew, Will LaValley, brought our Kickstarter campaign to your attention late 2013. You talked about it on your podcast, and I think we got a lot of tech-savvy coffee-loving backers because of that mention. We really appreciate it. You were also our second Titania mug backer. And since we happen to be shipping the Titania mugs first, you get the second-ever Temperfect Mug. I hope you love it. Feel free to get in touch with any questions or comments." So I just have to say it's the real deal. The good news is I think the reasonably priced ones are, like, $40 or something.

Leo: Yeah. That's the one I got, $40. And still haven't received. He said it may take a while.

Steve: Yeah. And it actually works. It kept coffee hot for three hours, I mean, like truly hot, while the outside was weirdly cold because I think the AC was on that day last week. And so it would just, I mean, there was no heat leakage except out of the very top where there's a plastic lid.

But for what it's worth, I mean, it's been - I'm sure all of the backers know, because we were getting constant email from these guys, all of the problems they had. They are

perfectionists, and they were not happy with the way the shutter was working. The first three samples didn't hold vacuum. Then they figured out how to do that. I mean, it was just one thing or another. They didn't give up, and they did deliver. So bravo.

And it's a beautiful piece of work. I mean, it is 100% commercial grade. It's got a beautiful seal on the top. And you can feel the heat coming through the plastic, so there is some nominal heat loss. But the bulk of it doesn't lose heat, and it surely does keep the coffee hot for hours. And other people responding to my tweet said, "Who wants to drink three-hour-old coffee?" And that's, you know, you're right. You're normally going to drink it before that. And the point is you can. So there is a very nice solution for keeping our coffee hot for a long time.

Leo: Can you still - you can buy them, he's selling them, if you didn't get in on the Kickstarter?

Steve: Yeah.

Leo: Yeah. So, yeah, you can.

Steve: Okay. So the Healthy Sleep Formula is a hit also, but wasn't effective for everyone. And I think this change will change that. It's something I finally got around to exploring four days ago, and it's made a huge difference. And the difference is I switched the L-theanine from a capsule to a tablet. There's a well-regarded company, Source Naturals, which makes effectively a slow-release or extended-release version of L-theanine. That's the amino acid in green tea. And it is one of the key components of the Healthy Sleep Formula. What it does is raise the level of glycine and GABA, both which are inhibitory neurotransmitters, and also raises dopamine nominally.

The problem is that the ability for it to get into our brain through the so-called blood-brain barrier is rate limited. It shares something known as the leucine transport, which is what main dietary amino acids use. And that is a rate-limited transport. So what happens is, if you take L-theanine in a capsule, which when it's dissolved dumps all of the theanine into your blood stream, you get a short spike of high concentration which our livers start metabolizing and rather quickly remove from our blood.

One of the things that happens is the greater the concentration, the greater the rate of removal, which creates a half-life effect where the half-life, for example, might be an hour. So an hour after you've taken it, the concentration is reduced in half, and then another hour later that half is reduced in half, and another hour later that half is reduced in half. So you get an exponential decay curve. The problem, though, is if our ability to get it into our brain is rate-limited, then we've lost the bulk of the effect because, even though it was initially high concentration, it didn't have a chance to get into us. And of course the melatonin that I chose is similarly time-released for the same reason. We want it over the course of the evening.

So what this one change, by switching to this tabletized form of L-theanine, does is it trickles it into our bloodstream over the course of the night. So it raises the level in our blood. Since the concentration level is never super high, our livers' rate of removal of that L-theanine is also not super high. So it gets to stay present. And that's at a compatible level to the rate at which it is able to cross the blood-brain barrier and get into us.

Bottom line is this changes everything to such a degree that I'm now having, I mean, to rejigger the formula. I tried removing glycine completely last night. That was a mistake. So I had a middle-of-the-night wakefulness for about 90 minutes. But after I realized I wasn't able to get back to sleep I quickly took some glycine. And as soon as it got into me, then I was. Anyway, I will have - there will be more changes coming. But Leo, you, my sister, and my best buddy...

