Listener Feedback #213

Description: Leo and I discuss the week's major security events and discuss questions and comments from listeners of previous episodes. We tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world application notes for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-510.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-510-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We are live, and we are going to do this show come heck or high water. Talk about the latest security information. Steve's got questions and answers. Why is he moving to Windows 10? That's a really good question, coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 510, recorded Tuesday, June 2nd, 2015: Your questions, Steve's answers, #213.

It's time for Security Now!. Leo Laporte with the Inartful Dodger, Steve Gibson. And we are here - but I say that in the best way. Inartful because he has no artifice. What you see is what you get with Mr. G. We are here each and every week to talk about the security news.

Steve Gibson: For good or bad.

Leo: For good or ill. But isn't that how you want it, right, you don't...

Steve: Ah, yes, exactly.

Leo: No artifice.

Steve: So we're in a Q&A finally because we had a blessedly quiet week, and nothing catastrophic happened in the last seven days. Well, actually, the Mac EFI, UEFI BIOS

arguably is a concern. And then there was the crashing of your friends' iPhones on purpose. And Microsoft now annoying and frightening users with an unsolicited offer to upgrade to Windows 10, we'll talk about.

Leo: Really? That's a bad thing?

Steve: Oh. Well, it appears on their toolbar. And Microsoft has never given anybody anything.

Leo: Oh, interesting.

Steve: Let alone the next version of Windows.

Leo: Right.

Steve: So people are assuming it's malware.

Leo: Oh, wow.

Steve: That it's a come-on, and that they're being tricked into this. So, and then of course everyone's wondering what I think about Google's Vault project, and so I'll put that in context. And I have to talk about Soli because I'm just - that just curls my toes, it is so cool, the other Google ATAP project. There was some news about supercapacitors, that we haven't talked about for a long time. A bunch of media miscellany that we're not going to take much time with, but I just wanted to note things because they tie into previous podcasts. And a great Q&A. So a neat podcast, full of stuff.

Leo: I cannot wait. All right, Steve. Put down that coffee. It's time to do some news.

Steve: So our photo or our Image of the Week on the first page of the show notes is a screenshot of the bottom of somebody's Windows installation with this "Get Windows 10" when they hovered over the little Windows icon.

Leo: Well, you wonder, what is this new flat icon there in my toolbar? I didn't see that before.

Steve: Yup, yup, yup. And so what's happening is Microsoft is proactively putting this in people's Windows 7 and 8 machines, offering to have them reserve, pre-reserve their copy of Windows 10.

Leo: I don't really understand what the benefit is to that, frankly.

Steve: I don't, either. And, you know, I made a post, I guess I tweeted that I had installed Windows 10, the current build whenever it was, a couple weeks ago. And I found it really, like, surprisingly unready. And Paul, I guess I must have included Paul because he replied, "Yeah, tell me about it." And so now they've got this end-of-July official ship date, and I'm thinking, oh, boy. So, wow. And I guess it's that they really want everybody to move. And so since they decided they're going to make it free, they've said, well, not only are we going to make it free, but we're going to, like, send the word out that this is coming. And so this is so - it's like, weird. It's like, why do you have to reserve your copy? It's being downloaded.

Leo: It's free.

Steve: It's not like there's a limited number of them or anything. So it's like, I don't know. Anyway, so what's really funny is that people are seeing this and going, what? Oh, this, you know, Windows 10? And they know that there is no such thing yet. So they just figure because the little - the hover-over shows "Get Windows 10," and they, like, immediately back away from their computer, figuring that this is malicious.

Leo: Right.

Steve: Anyway, I got just a kick out of that. And Microsoft, you know, pushing it. You can - there's a link, I'm coming back to this in the notes, but there's a link that you can go to on their site to sign up for the preview. And I don't advise anyone to do it because from what I saw, as I said, it's surprisingly far away from done, if they're going to be shipping it in two months. So I wish them luck. Of course, top of the news was this iMessage crash that was just, you know, a black eye for Microsoft.

Leo: For Apple. For Apple.

Steve: For those who don't - I mean for Apple, Apple, yeah.

Leo: Let's not beat up Microsoft too much today. This is Apple's problem. Yeah.

Steve: Nah, not for this one. So if there's anyone who doesn't know what it was, it turns out that someone discovered a bizarre combination of characters. And the only way I can imagine this was found was through some reverse engineering. You know, you're not going to arrive at this randomly. A couple English words, a bunch of unicode stuff, and some Japanese characters. And the point is that there are three places where messages can appear, iMessages can appear. They can appear in the notifications area where, if your phone is locked, you can still see notifications coming up. They can appear in the preview mode, where you see all of your various dialogues, and it's there. Or they can appear where you see an entire single dialogue.

Two out of those three locations, the first two, would cause a complete crash and reboot of the phone any time it attempted to display them. So if somebody sent this wacky string through iMessage to, you know, you want to say a friend, although you wonder what kind of a friend the sender is, to somebody else who had notifications turned on. In

the act of showing it, that person's phone would crash. Or, if they then showed it in the preview, if they had previews set up so they could see the beginning of individual messages in different message conversations, then again it would crash.

So it turns out that there's a module called CoreText, and it's not surprising it would be called that because this is clearly some sort of a text string rendering problem. And the crash was occurring in an API call, CopyFromStorage. So something, and I didn't go any deeper into it because the world knows about it. There were a number of weird sort of workarounds that were discovered, and I heard you discussing one of them, Leo, where you used Siri to help you eliminate...

Leo: None of them are workarounds. It won't go away. It just mitigates it by deleting that message until somebody sends it to you again.

Steve: Correct.

Leo: It doesn't fix the problem.

Steve: Correct. And so what we're hoping for and expecting is that Apple will respond to this quickly and get us an update. And by the way, iPhone 4's and earlier are safe. Not the 4s, but the 4, because the last iOS version is 7.1.2 on the iOS 4, and it's not vulnerable. So this is another instance of, you know, problems creeping in as features are added. And they then need to get found and fixed. So...

Leo: That'd make you wonder how the bad guys found it because it's a very obscure thing.

Steve: Oh. Yeah, you can't arrive at it randomly.

Leo: It's multiple languages, that kind of thing. But doesn't it feel like it's a buffer overflow, that it's somehow crashing because it's writing into memory somewhere it shouldn't be?

Steve: Yeah, I mean, I'd like to use a...

Leo: I guess you can't really tell.

Steve: Yeah. I know that from - in fact, there's a link in the notes here to that ghostbin.com/paste/zws9m, all lowercase, which shows some crash dumps of it occurring. And so the top item in the crash dump, so if you scroll up a little bit, or down, there's a list of - that's the call stack. And so the last entry, that CoreText call, was a crash in the CopyFromStorage API. So, I mean, I don't want to use these terms loosely because I don't know exactly what it was that happened. But it may have been fuzzing. Fuzzing is this act where you just throw a lot of stuff at something and see if it crashes it. And when it does, you say, whoa, and then you scroll back in your log and zero in on

what it was you threw it. So, I mean, and that's one of the, you know, the guys at, I want to say FireEye, used fuzzing on Windows years ago to find all kinds of API problems, things you would just normally never find, that it just, you know, random data that's unexpected could crash the system.

Leo: The reason I kind of assumed it was a buffer overflow, anytime you see a copy, a memcpy or a strcpy, that kind of implies that it's copying data from one place to the other. If that place it's copying data to is not big enough, then you're going to get a buffer overflow. So that's the only reason I assumed that.

Steve: Yeah.

Leo: Because you know, if it is that kind of crash, that's just a precursor to finding an exploit that could give you far worse results than just crashing.