Leo: We've received the patch. We have the update, the patch to the formula.

Steve: Yes.

Leo: Okay.

Steve: Exactly.

Leo: And I realize I should take the Taurine out. I just reread the page, and you've decided Taurine causes you to pee too much. So let's not do that. Okay.

Steve: Yes. Many, many people reported that the diuretic effect of Taurine was just - it was causing them a problem. And while it can be beneficial, it's like, eh, okay, maybe take it in the morning, if you're a morning supplement taker. It's good for you. There's lots of benefits to having Taurine, to supplementing Taurine. But you don't want to take a diuretic just before bed. And so Taurine's removed, or I should say relocated to the morning. You might as well use up what you've got.

But please, I mean, I have to say I am amazed at the difference this makes, and really delighted, because some people were not finding a success with the formula, and I think this will change that, probably across the board. So I've got the links on the Healthy Sleep Formula page. I knew that it was going to be subject to change, and this is the nature of this sort of work. Other people have had problems, for example, finding GABA. I think Australia you can't get it, and there are some places in the U.K. where it is not available. This may obsolete it. I don't know yet. I'll be finding out, challenging myself with some sleepless nights.

So it's still subject to change. But absolutely, without question, you want to change to this particular Source Naturals L-theanine. They have some others, but unfortunately - some other L-theanine-containing tablets, but they've also got Taurine in them again. And so I think we probably want to stay away from that.

Oh, and I've been in constant touch with the InterPlexus people that make Seriphos because of course this is the great Seriphos shortage of 2016, that apparently is going to end in about two weeks. So I did make a note on the page also that, by the end of this month, it should be back in stock at retail. They were encapsulating it two weeks ago. Now they're running it through quality assurance and hoping to have it within about a week and a half. And it ought to take some time for it to get out at retail. But many people, I mean, there has been no Seriphos in the industry since shortly after this Healthy Sleep Formula caused all the retailers to sell out of what they had. And they've been reformulating it. Apparently we're going to get an even better one next round.

Leo: Good.

Steve: So the wait is almost over. And I just did want to make - I wanted to make sure that people who may not have moved on the recommendation last week of The Sequence puzzle, I wanted to remind people about it. It's been a huge, huge hit. And you said, Leo, before the show, I think, that it was your pick for iOS Today yesterday?

Leo: Yup, yup, my app cap, yup.

Steve: Do you have any idea how far...

Leo: It's really fun.

Steve: Yes, it is. Do you know how far along you are?

Leo: Oh, not very far at all.

Steve: Yeah. Many people, there are a couple people in the 40s.

Leo: How many total levels are there; do you know?

Steve: I don't know. I don't know. So 22 I was hung up on for a couple days. And I should say, like, I'm not in a hurry to finish this. I would recommend to people that they just sort of take it as it comes. Look at a level, spend a few days. What I notice sometimes is that I'll work at it, I can't figure it out, and I just - I get tired. And it's like, okay, I'm going to put it down. And I pick it up the next day, and it comes to me. So anyway, I'm at 29 at this point. No, I finished 29. And I actually solved it with only three pieces. There were seven available, and I only needed three because I'd noticed something in an earlier level that was not obvious. So for what it's worth, people are really liking it.

I had also mentioned that someone in the GRC health newsgroup, where there's been a lot of conversation about the Zeo EEG headband, was working on and nearly finished with a piece of free open source software that is now at v1.01. And on the Zeo page at GRC, just GRC.com/zeo.htm, you can find links to that. It's got just an amazing amount of additional features beyond the standard Zeo software. And we now never need to worry about that Zeo software disappearing. This thing is, like, exports the data, shows much finer grain resolution. If anyone is, like, deeply into the Zeo, then I recommend it. I'm really quite happy with the standard app. It just tells me enough of what I need to know for my own, you know, for the Healthy Sleep Formula research that I'm doing.

Second to last is that many people have asked about how I'm cooling the hard drives on this mega machine that I built and talked about a few weeks ago, because I talked about putting some big copper heat sinks directly onto the hard drives. And the problem is that I didn't just buy the heat sinks. I've had them for years. I used to have them on the hard

drives in my Series One TiVos, just because I believe in keeping drives cool. And so the air circulation in the TiVo would blow across the fins and bring the drive temperature down.

What I did do was I put a link in the show notes to the Arctic Alumina Thermal Adhesive which I used. This is a two-part epoxy adhesive, and it is way permanent. So what I did was I peeled the plastic label off of the top of the hard drive so that it's metal on metal, or rather bonded with this thermal adhesive. You want to be careful to see whether there's a vent hole. Many hard drives, if not all, will have a little vent hole somewhere to keep the internal and external pressure equalized. So you don't want to cover that up.

But otherwise, if you just eBay or use Amazon or just google "copper block heat sink fins" or something, you get Google's images, or just like pictures of them. And all you really want is just a big thing that will fit over, occupy a lot of surface area over the drive. And so it doesn't really, I mean, if I'd just purchased them, I would have a link to offer. But it's really noncritical. You just want to make sure the fins are not too tall so that they'll fit within your enclosure.

And there's just tons of copper block heat sinks. So just google that, or look on eBay, and get a couple, and just glue them to the label-removed metal surface of the hard drive, and you should be good to go. And also arrange to have it in the air flow. You want some air to flow over it, and it makes an incredible difference in the drive's temperature.

And lastly, many people said, "Hey, Steve, don't you know that when you transfer a domain, the recipient registrar always honors the total remaining life of the domain?" And the answer was, no, I didn't know that. Now I do. So thank you, everyone, first for telling me. And then I just finished performing a series of experiments, moving some domains that had lots of time left on them over from Network Solutions over to Hover.

And Hover wants me to pay for one year at that domain's annual fee for moving it over, but then they tack that year onto the existing remaining time the domain had at the old registrar so that you're not disincentivized from moving to them. Which makes sense. I was just surprised because they're not getting any money, potentially for a long time. So that's why I was just assuming they weren't going to honor the existing remaining time on the domain. But they do.

So for anyone who might also not be sure, I wasn't; now I am. And everybody else knew. So thank you for letting me know, everybody. And I've confirmed it.

And speaking of confirming, not that we need much confirmation at this point of what SpinRite's able to do. But I found a fun story. Actually he sent it to Sue, who forwarded it to me, from Kev Blythe in the U.K. He said: "Hello, Steve. I would like to say thank you for that magical item of software you call SpinRite. A local garage called in a panic." And it's funny, Leo, because you were just talking about some old laptops that are still necessary for car service of some sort?

> **Leo:** Oh, yeah. There are, whatever it is, 15 McLaren F1s out there, these very, very expensive cars. And the way they created them, I'll see if I can find the image, they can only be modified by a particular old laptop which they're running out of because there aren't that many of them.

Steve: Yeah, well, so this may - I don't know if that's this, or just what the garage had, but he said...

Leo: Twenty-year-old Compaq. This is it.

Steve: Yeah?

Leo: That's it. That's the only one they can use.

Steve: I have one of those laptops, by the way.

Leo: Well, you should contact the McLaren folks.

Steve: No. I'm keeping it for the Gibson Museum.

Leo: Yeah. This is one of the - this is probably the most expensive production car ever produced.

Steve: Wow.

Leo: Yeah. It's like a $10 million car.

Steve: Oh, no.

Leo: Yeah, yeah, yeah. They only made a hundred of them, and they have to use - they only built 106 of them. There are a hundred left.

Steve: And so it is tied to some aspect of that particular laptop.

Leo: Yeah, because the - actually...

Steve: The software will only run on that laptop?

Leo: It's for a particular hardware interface.

Steve: Oh.

Leo: So that's the engine, by the way. Looks like a jet aircraft engine. And the interface is, well, there you go. You see those big plugs?

Steve: It does look like the inside of an airplane.

Leo: Yeah, yeah, yeah.

Steve: Wow. So anyway, so this...

Leo: LTE, if you've got a Compaq LTE-5280, I would call McLaren.