Steve: Oh, yeah. Absolutely, yeah. And I thank you for mentioning me when you talked about this before because you talked about how we've often said that these vulnerabilities that start out as a crash, that's where the hackers roll their sleeves up and then figure out how to weaponize what was just a crash into carrying their own payload into memory and, you know, using it for a jailbreak or to, who knows, lower the defenses on the whole system.

Leo: Right, right.

Steve: So Macs have had a problem also.

Leo: Oh. This one is scary. This one's really scary.

Steve: Yeah. Yeah. What was discovered by a researcher, the way he tells the story, he stumbled onto this because he was looking very closely at a particular system whose passwords he had forgotten. So he was trying to get into it for his own - just to, like, recover some passwords that had been lost. And the tools that were available at the time were so slow in pulling data out of the EFI BIOS that it just was infeasible. But some newer tools had arrived that made it more possible. And so he thought, okay, I'll take a look at this.

And what he discovered was that normally when the Mac boots, as part of the BIOS, before the OS gets running, just the BIOS, part of that process locks BIOS memory down. The BIOS is not stored in ROM, it's stored in EPROM so that you could have BIOS updates, which are certainly handy when problems are found or we need to extend it, we need to add more drivers, you know. This is all in nonvolatile memory, most of it, you know, on the motherboard, not in the - on physical rotating or mass storage media.

So part of the process of the BIOS coming up after it's through doing whatever it needs to do, for example, and we talked, we had a podcast about how UEFI boots a couple months ago, after it's through creating its logs and getting itself going, it write-protects vast regions of itself, that is to say, making it read-only. And it does that because it

doesn't want to be modified. It doesn't want to allow any software running afterwards the opportunity of reaching down and making changes. It turns out that on a range of MacBook Pros and MacBooks and MacBook Airs, dating from about a year ago and older, so this looks like something that Microsoft - I'm sorry. I'm sorry.

Leo: I confuse the two easily. It's not...

[Crosstalk]

Steve: ...something that's Apple.

Leo: Yes, it's not - of course.

Steve: Looks like something that Apple found and silently fixed. The problem is these are, the ones that are still vulnerable, are using the latest firmware, which Apple is no longer maintaining. So it's not...

Leo: Oh.

Steve: Yes. So it's not clear whether this issue coming up will induce Apple to fix this problem, now that they've essentially been caught out because, as this researcher put it, this is not something you could fix by mistake. Someone found it and said, "Oh, crap," and, like, fixed it around the middle of 2014.

Leo: But didn't fix it for earlier versions of the computers. That's the vast majority of Macs.

Steve: Correct. So what happens is this. If, and only if, the Mac comes out of a suspend-resume, through whatever path the code goes in these buggy UEFI BIOSes, the read locks or the write locks, making it read-only, are forgotten. So if you boot up from power off, there's no problem. And in this guy's detailed description, I have a link in the show notes if anyone's curious, he shows a breakdown of the BIOS map after a normal cold start and after a suspend-resume. And there are a couple lines that are clearly missing from the recovery from a suspend-resume, where the BIOS is writeable. And so his discovery is that, from userland, that is, from an application running as a user, it might need admin privileges, which may be a mitigation. I saw one reference to you needing to be root in order to have the access that you would need.

Leo: Yeah. That's what Rene Ritchie said. But almost everybody who uses a Macintosh runs as administrator because, unlike Windows, Apple, even if you're running as administrator, will require an admin password to do anything significant, anything risky like installing new software or affecting a system file or folder. So I've always, you know, we've always said, and I've been following your lead, if you're using Windows of any stripe, do not run as an administrator. But I've always said, eh, you don't have to worry about it so much on the Mac because you have to

escalate even if you are. This is the reason why all of a sudden you must not run as administrator.

Steve: And there was something we talked about a couple months ago, too, where the advice was create another user, log in as that person, and then remove admin privileges from the normal login.

Leo: Right. Right.

Steve: So we're beginning to see the need to do this, I'm afraid, on the Apple Mac platform, you know, in the same way...

Leo: I guess you could turn off sleep, but that's not...

Steve: Well, so mitigations are, as you said, do not use sleep. Only use shutdown. Do not run as an admin. And we're assuming, and if Rene has confirmed it, then that's good enough for me.

Leo: Yeah.

Steve: So I'm glad to have his confirmation. So do not run with admin privileges. Or, hopefully, get updated firmware from Apple. Or get a newer Mac.

Leo: Ha. Mid-2014 ain't that old.

Steve: I know.

Leo: That's only a year old.

Steve: I've got one here that is, you know, that is...

Leo: Yeah. Well, most of my Macs are more than a year old. I'm doing it right now on the iMac here, and I'll do it on all my laptops. Yeah. Hmm, wow.

Steve: Yeah. So anyway, I mean, this is where we have a little bit of a problem with Apple. Apple has - I don't know their internal thinking. I can only guess. But what we do know is that Microsoft has finally gotten serious about security. And we went through a decade of pain while - and I do mean to say "Microsoft" - while Microsoft got themselves up to speed. And now we get a lot of information from them when they have a problem. Apple is famously rather mute about it. They say, "Oh, yeah, we fixed a bunch of security problems." Okay. I mean, without much more detail. So it'll be interesting to see how

they handle this. As you said, Leo, a year is not a long time ago.

And at the moment, these - so this was tested against a MacBook Pro Retina, a MacBook Pro 8.2, and a MacBook Air, all running the latest EFI firmware available. All were vulnerable. And so what this means is that, if on one of those platforms, if you were running with the default admin privileges, as you said most, I mean, like virtually all standard Mac users are going to be, and you use suspend-resume, and you have resumed from a previous suspend, and something malicious gets into your system - so, you know, it's just a chunk of ands, it's a lot of ands - then that program can modify your BIOS. And that's the end of the world. That's, like, people are calling it a rootkit because we don't have anything lower than root. But it's actually a pre-rootkit.

Leo: Wow.

Steve: It's, I mean, a rootkit is something that normally gets control of your system before the OS, but after the BIOS. This allows malware to change the BIOS to do whatever it wants. And of course today's UEFI, it's a little operating system in and of itself, as we said a couple months ago when we were talking about how the EFI system works. So I think we have to just watch and see how Apple responds. I hope they're going to be responsible. I hope there's an outcry from people saying, hey, I bought this last summer, and now you're telling me there's no fix? That does seem like they need to go back further in time.

Leo: I want to clarify because Rene said that you would - so first of all, this can be activated remotely. But you have to first compromise the machine with something like Rootpipe before you can then do the subsequent UEFI modification.

Steve: Correct. Well, the idea of a remote hack would be you'd get in...

Leo: You need a remote root.

Steve: Yes. Yes. So you get in and then force a suspend-resume. So that's what the remote guy would...

Leo: That's why. Ah, yes, of course, yeah.

Steve: Yes, yes.

Leo: Otherwise you can't do that, yeah.

Steve: Right. And so...

Leo: But that means, you know, most of these hacks, you know, with the Mac

especially, you need access to the hardware direct, you know, you need to be in presence of the computer. This does not.

Steve: No. This is software running one way or another, whether you downloaded it by mistake, or a malicious Flash app infected you, or who knows what. So the easiest thing to do is not use suspend-resume. Simply do a full shutdown and a cold boot whenever you want to use your machine, and then BIOS will be write-protected as Apple intended it to be. And I did think it was interesting that this guy found them having fixed it. And as he said, this just, you know, you don't fix this by mistake. You say, oh, wow, and, like, creep around and fix all of the BIOSes in your machines and then hope nobody notices. And unfortunately for Apple, somebody did.

Leo: Wow.

Steve: So we already talked about - the title on this next one was "All roads lead to Windows 10" because there's, like, Microsoft is pushing it from all these different directions. There's a, if you go to windows.microsoft.com/windows/preview-download, here's Microsoft doing something I've never seen them do, offering to the general public to download a preview version of Windows, the next version of Windows. And of course it's, I mean, this major change of philosophy which we've talked about, I'm sure you and Paul have ad nauseam about Microsoft suddenly saying, oh, we're going to give it away. We're going to allow Windows 7 and 8 and 8.1 users to upgrade to Windows 10 because that's what we want everyone to be using. So as I said, in addition, they've now - a tray app has been installed. It turns out...

Leo: I got it. I just turned on my - I was just curious, so I...

Steve: No kidding.

Leo: Yeah, I just turned on my Windows 8 machine, so I can actually, well, I don't know, it's kind of small. But if I go to the desktop there's a little flat Windows icon there.

Steve: Yeah.

Leo: And if I hover over it - oh, you see, you're not going to really be able to see it, it's so small. It says "Get Windows 10."

Steve: Yup.

Leo: Now, I presume - so it...

Steve: Now click on it, and you get a big blue panel.

Leo: It says "Reserve your free upgrade. Go to Windows Update. Get to know Windows 10." So let's reserve my free upgrade. By the way, nice. UAC, User Account Control, says "Do you want to allow the following program to make changes to your computer?" I can see why people would be a little nervous.

Steve: Yeah.

Leo: Oh, that's bad. What happened there? It just went away. "Check your upgrade status." I'm good to go. "Once your upgrade is available on July 29th, Windows 10 will be downloaded to your device." I wonder if you can back out of this? Like if I say yes and then change my mind, or hear some things, can I just say no, I don't want to do it? Well, I'm going to do it. I like Windows 10. You know, Steve, it's a fix for Windows 8.

Steve: I know.

Leo: Which you never saw.

Steve: I've already got it on one machine. And in fact the number one question I think today is, Steve, why are you talking about going to 10? So, like, you know, what happened? What's changed? So I thought I'd explain that a little bit. For what it's worth, this thing doesn't go away. You only have to bear it for two months or just ignore it. Presumably you can use the little hide tray things feature in the taskbar to tell it don't ever display that. But there are two - people are wondering, how do I get rid of this? And so there are two updates. If you go to Control Panel > Programs and Features > Uninstall an Update, then you look for KB3035583 and KB2952664. So these were standard Windows updates that just sort of slipped in, and that's the functionality that they provide. You can uninstall them, and then that'll just disappear from your machine, if for whatever reason you want to stay where you are.

Leo: By the way, yeah, I've clicked through on the Windows 10. It says "You can cancel your reservation at any time." So once you reserve Windows 10, you don't have to install it.

Steve: Well, and what is this, it's nonsense, reserve? Because they've, like, got a limited number of bits?

Leo: Bits. I know, bits, they're running out of bits. It might be, you know, this is probably, what, three or four gigabytes. It might be that they expect millions of people to download it on Day One, so they want to stage that out. That's the only thing I can think of. But, you know, it's also just an ad. Because notice, by the way, that Windows icon does not go away from my taskbar.

Steve: Yup.

Leo: My system...

Steve: Yeah, I think that's what it is. I think this is Microsoft, yeah, this is Microsoft saying, since we've decided we're going to give it away, we're now going to push it, like a drug pusher, and make everybody have it. So it's like, oh, well, okay.

Leo: And you should probably know that this says pretty clearly that it will, as soon as it's available, it will download in the background. So that may be part of the staging process, like...

Steve: So on August 1st, when no one else in the house is able to get online, it's because you've saturated your Internet connection loading Windows 10.

Leo: It says, by the way, a 3GB download required. That's pretty hefty.

Steve: Oh, yeah.

Leo: I, on the other hand, I feel like this is a good way to do it. Windows 10, in my opinion, is an improvement. Now, we don't know bug-wise, reliability-wise, stability-wise. Just UI-wise it's an improvement on Windows 8.1.

Steve: Well, yeah. In fact, so much so that they didn't want to confuse anybody with 9. They thought, we're going to put as much...

Leo: Yeah.

Steve: They're going to put as much distance between themselves and 8 as possible. So going any further than 10 would have been a little too embarrassing, you know, Windows 100. But, you know, 10, it's like, oh, okay. We get it, Microsoft.

Leo: Keith in the chatroom says you can go to Task Manager and turn the nag off. It doesn't have to be - it's kind of annoying to have an ad for Microsoft running at all times.

Steve: Well, and so now you can see, Leo, if this appears, and someone isn't expecting it...

Leo: Yeah, right.

Steve: It's like, it looks very suspicious.

Leo: Especially since it has a UAC warning.

Steve: Uh-huh. Yeah, bend over. So...

Leo: I like - I, for one, love Windows 10, and I'm going to get it.

Steve: Leo, I think I'll be there. But, you know, cautiously.

Leo: Well, you were lucky because you skipped 8 for the most part.

Steve: I skipped 7. And I skipped Vista.

Leo: Vista you were lucky.

Steve: Vista and 7 and 8.

Leo: Yeah.

Steve: So I'm just, you know, and that's - okay. We'll talk about that in a little bit when we get into our Q&A.

Leo: Okay.

Steve: So we've talked about Apple. We've talked about Microsoft. Now we've got to talk about Google. Of course Google I/O was the never-ending keynote. Was that - when was that? Was that last...

Leo: Thursday and Friday.

Steve: Thursday and Friday, yeah.

Leo: Four days ago.

Steve: Wow. Okay. So they have something called ATAP, the Advanced Technologies and Products Group. And they showed three things, two of which, of course, well, one of which I have to talk about, which is Vault. And the other one just, oh, lord, if I had any time - and don't worry, I'm not going to get myself distracted. But I would love to play with Soli.

Leo: No kidding. Doesn't that look cool? Yeah.

Steve: Oh, Leo. I just think we're going to see a revolution in clever stuff. Well, we'll get there in a second. First Vault. So the press hasn't really understood what this is, but our listeners will. This is a cleverly designed HSM. We've talked about HSMs before, a Hardware Security Module. I have one right here. This is an early one from Yubico. This is Yubico's HSM. The idea with any HSM, Hardware Security Module, is it holds the keys, and it performs some operations on those in such a way that no sensitive data ever leaves. Parts of it are write-only, that is, there's no API, there's no means for reading these things out. And, for example, we've talked about it, you know, Apple's so-called Secure Element in their iPhones is the same thing. That is a, in many senses, a coprocessor, which is also what Vault is, which does trusted work for you of a very secure nature.

So Google's got one, too. And what's clever is they've packaged it in a microSD card form factor. Now, this is very much like Stina from Yubico, who packaged their original one-time password device in a USB keyboard emulator. And that's what I - that's where I just instantly loved what she did was that, as our listeners will remember, this little thing pretended to be a keyboard. And it automatically typed out a one-time password, every time you touched the little button. And what was so elegant about her solution was that there were no drivers needed because all computers know how to accept a USB keyboard being plugged in.

Well, what Vault does, because Vault tackles a different problem, it's doing bulk encryption and decryption. It can handle streaming audio and video and connections and high-speed file encryption and decryption. So they needed an interface much more robust that a USB keyboard. What they did was they stuck this in a microSD form factor, and it creates a virtual file system. There's not actually a file system. But what any operating system, Android or Windows or OS X, anything that is able to read and write data to an SD card is able to talk to this. So it pretends to have an "R" file and a "W" file for write and read. And so you communicate with this thing by writing commands and data into the write file and reading back its results from the read file. They aren't actually files. They're just sort of convenient file descriptors that allow any operating system to not need drivers. You'd still need custom software that understood it was talking to Vault and that it was doing Vault-ish things. But what they avoid, in the same way that Stina's clever keyboard hack does, is any issue with kernel drivers. Linux can handle it; all the OSes can handle it. So I just think it's a clever piece of work.