Steve: Yeah, we'll see what they're willing to pay. So anyway, in this case he says: "A local garage called in a panic. An old diag laptop had failed with a BSOD and was going round and round in circles, like the owner. So I picked it up for a look. I confirmed a hard drive issue; and, having worked in a local PC repair shop, where I often witnessed the proof of the power of your software to get hard drives back into bootable state, I headed to GRC for my own copy of SpinRite. I grabbed a copy, and before lunchtime the machine was repaired, imaged, returned, and smiles all around. Many thanks. Kev Blythe, U.K., and a local garage." So, Kev, thanks for sharing that.

Leo: Yeah. Maybe you should - I bet the McLaren folks have a SpinRite lying around. Apparently it's DOS.

Steve: I have a lot of the early Compaq laptops. I was, I mean, they weren't really practical back then. They were monochrome. But, hey, I'm DOS, so it was fine.

Leo: It's DOS, yeah.

Steve: Yeah.

Leo: Still use Brief. All right, Steve. Now, I should tell you, a little disclaimer upfront, SmartThings is a sponsor of our network. They were a Kickstarter project which I invested in and love. I bought the original Hub. The idea was a single hub and a single app will translate and talk to all the other stuff. And it uses most of the protocols. And it's really convenient. I got the upgraded Hub when Samsung bought them about a year ago, upgraded the Hub. And I have all of the devices. So tell me, am I in trouble?

Steve: So, yes.

Leo: Oh, dear.

Steve: It's a case of the classic tradeoff between simplicity and security.

Leo: Yeah.

Steve: And the initial pass being used for more than it was intended to be used for. So, I mean, and the good news is there's a future in v3 of the ZigBee protocol. ZigBee is a low-energy, low-power, low-data rate WiFi that links all these things together There's also Z-Wave, and then of course Bluetooth Low Energy are the various technologies. Bui ZigBee is the one that's - it's been around for more than a decade. It's an IEEE standard 802.15, I think it is, dot something or other. And so most of these devices are running on top of ZigBee. And ZigBee is at v1.2. I don't know what happened to 2.0 because everyone's already talking about 3.0.

And the problem is that - okay, there are a couple problems. So as I understand it, Samsung purchased SmartThings from the SmartThings guys. Without being a fly on the wall or being privy to their development decisions, I have no context for understanding many of the decisions which an analysis of the result demonstrates were made, which seem wrong in retrospect. So it may be that what's happened is that, due to the way the Internet of things has evolved, we're using this in a way where I'm tempted to say we're misusing it, or we're abusing it, which is to say we're relying on a system that was never designed for security, for security.

And I was thinking back, for example, to the origin of email, and how we've often talked about how difficult it is to secure email because it was never designed to be secure. And the people who designed it knew that it wasn't secure. It was for academics to send papers and stuff back to each other. And then fast-forward 15 years, and you're wanting to send corporate confidential documents to your patent attorney. And it's like, whoa, whoa, whoa, whoa, whoa, whoa, whoa. Email's not secure. And it's like, well, yeah, but we want it to be. It doesn't matter. It's not.

So probably the SmartThings guys are absolutely aware of the fact that this should not be controlling your door locks. This should not be used for an alarm system. Fine, make your lighting green or blue. Have it control your light bulbs and maybe tell you when your toothbrush has been recharged. But don't use this for mission-critical things. We didn't design it for that.

Yet the problem is that, wouldn't it be fun if you could use it for your home security. There's a market there. And it's like, yes. But the infrastructure isn't secure. And so you can imagine how it goes from there. So it is a very cool, open standard, easy to develop for platform that is super popular. It is by far and away the most popular standard that we have at the moment. There's Samsung SmartThings. There's Apple's HomeKit. There's Vera Control has something called Vera3. Google has their effort, Weave and Brillo.