Now, you know, the newspapers and websites were sort of carrying the message that, oh, my god, you know, this is the end of passwords. Well, it's part of a solution. I mean, it's a hardware security module. So you could put things that are critical to you in it and have it do work for you. What, you know, in use, for example, imagine that you were using it with a video streaming app. You could run all of your raw audio and video into it, and out comes the enciphered result. And notice that the key is - pardon the choice of words - that the key never leaves. That is, you route the data through it, and it does the work without ever revealing any of the cryptographically sensitive material. So, which is what sort of by definition any hardware security module is.

So, you know, neat piece of technology. I'm glad to see it. And it's a very clever form factor. It means that it's going to take a while for this to get incorporated into products and for it to be out. And I don't, I mean, at this point it's sort of we're seeing prototypes, and they're showing it at Google I/O. The source, I think the whole thing is open and at GitHub. I have not gone through and looked at the API and looked at it in any greater

detail. And we'll see what sort of trajectory this takes, how long it takes to get traction and to what degree. And if it makes sense, we'll do a podcast that talks about it in much greater detail. But a just very nice piece of work.

Leo: How does this work with FIDO? Isn't FIDO, too, the competitor to SQRL, the single sign-on solution, blah blah blah? Is this related?

Steve: So it could be used by FIDO, potentially. To the degree that FIDO has credentials that you need to keep secure, you could presumably put them in there, and then it would protect them.

Leo: Okay.

Steve: So, and it's got a couple cores, and it seemed to have some strong processing power. So I don't know how much of FIDO might be able to run in there. But if nothing else, it could do the - it could provide ultimate protection from your credentials escaping from you, from your control.

Leo: Yeah. And then presumably PGP keys and all that stuff, too.

Steve: Yes. Now...

Leo: Your private key. That would be great.

Steve: What's different, though, I mean, and the thing I want to, I mean, yes, that would all be great. But those are all, FIDO and PGP and so forth, are relatively low-bandwidth requirements, much like Stina's one-time password. This struck me as very cool for bulk data encryption, so for like being in your phone and providing encryption operations for your phone and for communications in real time, on the fly. I think that's where this - I really want to say that that's where I think their choice to interface this as an SD interface with the pseudo file I/O, that's where they were aiming was - because even if you had a hardware security module that could hold your keys, unless it can also do bulk encryption, then at least an instance of the key has to come outside so that the processor can do bulk encryption.

And so what's very cool about this is all of that stays inside because it's got the horsepower to do the bulk data encryption, rather than it sort of having to, well, let the external main system processor do the encryption and decryption, in which case there's a key exposed. And so this allows no exposure of your key. And that's certainly what you want. I just - I think it's a nice concept.

Leo: Is it like a TPM?

Steve: Yes, yes. I would say it is. Now, more than a TPM. A TPM can do public key crypto, as can Vault. But a TPM is not bulk data. So this is a super TPM. This is more than

that. And it is of course transportable. The TPM is by design a fixed function on your motherboard that is not transportable. This you're able to, you know, stick into an SD slot, a microSD slot, or SD with an adapter, and move it from system to system. So it could contain, you know, stuff. And we'll have to see as time goes on what is in there. So it's a TPM with a lot of processing power. Whereas a TPM mostly is just doing public key operations and providing that same level of security, but not able to do bulk encryption. Now, Soli. Oh.

Leo: This is still pretty blue sky; right? I mean...

Steve: It is blue sky. But as I said, if I weren't already committed for the next several years of development work...

Leo: Well, good, because in two years this will be ready.

Steve: ...I would be first in line for one of these things. I just think it is so cool. So for people who haven't seen it, what Google designed is - imagine it being done optically first because that's sort of the way to get into this. If you had a little lens looking up at your hand, and seeing your hand doing gestures of various sorts, like clicking your first and second fingers together, or rubbing your first and second fingers, in order to change - and of course tapping your fingers together is pushing a button. Rubbing them is turning a dial. Making a fist and running your thumb along the top of your closed fist is sliding around in 2D as with a mouse. So that's optically.

And it could be done optically, but what Google has done is they've done this with very high-frequency radio. They're using an existing set-aside band, the 60GHz band. And what they've created is a chip which offers super high resolution, super high frame rate, like 10,000 frames of data per second. At 60GHz the wavelength is 5 millimeters, which is a fifth of an inch. So a fifth of an inch is not that much resolution, but they're using doppler. And so that's got infinite resolution.

So in the same way that inertial navigation uses its awareness of rate of change in order to fill in for lack of instantaneous position, by using both a lower resolution instantaneous position and a very careful measurement of rate of change through doppler shift, by bouncing the 60GHz radio off of your water-bearing flesh, which is what bounces it back in, and mixing the outgoing and the incoming signal together, you get a beat frequency which is directly proportional to the rate at which you are moving in a direct line to and from the transmitter. And that's why they have an array.

They have, if you look at pictures of this, they have two sets of two transmitting pads and then a set of four receivers. And so it's because everything is on a straight vector relative to the transmitter and receiver that they spread this out in an array. And that gives them 3D space from what would otherwise be a 2D vector. So the upshot of this is it's super low power, and it isn't optical. It can be underneath a surface. And they've got kind of a cool little logo that, with luck, maybe they'll stick with and we'll see in the future, where they sort of - and anyway, I'm just stunned by this because what this allows is sort of a personal UI interaction which maybe is more like, what, the Microsoft, is it Kinect that - yeah, yeah, Kinect with a "K," you know, where you wave your arms around...

Leo: Right, right, right.

Steve: ...in the living room, and it tries to see you. Here, you're making superfine - yes, and you're showing the video now. For listeners I created - there were three things I wanted people to see. So I created three bit.ly shortcuts. This one is "c." So this is bit.ly/sn-510, which is this episode number, lowercase "c." Everything's lowercase. Bit.ly/sn-510c. That's Apple's produced video showing this technology.

Leo: Apple or Google?

Steve: Oh, god. There I go again. Sorry.

Leo: Okay. No, you never know. It could have been Apple.

Steve: Just keep listening. Keep listening and fix me. Yes, Google's technology for doing this. And, oh, I just think - my belief is they know they've created a cool technology. It can operate from super close, 0.05 meters to 5 meters.

Leo: That's kind of amazing, too. I mean, that's a large range.

Steve: Yes, a hundred-to-one scale. So, I mean, imagine...

Leo: You can make a hell of a theremin out of this; right?

Steve: Well, it could obsolete mice and track pads, so that you now just sort of - you wave your hand over the region of the track pad, or maybe over the keyboard because it could be down in the middle of the keyboard. So now we lose the whole track pad region, no longer needing it. This thing has a 180-degree field of view. So if it's sitting on a flat surface, it creates a spherical region in which it can perceive tiny, tiny motor movements.

Leo: You're making some money today. I'm like, that's the second yabba dabba. Is this harmful, potentially? Is this like microwave radiation?

Steve: Yeah. It's not harmful. It is super low power. I mean, you know, we're bathed in radiation no stronger than that all the time now. Your telephone is far worse for you when you're talking on it near your head than this is.

Leo: Okay.

Steve: So, yes. And the only reason this works is that it's coherent doppler radio. So it knows what it's sending, and it knows what it's receiving, so it's able to filter out all the

other noise. And actually there's not much up in the 60GHz band. Japan uses this for their vehicular radar.