And then there's something called the AllSeen - it's a little creepy name. At least it's not "AllSeeing." If it was the AllSeeing Alliance, that would be too strange. But the AllSeen Alliance, which has something called AllJoyn. And they're, like, the Who's Who. Basically everybody else is there, more than 200 members. I put a link in the show notes, Leo, AllSeenAlliance.org/alliance/members. And, I mean, the page just scrolls on and on: Canon, Electrolux, LG, Microsoft, Philips, Qualcomm, Sharp, Sony, Buffalo, ASUS, AT&T, Cisco, DigiCert, Honeywell, IBM, LiteOn, Netgear, Panasonic, and those are just the big names. I mean, it's just, again, everybody else. And if numbers matter, there's a lot there.

On the other hand, SmartThings is where all the action is today. So it's certainly

important for us to recognize that we're in early days. And I think where we are is in this awkward place where we're wanting to do things that we don't have the underlying framework for yet. And, boy, that's not a new tune. That's the story of the Internet, where we decided, oh, yeah, let's add forms to the web so users can submit things. And then people say, okay, but that's not secure. Oh, well, but we want it to be. But it's not. Well, but, yeah, but we want it to be. Well, okay, sorry, you know.

So several things. Two researchers from the University of Michigan and a researcher at Microsoft Research did a deep dive specifically into the SmartThings system. And they analyzed 499 different SmartThings apps, which are called SmartApps; and 132 different device handlers were examined. I mean, there was, again, without talking to the original developers, without understanding why they made the decisions they did, we can't reverse-engineer their intent. But, for example, there is a privilege separation model as part of SmartThings, where devices that share the Hub are intended to be isolated from each other, and separated.

Yet the nature of the way this was implemented forces what these guys call "significant overprivilege." And I'll define that a little more closely with some examples. But what they found was that more than half, 55% of SmartApps are overprivileged due to there being insufficient granularity in the privileges. So again, I don't know why, maybe they tried to fit all the privileges into a 16-bit token, and so they just lumped them up by category rather than enumerating them for whatever reason. But they also found that, once installed, a SmartApp is granted full access to a device, even if the app specifies needing only limited access.

So that, again, we want, in order to have a secure system, we want much tighter control. SmartThings has an event-based architecture or platform, where devices communicate asynchronously. They indicate what events they want to be notified of, and then receive that code, receive those notifications. But what the researchers found was that it did not sufficiently protect events which carry sensitive information, such as door lock codes.

So I just picked four examples from their work, where in exploring this with no documentation or help from the developers, just doing essentially the work anyone could do, they remotely exploited an existing SmartApp, which is available on the app store, to program what they call "backdoor pin-codes," meaning additional pin-codes, into a connected door lock. Their attack made use of what's called the LockCodes capability that the SmartApp never requested, but the SmartApp was automatically overprivileged due to the current protocol lacking sufficiently granularity. They were able to eavesdrop on the event subsystem within an installation in order to snoop on the lock pin-codes of a Schlage smart lock when the pin-codes were being programmed by the user and then leak them using the unrestricted SmartThings-provided SMS API.

So essentially they installed the SmartApp, which was a spy. And when the user programmed pin-codes, that was SMSed out to the outside world. And the app that was created simply advertised itself as a battery monitor, and only requested battery monitoring capability, yet was able to do much more. They were able to disable an existing vacation mode on the SmartApp, which was available in the app store, using a spoofed event to stop the vacation mode simulation. So presumably that, like, shuts things down or turns something off when you say that you're on vacation. And they were able to defeat that remotely. And no capabilities were required for that attack.

And, finally, they were able to invoke a fake fire alarm using a spoofed physical device event. And that attack showed that an unprivileged SmartApp was able to escalate its privileges to control devices it's not authorized to access by misusing the logic of benign SmartApps.

Then, separately, several years ago - because this, as you noted, was a Kickstarter a long time back - another researcher was able to trivially jam the well-known ZigBee radio frequency used by SmartThings and was able to enter a protected home.

Leo: But this would be anything that used ZigBee would be susceptible to this; right?

Steve: True, true.

Leo: Well, so it's not a SmartThings flaw, it's a flaw with any hub that speaks ZigBee.