Leo: Oh, really. Oh, that's interesting.

Steve: And it is a designated band for this kind of radar. However, oxygen absorbs 60GHz. So it's strictly range limited. That's why they talk about it going up to 5 meters. Beyond that, they're not generating enough power to get enough reflected power back to their receiver. And it's just - it's not useful for super long range unless you really crank up the power. And here it's just meant to be a really slick UI. Anyway, everybody, please, sn-510c at bit.ly to take a look at this video. Or just put in "Project Soli," S-O-L-I, to Google, and I'm sure that Google will take you to their own YouTube video.

But, wow, it's - I'm just - I mean, again, you could move your hands over your keyboard as part of the UI, where it knows the distance they are. There was an example, for example, of adjusting the time on a watch, where you put your hand near where the crown would be and just make a turning motion with your thumb and first finger, and the hours adjust. Then you move further away to do minutes. And you move back to do hours, and you move further away to do minutes.

Leo: So cool.

Steve: So, I mean, it really works. I'm, you know, I have a strong sense that this is - we're going to see some amazing UI stuff come from this.

Leo: Neat.

Steve: Oh. Okay. So there was another article about supercapacitors. We of course talked about this a long time ago when some company, my memory is saying that they were in Texas, were...

Leo: Oh, yeah.

Steve: ...telling us that they'd solved the problem, and they were going to do supercapacitors.

Leo: Yeah, yeah, yeah.

Steve: Well, there's a joint venture of the Edison Company, which is down here in Southern California - that's our equivalent of PG&E up in Northern California - and Sun Vault Energy. And their press release from the 6th, so, wait, no, 5/6, can't be that. So from the 5th. Maybe they predated it. Or, no, it might be May. I'm sorry, it was May. Their press release disclosed the fact, claimed that they had a 10,000 Farad capacitor. So that's big. And what they didn't say was...

Leo: How big is it?

Steve: Well, I mean, the idea is the closer you can get the two plates, the positive and negative plate of the capacitor, the greater the capacity for that to store electrostatic charge. But the greater the problem with breakdown, that is, with the so-called dielectric, which is the thing, the substance that separates the positive and negative plates, you need it not to short out. That would be very bad. So they don't ever, I couldn't find anywhere them talking about the breakdown voltage of their 10,000 Farad capacitor. And that's a crucial missing piece of information because, while 10,000 Farads is a lot of capacity, if you can only charge it to a volt, and if you went beyond that it would short out, that may not be much use. But if you can charge it to a thousand volts, then that starts to get really interesting.

So as our listeners know, this is interesting because it's one of the challengers for a means, I mean, it's an interesting challenger for a means of providing mode of power for electric vehicles. You know, we have petrochemical power, which does not combust very easily, I mean, yes, you know, in an accident, if the gas leaks and there's a fire or a spark, you can have a problem. But in general, gasoline is pretty safe. Of course it's nonrenewable, but it is fast to refill, so it has those advantages.

Then we have electrochemical, which is battery storage. And the problems there is it's got a limited, they have a limited lifetime in terms of cycles. You know, gasoline, you can fill your tank as much as you want, as long as the gas lasts. But batteries do die after both cycle times and just age. They have noxious chemistries. Lithium is a volatile chemical that you don't want - you want to do something with responsible recycling. And it's very slow to refill. You know, as we know, it takes time for our devices to charge.

Then there's electromechanical, which has been experimented with, and typically in the form of a flywheel. And the problem is they are extremely dangerous in a crash. You end up with this - basically all of the energy that has been stored in this spinning whirling dervish has a chance to escape from containment and just shred everything in the neighborhood. So it is renewable, and it can be fast to spin up. But it's just too dangerous.

So Ben Rosen, who was a major venture capitalist in the early days of the PC industry, spent a lot of time working on a startup that was trying to do a vacuum-contained, high-speed flywheel and some neat other ancillary technology that they developed in order to support it, but they ended up giving up. I mean, they had, like, a crash wall between it and the passenger compartment because they understood that if, you know, it could not get loose. So it's like...

Leo: If you think about it, that's a fundamental problem with anything that can store enough power to move a three-ton vehicle in a small enough size. There's going to be a lot of energy somewhere.

Steve: Yes. Exactly. There are some...

Leo: Lithium ion batteries are explosive, too.

Steve: Yeah, and a supercapacitor, it's, I mean, that energy is there. It's there in the form of a whole lot of very high voltage. And you'd want it to, like, sort of implode. You'd want it to just short itself out instead of...

Leo: Right, right. Yeah, don't explode, implode, yeah.

Steve: Yeah. Or don't run the current through the car on the way to shorting yourself out.

Leo: Yes, that's right.

Steve: Keep it in the family. You know, keep it inside. So anyway, it'll be interesting to see how this evolves. But right now supercapacitors are in use in a number of electric vehicles. They use them for the short-cycle regenerative process, where you put your foot on the brakes, and that braking energy which is recaptured by the wheel motors does not go into batteries. They go into a supercapacitor. Because that short cycle, it wants to take the energy very fast and then dump it out very fast. And batteries, you don't want to be pumping in and out of batteries like that. You want that to provide more of the long-term drive current, not the short-term current. So supercapacitors are already finding a role, but not yet as the primary store of energy for vehicles.

Leo: Yeah.

Steve: Okay. Now, this is "a." I told you I had three different pieces of media. Leo, you might want to play this while I talk about it.

Leo: Okay.

Steve: This is bit.ly/sn-510a, just a very fun video I recommend to our audience. I tweeted it, got a lot of neat feedback. Some guy asked the question, he said, "I've spent a lifetime riding my bicycle. How deeply wired into my brain are the reflexes, essentially, that I've developed?" He had an engineer add a single set of gearing to the throat of the bicycle so that the handlebars act in reverse. So when you turn the handlebars to the left, the front wheel goes the other direction.

Leo: Oh, this guy's great. This is the science guy. I love him.

Steve: Yes.

Leo: Yeah.

Steve: He does a great job.

Leo: "Smarter Every Day" is the name of his podcast.

Steve: Right, right. So anyway, I commend our listeners to it. What he found was that, first of all, he could not ride the bike. His brain could not override the instinct. And here in the video he's showing the mechanical engineer, who said, "I'm not getting on that thing." But he said, "Okay, you know, I'm going to try to ride it." And here, I mean, he's not spoofing this. It is that difficult.

Leo: It's the gear system.

Steve: All it is.

Leo: But you know, anybody who's ever had their joystick reversed in a flight sim or a videogame knows it's weird. And, you know, pilots are used to doing it in reverse like this, but it takes a while to get your brain used to it. Oh, I, oh, you're - oh, don't ride - no, no, what are you - oh. This is, by the way, this show is so great. You've got to watch the one where he shows the Archer's Paradox. It's called "Smarter Every Day." I shouldn't tell people about other podcasts, but he does only a couple a month. He's on Patreon, too. And these are just hysterical. This guy [Destin] is really clever. Really clever, yeah.

Steve: So what he found was that it took him eight months of daily effort...

Leo: And this is why he only does two shows a month, I've got to tell you. This is a lot of work.

Steve: Eight months in order to relearn how to ride this bike. Then he was unable to ride a normal one. And it did not take him that much longer to come out of it. He shows all of this on the video. So bit.ly/sn-510a, really recommend it. He does a great job. He, like, tries to reverse his hands on the handlebars and so, like, to counteract that effort. He shows other people trying to do it. Anyway, it's just great.

Leo: It just shows, you know, we really - these brain pathways are really not conscious. You can't just override them.

Steve: Oh, and what was interesting is his son was able to unlearn bike riding much faster. So somebody much younger has remained more plastic.