Steve: Well, except that it also - the problem with SmartThings is that there was no acknowledgement given that there was jamming going on.

Leo: Oh, I see.

Steve: And so you'd like to be able to at least say something is jamming us. There's like a malicious signal in the air. So, but again, I mean, so agreed, Leo, this is a problem with any radio frequency-based system which you're using for home security, which is using sort of consumer-grade technology. So this guy was able to enter, tripping window and door alarms, and move through the interior, suppressing all warnings, and the system didn't acknowledge that there was a problem.

Leo: Wow.

Steve: Yeah. So, and I don't want to mischaracterize this final piece, so I'm going to share what Dan Lieberman, who is the head of research and standards at SmartThings, said just this last December, because there's something known in the protocol that they're built on, on this ZigBee protocol. And again, it's not their fault that they're using ZigBee, except that ZigBee's what everyone uses. And so my point is that it's not ready for primetime. It's an insecure system.

So he explains in his FAQ at SmartThings, he says: "There are really two distinct things at play here, and I'll do my best to describe them, what their potential impacts are, and what we're doing at SmartThings to eliminate or mitigate them. I apologize in advance if this is overly dense, but there's a lot to get to here." And of course it won't be dense for our audience.

He says: "What are the issues? First, as has been pointed out in this thread, there is a designed 'moment of insecurity' in the ZigBee Home Automation 1.2 spec that uses a well-known symmetric encryption key, known as the Trust Center Link Key, to distribute a unique network key when a device first joins the network." Okay, now I should pause here and say that it's much worse than that. It is possible, since this Trust Center Link Key is globally known, it's been tweeted, anyone with a ZigBee radio and an Arduino can become a device on anyone else's SmartThings network. That is, it is trivial to

authenticate yourself, unfortunately, to the network. And the reason is that they want to make it easy. And it is. Unfortunately, it's easy to abuse.

Anyway, he continues, saying: "This is a tradeoff that the ZigBee Alliance chose to make between security and simplicity, with a mitigated impact, given that an attacker would have to be capturing ZigBee network traffic at the same time that a new device is being joined to the network." And that actually is not true. Many people - there's a lot of demonstration of researchers who have just added themselves to existing networks.

He says: "This method" - and this is the key, though, the good news is "This method has been removed from the upcoming ZigBee 3.0 specification and replaced with a process that requires a per-device installation code that is used to generate a unique joining key, which is then used to acquire the ZigBee network key. The install code may be printed on the device, may be a 2D barcode that is scanned by a camera, or some other out-of-band method of passing the code from the end-device to the ZigBee Coordinator device - in our case, the SmartThings Hub - such as NFC or Bluetooth Smart."

Okay. So again, where we are is, as he says, the acknowledged tradeoff between security and simplicity. And the problem is we're in this place at the moment where an insecure technology that its designers probably never intended to be used for secure applications, is nevertheless being used for security applications. But work is underway for the spec to catch up. The problem is none of the existing devices will be 3.0 ZigBee. It'll only be things after the ZigBee 3.0 spec happens which understand this secure protocol join technology. And they won't be as easy to join. But they shouldn't be because the fact that it's so easy means that attackers can do it, too. And so nothing new here for our audience.

He says: "The second issue described by the CognoSec" - there was a report that I've linked to at the bottom which is an extensive reverse-engineering analysis, which is different than the research that I talked about before, the U. of Michigan guys and the Microsoft Research researcher - "is a method known as 'insecure rejoin.' Insecure rejoin also exists in the ZigBee Home Automation 1.2 specification as a tradeoff between security and simplicity. This method allows a previously paired device to rejoin a network using the same well-known Trust Center Link Key in the event that the network key changed since the last time the device joined the network.

"This enables battery-powered devices that aren't always listening for commands from the ZigBee Coordinator - otherwise known as 'sleepy' devices - to rejoin a network if the network key changed, as the sleeping device wouldn't have received the new key update from the ZigBee Coordinator. So if an end-device such as a motion sensor or contact sensor fails to join the network using their stored key, they can ask for the new key, which is transmitted using the well-known Trust Center Link Key." Well, okay. Wide-open security breach because it means that anything can pretend to be an "I don't know the network key, please send me the network key using the Trust Center Link Key, which is public knowledge."