Leo: That makes sense, yeah.

Steve: Yeah.

Leo: Wow. Really, really great stuff.

Steve: Really neat.

Leo: Smarter Every Day, yeah.

Steve: Okay. Next up.

Leo: That's one, okay.

Steve: Yeah, that's 510a. We already did "c." Here's "b." There is a series that I was very impressed by, coming out on USA Networks beginning, I want to say, later this month. I didn't put the note in my - I didn't have the date. I think it's June 26th. It's called "Mr. Robot," which is a bad name for what this is. But it is a very well done cyber hacking series with sort of a disaffected, very skilled hacker who works at a security firm by day and hacks people by night. And there's much more to the plot. The point is the entire premiere episode, full-length episode, is released, formally released by USA Networks, and it's everywhere. It's on YouTube. It's on...

Leo: Yeah, it's great, yeah.

Steve: ...VUDU.

Leo: But have you seen the website? Have you seen whoismrrobot.com?

Steve: Yeah, Christian Slater.

Leo: No, no, no. Watch this. Go to whoismrrobot.com.

Steve: Okay.

Leo: And it launches a Linux. It's a hack. And I saw this before I'd ever heard of the show. And it says, "Hello, Friend. If you've come for a reason, you may not be able to explain it yet. But there's part of you that's exhausted with this world." It's so cool. It's the setup for the show.

Steve: Nice. Well, the show...

Leo: And so there's commands. So I'm going to type "inform," and then it gives you

some information. It's really - this is a beautiful - whoismrrobot.com. One of the best promo sites I've ever seen for a TV show. And it gives you some hope that there's actually some computer - somebody behind this is intelligent enough.

Steve: Well, I was going to say, Leo, the whole first episode is there. I've watched it. I was blown away. They're accurately talking about Tor and about IT, about proxies.

Leo: Whoever did this knows what's going on.

Steve: And, oh, no, it's serious technology, but also very approachable. So definitely of interest to our listeners. You can find it anywhere. I have a link to it. Again, it's sn-510b under bit.ly because I'd really commend our listeners. So again, they'll start airing the series at the end of this month, but the entire premiere episode you can get. And I can't imagine anyone listening to this podcast who won't want to watch it. And it's available everywhere.

Leo: [Laughing] "If you're ready to join me, enter your email address."

Steve: And the tech, my jaw just dropped open in the first five minutes. It's like, oh, my lord. I couldn't believe they were getting it right. So, you know, a DDoS attack of a certain size and...

Leo: Yeah. Only a matter of time, really, if you think about it, that the people who know how this stuff works would get a chance to make an actual television show, thank goodness.

Steve: Yeah.

Leo: So if you search for the "Mr. Robot" official trailer, there's a link right at the beginning to the rest of the show, the first episode. Yeah, I'll be watching this. This looks really good.

[Clip] MAN: And now I think they're following me. Employee No. ER280652.

Leo: Makes you want to be a hacker.

[Clip] MAN: Just a regular cybersecurity engineer. But I'm a vigilante hacker by night.

Leo: You could see this is going to be the kind of show that our listeners will want to watch.

Steve: Yes, yes, yes, yes.

Leo: Okay.

Steve: So, next. I watched the other day a sci-fi time travel movie that did not get well reviewed, but I thought it was pretty good. It was released last year, in 2014, called "Project Almanac." And it's high school kids with an unsteady cam who build a time machine. What could go wrong?

Leo: Okay.

Steve: So for what it's worth, it's still so new, I couldn't find it for free anywhere. But so, you know, if our listeners want to track it down, "Project Almanac," I thought it was definitely worth the time. I'll just mention that "Halt and Catch Fire" has just started a second season. The first episode of Season 2 began to air this Sunday. And, you know, I was not a huge fan of it. But it was entertaining and engaging, and all the same characters are back, and they're off on a new trajectory. So we'll see what happens for a second season. But for anyone who didn't catch the return of it, I wanted to let everybody know.

Okay. Now, this is going to seem a little weird. But there's a series I've mentioned before on FX called "The Strain," which is a whole new take on vampires. The first season started last summer, on July 13th, for 13 episodes. And I was completely entertained. The second season begins on July 12th for another 13 episodes. So for what it's worth, if you missed the first season, and you think that might sound interesting, I know it's not going to be for everybody, but very well done. Is it Benicio del Toro, or, no Guillermo del Toro.

Leo: Guillermo del Toro, yeah.

Steve: Yeah. He's behind it. And it was great. So I'm delighted that we're going to have a second season, and I just wanted to pass it on. And people have asked me about "Orphan Black," which has now had several episodes of Season 3. And for me, it went off the rails. I watched the first couple, and I thought, eh. You know, we all remember when "Battlestar Galactica" sort of...

Leo: Yeah.

Steve: ...went, lost it. I think the problem is some of these great ideas, they've only just got so much material.

Leo: Right, right.

Steve: And then they're done. And so, but they have a hit series, and they want to keep it going, so they make the writers keep producing episodes when they should have just

said, okay, we've told the story.

Leo: That's true for all of us. It's hard to know when to quit. You just don't know.

Steve: Know when to fold 'em.

Leo: Yeah.

Steve: And I did hear you mention yesterday on iOS Today, but you never got around to talking about it, but at least you said the word, and I said, "Oh, we got Leo hooked." And that is "Blockwick."

Leo: I was going to make it my app cap. I'll do it next week. I'm stuck.

Steve: Yeah. Oh, you are.

Leo: I got stuck, yeah. You're too smart for me.

Steve: I'm stuck actually on the third chapter somewhere with a bunch of yellow things down both sides and a big square one in the middle, and I'm just - yeah.

Leo: I'm stuck, I think, on 219, I think is the one I'm stuck on. It's just - you can't, there's no way you can get that thing up to there to get to this thing. I can join those things, but I can't get this thing. It's very challenging. I like it a lot.

Steve: Yeah, I do. As I said last week, not all puzzles are good. There are some that are just sort of annoying and frustrating or don't have a good model. This one is just the right amount of degrees of freedom where, you know, there are, for example, many solutions to these because the goal is to pull like-colored tiles together. And you can decide where you want to aggregate them. So anyway, again, Blockwick 101 is free. Unfortunately, it's only iOS.

Leo: That's the one I bought, 101. I paid five bucks for it last week.

Steve: No, no, 101 is free. But Blockwick 2, there is a bundle of Blockwick and Blockwick 2 that I think is $5. But Blockwick by itself is $3. So...

Leo: Well, so by the way, there's a YouTube video solution for all of the levels. I watched the solution. I still can't do it.

Steve: Oh.

Leo: That's a lot of moves.

Steve: Yeah, you just sort of - you just want to relax and not be in a big hurry and so forth. Now, I have my Mac here, which has gone to sleep on me now - there - because I wanted to show a demo of SQRL logging in.

Leo: Oh. What?

Steve: But it's sort of hard to do this on the camera like this, and I don't have my lovely assistant with me. So I thought instead I'll log onto your computer using SQRL, Leo.

Leo: What? What?

Steve: So open your computer.

Leo: Okay.

Steve: Go to GRC.com.

Leo: Oh, this is making me nervous here. All right. GRC, doesn't matter what I use; right? Like I can use Chrome or anything else; right?

Steve: Use whatever you want.

Leo: Okay. Let's go to GRC.com. All right.

Steve: Slash...

Leo: Oh.

Steve: Slash, oh, sorry, /sqrl/demo.htm.

Leo: Okay. Slash sqrl, S-Q-R-L.

Steve: SQRL.

Leo: Slash demo.

Steve: Slash demo.htm.

Leo: Oh, okay. Still uses those old htm [crosstalk].