So anyway, he says: "The specific issue that CognoSec describes in their publication is the ability to spoof a device on the network to send a false insecure rejoin request, triggering the network key to be sent using the well-known Trust Center Link Key. This bypasses the mitigation effect described above" - which, as I already said, isn't valid, I mean, isn't a mitigation even - as an attacker could, he says, potentially cause, well, yeah, I would say readily cause, "the network key to be transmitted at will."

So then he says: "How is SmartThings impacted, and what are we doing about it? SmartThings currently supports insecure rejoin, as many ZigBee Home Automation

devices will only attempt to rejoin once with their stored key before reverting to an insecure rejoin mode." Meaning that the SmartThings Hub and architecture have had to come down to the lowest common denominator in order to be functional with the least secure of any of the ZigBee Home Automation devices.

"This means," he says, "that without insecure rejoin, if there are any issues rejoining the network after a Hub reboots or a router in the mesh goes away, the device would not be able to rejoin the network and would be effectively stranded. The only way to resolve a stranded device would be to delete it from SmartThings, perform a factory reset on the device, and put it back through the initial join process.

"We do recognize the security concerns presented by spoofed insecure rejoin requests, and since the issue was brought to our attention we've been developing an update that will give users the option of turning off insecure rejoin while we work to understand the broader negative impact of simply disabling it by default. We hope to have this update in place within the next 60 days." Well, that was written in December, and it's not in place today, so it's taking longer than they had hoped.

"Once the feature is available, we'll let you know how to go about disabling insecure rejoin. In the longer term, the ZigBee 3.0 specification eliminates the insecure rejoin process." And again I'll say the problem being that none of the existing devices will know about 3.0, and they will all assume insecure rejoin is available. So I don't know how that's going to get handled.

"As for the initial joining process, SmartThings must support the standard ZigBee Home Automation 1.2 Trust Center Link Key join process because that's how nearly all ZigBee Home Automation 1.2 certified devices join a ZigBee network." Again, lowest common denominator problem. "And as an open platform, we support many ZigBee Home Automation-certified devices from many manufacturers. As mentioned above, ZigBee 3.0 will eliminate the 'moment of insecurity,' but we're also exploring methods," blah blah blah blah.

Anyway, so you get the picture. So I don't mean to beat up on them. This is the dilemma of a system where user convenience completely trumps security. And if it was light bulbs, you know, and your TV, I mean, things where security didn't matter, fine. Unfortunately, it's because of the convenience and people saying, oh, hey, let's do home security. Well, as long as you regard it as a toy, it's fine. Don't expect it to protect you. Or at least, I mean, in the default case it probably can.

But it is not robust by any means in the face of anyone who wants to defeat it. At this point, it's just a wide-open system. And again, not SmartThings' fault. It's the fact that they're trying to be compatible. In order to say they are ZigBee Home Automation compatible, they've had to accept the operation of things that are just not secure. And unfortunately, it's brought the whole system down to that level.

So again, we're in the early days. And I would simply urge people to wait until we have a standard defined. If you really want security, just don't rely on this for any application where you're relying on it for affirmative serious residential security. Use it for things that are fun. And also consider that you're probably going to have to replace a lot of your early hardware once a secure spec occurs.

The good news is it is being worked on, and the problems are recognized. And ultimately it'll be less easy to use. But it needs to be less easy to use. There has to be an out-of-band process. And we've talked about this often. I mean, that's why authentication is a problem. It's why Signal and WhatsApp and Threema show you an optical instance of an

identity, because you need out-of-band authentication. There's no way around that. Otherwise, anybody can pretend to be a valid device and get into your network. So this is going to advance over time. It's early days. I would consider this a toy at this point, not something you use for mission-critical work. But I think we're going to get there.

Leo: Good. But, now, just to be fair to SmartThings, this would be a problem with any hub that used ZigBee; right?

Steve: Yes. Any. Exactly. It's not about SmartThings.

Leo: I think SmartThings is getting the attention because they're responding to it. I think most of them are - ZigBee's a widely used protocol. So what we're really saying is don't use ZigBee for home security.

Steve: Yes. Yes.

Leo: SmartThings does support other protocols, like Z-Wave. So I'm not sure, I imagine somebody's looking at Z-Wave, as well, which is a similar protocol.

Steve: Yeah.

Leo: Sounds like these shouldn't be used for home security because radio jamming would be an issue.

Steve: Yes, yes. And there are, like, 500 SmartThings apps and 50 other things apps. I mean, they're, like...

Leo: They're the king of the hill. No, I agree, yeah.

Steve: SmartThings is the absolutely...

Leo: Yeah, you're right, right.

Steve: And so of course they're the people that the people...

Leo: I just want to be fair to them. It's not something they did.

Steve: Agreed.

Leo: It's a flaw in a protocol they support.

Steve: Although earlier I was talking about things that are hard to explain, the overprivilege of devices, the fact that unprivileged devices are able to do things, that's different than the ZigBee level. That is about the SmartThings protocol.

Leo: Right.

Steve: And it's not fair. They're not here to defend themselves. So again, and as I said, I don't mean to attack them. I can't - I don't - there's no context for understanding what the security researchers found and were able to do. And if someone sends me a link, I would certainly happily cover that in the future.

Leo: Yeah. Well, there you go. Once again, Steve Gibson. He is our support, our staff, our candle in the wind.

Steve: Our now-exhausted weekly...

Leo: And he's sleeping well. He didn't sleep well last night, but he's going to sleep well tomorrow.

Steve: Actually, I got eight hours because I gave myself a buffer, knowing that I might lose an hour and a half in the middle. So I did get eight.

Leo: The rest of us call it sleeping in. He calls it "I gave myself a buffer." That's Steve, right there in a nutshell. I sleep in; he gives himself a buffer. Steve.

If you want to know more about the Healthy Sleep Formula, the latest, GRC.com. There's lots of free stuff, lots of interesting information. We should say Steve's not a doctor. He's just an interested amateur. You know, take it with a grain of salt.

Steve: Yeah. Well, and you know what I was realizing, too, is that the constant theme here is technology.

Leo: Yeah.

Steve: And I think of technology as applied science. So science is sort of the theory and an understanding of what happens. Technology is taking that and making it do something. And so for the last 10 years I've been learning about the science of our biology. And so just in the same way, what intrigues me is the technology. Like, okay, why does 200 milligrams of the same amino acid dribbled out over time have a phenomenally more powerful effect than that 200 milligrams released at once? And I understand it, and half an hour ago I explained it. And to me that's just fascinating.

Leo: Oh, yeah, yeah.

Steve: And, oh, Leo, wait till you try this. It is night and day.

Leo: He's hacking his sleep.

Steve: It changes everything.

Leo: I can't wait. You should also check out SpinRite. That's there, too, GRC.com. That's the world's best hard drive maintenance and recovery utility. And also text transcripts of the podcast are at the website, GRC.com. So are, of course, the podcasts themselves, the audio versions of the podcast. And if you have a question for Steve, you can leave a question there, GRC.com/feedback. He also accepts the occasional DM. Well, he accepts them all, I don't know if he reads them all, @SGgrc on the Twitter.

We have full-quality audio and video on our website, TWiT.tv/sn. Doesn't matter where you get it. Either way, just fine with me. Or subscribe, because it is a podcast. That means there is an RSS feed, and you can plug that into your favorite podcatcher, and you should get it. Or use the TWiT apps - they're everywhere - and subscribe that way. But we do this show every Tuesday, 1:30 p.m. Pacific, 4:30 p.m. Eastern, 20:30 UTC. If you want to stop by and watch live, you can also do that. Make sure you're here next Tuesday and every Tuesday for Security Now!. See you, Steve.

Steve: Thanks, Leo.