Steve: That's right. Hit Enter.

Leo: Hit Enter, all right.

Steve: Okay. So now you're looking at SQRL's demonstration. And so you...

Leo: Yeah. Proceed, proceed.

Steve: Yup. Do that.

Leo: Okay. Now what do I do?

Steve: Okay. So now we're looking at what any website on the Internet might show you when you are logging in. I just took a picture of that QR code, and now you are logged in.

Leo: What? Knock it off.

Steve: That's what this is about.

Leo: [Stammering]

Steve: Now, several things. Notice that...

Leo: What the hell happened there?

Steve: You didn't touch your computer.

Leo: No, I did not.

Steve: I didn't touch your computer. No authentication information went over your wires. So that if there was a keystroke logger in your machine, if somebody was watching, monitoring your traffic, you're just suddenly logged in. And the other cool thing about this, I just - this sort of occurred to me as a fun demo. As a parent, how many times have you needed either Abby or Henry to get, like, brief access to some Internet

account of yours?

Leo: Yeah, yeah, yeah, yeah. All the time, yeah.

Steve: Yeah. So I know, it happens all the time. So what I just did was essentially gave you access to one of my logons.

Leo: Can I get a SQRL on my door lock?

Steve: Many people have asked.

Leo: That was awesome.

Steve: There'll be lots of applications for this. This is a - there's a SQRL client which has been written by, he's still in the process of working on it, Jeff Arthur in the U.K. did the SQRL client for iOS. So I have it running, both on the iPhone 5 and 6. And so this demonstrates the optical QR login. And so normally you would do this with your phone to your computer or a friend's computer. In the example that I gave when I was speaking at the DigiCert conference, I talked about being in a hotel and not wanting to log into their business services computer because anything, I mean, anything could have been sitting there capturing my keystrokes.

Once SQRL happens, the Southwest Airlines just puts up that little QR code next to the username and password; and any SQRL user simply uses their smartphone to scan the QR code, and they're logged in, entering no credentials into that machine. So I've been talking about it for a year and a half now. Our listeners have been very patient. Lord knows SpinRite people have been very patient, waiting for me to finish this and get back to SpinRite. So I wanted to demonstrate that it is in fact coming alive and working. And, you know, all of the - it all works.

Leo: I have no idea what just happened.

Steve: Well, I'm going to fly up, and you and I will do the full walk-through demo.

Leo: Good. Let's have a special.

Steve: Yes, in order to explain it all.

Leo: And while you're here you can help me solve this level of this horrible, horrible - does this ring a bell?

Steve: Oh, yeah, I remember that one. Yeah, that's the end of Chapter 2.

Leo: Yeah, there's no way to get that up to here to get - I can get these around to there, but - anyway. Drives me crazy. This is...

Steve: Yeah, you've got to bring the red guys down through that one below the...

Leo: The red guys I can do.

Steve: Yeah.

Leo: But there's no way to get this blue guy...

Steve: Ah. There is a problem. Sometimes you just need to have - remember that they only have to touch. They don't have to be in the same area.

Leo: No, I figure I could get him there and him there.

Steve: That's exactly right.

Leo: So I've got to get - but I...

Steve: Yup. You've got to shuffle some things around first.

Leo: Oh, really. You think? Geez. It's horrible. I kill you. I kill you.

Steve: I do wish they would make this for Android because I really - I understand we have lots of Android users. And only, unfortunately...

Leo: Yeah, they're feeling left out, I'm sorry to say.

Steve: Yeah, unfortunately they only have Blockwick 2 for Android. And it's just not the same. They used a whole bunch of gimmicks. And they have an extreme 3D perspective, sort of pseudo 3D, that I find is annoying more than helpful.

Leo: Yeah.

Steve: Here you're looking directly down on it.

Leo: No, this is fine. I can see what's going on, yeah.

Steve: Yeah.

Leo: See, so I've - it's easy to get these red boys together.

Steve: Yeah, there you go.

Leo: That's no trouble at all. It's...

Steve: Okay, so now what you need to do, you need to get the black ones behind the big blue one up there.

Leo: Get them behind; right?

Steve: One of the ways to think about this...

Leo: But how do you get them behind if you can't...

Steve: Yeah, well, see, you can slide them...

Leo: I can't move this one hole there.

Steve: But you can slide it up. I'm pointing at yours. That won't work.

Leo: Yeah.

Steve: Slide it up where the thing is below the blue one, where the red is. Anyway. I know you're going to get it.

Leo: Oh, yeah, but, no, but then, but it's these horizontal ones can never be out of the way. That's the problem.

Steve: Correct. So you just have to pull them down below.

Leo: Below what? I - never mind. You understand my problem. This isn't getting out of the way. This, I mean...

Steve: Yeah, you can do it.

Leo: I know you can do it. I saw, actually, that's what's really frustrating. I watched it on YouTube.

Steve: Ah, the video, right.

Leo: I know you can do it. And I still can't figure it out. This show makes me feel like an idiot, by the way. Thank you, Steve.

Steve: Okay. So, and I'll just mention that that QR code that came up, every time the system displays it, it's different. So, and it's based on a counter and a bunch of other information, which are encrypted. So that QR code will never, ever repeat. So there's no replay attack possible. And yet at the same time the server knows, when my phone authenticated, which browser session that QR code came from. And that's what logged you on. So anyway, we'll go over all this once we get it finished. But it is, it's coming to life. And thanks to Jeff Arthur for authoring a beautiful iOS client. We're all approaching the finish line.

Speaking of SpinRite, I did get a nice note from Kyle Schmidt in Cheyenne, Wyoming. He said: "Just another SpinRite success story to share." He said: "I have a VAIO Win7 Pro laptop that I had to purchase while traveling on business through Seoul Incheon Airport at a duty-free shop." And he says in parens: "(Laptop that I was traveling with crashed)." I think we'll know why here in a minute. Then he says: "About a month ago, I was carrying same and dropped it while it was on. And even though it has a shock-protected hard disk drive, the results were predictable.

"After numerous unsuccessful attempts at Windows repair, et cetera, I remembered SpinRite from GRC. And even though it took almost a day and a half to totally rejuvenate the very troubled hard disk drive, lo and behold, it once again boots up and is usable. There were sectors that are still unrecoverable, but SpinRite was able to," and he has in quotes, "'raise it from the dead.' Thanks for continuing to offer the utility. I can personally attest to the fact that," and he has in caps, "IT WORKS AS PROMISED. Regards, Kyle Schmidt, Cheyenne, Wyoming." And Kyle, thanks for sharing your story.

Leo: Very nice.

Steve: SpinRite does indeed work. SQRL does, too, and I'll be getting back to SpinRite as soon as...

Leo: That was amazing. I just feel flabbergasted. Gob-smacked. Did you take a picture of the QR code on my screen?

Steve: Yeah.

Leo: Ah.

Steve: You put your screen in the feed. And so I let the phone...

Leo: Oh, okay.

Steve: ...see your QR code. And then my phone - and, see, the QR code contains the URL for the demo. So the phone contacted GRC, and it said, "This is Steve. I'm proving it by signing this QR code, and you can log on the person who you gave the QR code to."

Leo: Well, that's a goldarn miracle. I don't know how you did that.

Steve: But notice that, if Henry needed to use, to get onto one of your accounts, all he would have to do is arrange to show you the QR code which is being shown. You let your phone see that, and then he's logged in without...

Leo: So he could turn on the, I don't know, FaceTime, and use the camera on his phone to show me that code. And I could see it, and I would turn on my SQRL program.

Steve: Yup.

Leo: See the QR code he's sending me via FaceTime, and the door would unlock, and he could go in the house. Which he is right now, riding my Segways.

Steve: Or...

Leo: But I had to give him a key.

Steve: Or he would have access to a website where otherwise you would have to give him your username and password.

Leo: Password. Happens all the time.

Steve: No doubt you've had to do that with the kids.

Leo: All the time.

Steve: And so the beauty of this is it allows you to, at distance, one-time login, with

divulging no credentials to the person whom you're allowing to log in as you.

Leo: QR codes are pretty robust. You don't need great video.

Steve: Oh, in fact, it was blurry. It was blurry here, and I didn't know if it was going to work. They're robust, and they have ECC, error correction built in. So, and a variable level of redundancy.

Leo: There's a lot of redundancy. Yeah.

Steve: Yes.

Leo: There's a lot of redundancy in them. Well, golly. I'll never understand you wizards, you scientists. I don't get it at all.

Steve: One thing I forgot, and then we'll get into our Q&A...

Leo: Sure.

Steve: ...is I saw a tweet from the EFF that I just - I had to shake my head at. They tweeted that they have been - they, the EFF - has been sued for defamation by the patent attorney behind their April Stupid Patent of the Month blog posting.

Leo: How dare you say I'm stupid?

Steve: So, and get this. I thought, okay, what was it? So in April their Stupid Patent of the Month says, they say: "Imagine you're on your way to deliver a case of beer to a party. Before you get there, your boss sends you a text, and the text reads, 'They want two cases now.' You read the text while driving." And they say, parens, "(Don't do that.)" Then they said, "So you deliver an extra case when you arrive. Having successfully completed that task, you leave for your next delivery. Congratulations. You might get sued by the owner of April's Stupid Patent of the Month. This month's winner, U.S. Patent No. 9,013,334" - which they refer to shorthand as the "334 patent" - "has the prosaic title, 'Notification systems and methods that permit change of quantity for delivery and/or pickup of goods and/or services.'"

Leo: Yeah.

Steve: "It issued just last week, on April 21st. As its title suggests, the patent claims 'a method of updating delivery information.' It belongs to Eclipse IP," as in intellectual property, "LLC, one of the most litigious patent trolls in the country. Eclipse belongs to an elite group of trolls," and blah blah blah. Anyway, they talk about how that this was their highlighted patent. And now the attorneys have sued the EFF for defamation. The EFF's

attorney, of course, said, uh, let's take a look at what we said. Everything is factual. And where it's opinion, we're protected by the Constitution.

Leo: Right.

Steve: So go away.

Leo: It's a bogus - yeah.

Steve: Oh. But, my lord. And then, see, the problem is how could the Patent Office issue a patent for receiving a text message that tells you to change the quantity of items in an order?

Leo: And maybe that'll make these guys feel better. The EFF's not calling the patent trolls stupid. No, they're smart. They patented it. It's the Patent Office that's stupid because they gave them the patent. But the way the Patent Office works, and I think this will change, is the...

Steve: Oh, please.

Leo: I hope it does.

Steve: Please. Oh.

Leo: First of all, software patents are a terrible idea.

Steve: Yup.

Leo: But the presumption is it's a good patent. They don't do a lot of work on the prior art. They figure, well, if it's not a good patent, the courts will work it out. Because they don't...

Steve: And actually it turns out that this was a set of 20. And a federal court already overturned a bunch of them in this same group. And yet the Patent Office still issued this patent. I mean, this is trouble caused by the Patent Office that is just, I mean, a patent is supposed to be non-obvious to somebody skilled in the art. How is this a non-obvious use of a text message?

Leo: Yeah. But that's the thing, is I think the way it's set up, the way it's constituted right now is not good.

Steve: No.

Leo: Well, you know what, I give a significant amount of money every month to the EFF. I feel like they're - there's a couple of tech charities that I give to, and I encourage people to give to. I think I give a hundred bucks a months to the EFF and a hundred bucks a month to the Wikimedia Foundation. And I just feel like those two are the best of what the Internet has to offer.

Steve: Yup.

Leo: So I'm glad to be kind of a sustaining donor to both of those. You know, there are plenty other charities I give to, but those are the tech charities, I think, are really important to support. Wikipedia because they never took ads. And god bless them.

Steve: Nope. And thank goodness. And any time he puts up a banner saying he needs money, I say, hey, how many, I mean, I was there today, looking up some stuff.

Leo: Every day I use it.

Steve: I'm there all - yes.

Leo: You know, I should give them more money, frankly, because I use it every day. And it's a great resource. And we use the EFF like crazy. The EFF saved podcasting.

Steve: Yes. I meant to remind our listeners that, you know, we just got, we the industry, a great judgment as a consequence of them saying, no, no, no, no, we're going to challenge this. And the problem is small people can't challenge them.

Leo: No.

Steve: It is incredibly expensive in order to fight patents. And this is the real problem is the actions of the Patent Office toss this into the private sector, and then we're stuck litigating, and no litigation is inexpensive.

Leo: That has to change, frankly. That has to change. Let's go to our questions. Are you ready?

Steve: Absolutely.

Leo: Are you ready, Stevie? Here they go. The listener-driven potpourri starts with

Stephen_Sal on the Twitter, Stephen Salvatore. Steve, could you explain briefly on Security Now! about what Win10 is doing to deviate you from your normal recalcitrant upgrade path? You usually wait for a long time.

Steve: Well, do you think? I'm still on XP, Leo.

Leo: Yeah, yeah. There you go.

Steve: Yeah. So, okay. Mostly, to be honest, it's the association between the server side, that is, the Microsoft Windows Server platforms and the desktop, because I am a Windows developer. All of my code, for example, the SQRL login demo, is all written in assembly language for the Windows API on my Windows Server at Level 3. So I went to Windows Server 2008R2 because I was on Windows Server 2000, but obviously they stopped updating it forever ago. I didn't care because I was responsible for my own security. But it didn't know about any of the SSL improvements over the years. And so I moved to Windows Server 2008, and I got TLS 1.0, 1.1, and 1.2. So now I'm able to play ball with everybody else.

So I'm looking at this, and, I mean, I'm not going to jump immediately. But I don't think I'll go to 7. I was planning to go to 7 until I see that Microsoft, it looks like they've done a good thing with Win10. And I want to have a desktop and a server which are synchronized. It's just easier. For example, the same version of IIS, their web server, I can run on my desktop and on the GRC server at Level 3. So mostly that's what's pulling me. Otherwise I think I'd probably be on 7. But I think I'm willing to go 10. We'll see. But not immediately.

Leo: Yeah. I mean, that's the main point to be made, really, with upgrading, is that you get more modern protocols. The point you've always made, which is absolutely true, too, is it hasn't been banged on. It hasn't been tested in the real world, so there may be security issues, and there will be security issues, that we just haven't discovered yet.

Steve: And the other thing is Microsoft has promised that this is the last time they're going to do a major change. From now on, they're going to do incremental fixes. And I have a huge investment. Everyone who, like, sets up a new computer, you lose a week just reinstalling things and customizing. And so, I mean, I would be on 7 already, because I like it, I have it on many other systems, but it would take me so long to move my whole world over to it that I'm just - it's inertia. I'm just waiting. And so I figure, hey, if I'm someday going to be on Win10, and Win10 is the last time I ever have to do this, why stop in Windows 7 and get it working, only to have to go to Windows 10 at some point in the future.

Leo: Right.

Steve: I'll see how it goes, wait till the dust settles. I mean, I have a strong security perimeter already. So I'm probably going to be okay. But I'm excited. The idea that they fixed the 8 disastrous UI is all I needed.

Leo: Yes. I think they did. Yeah. I think even 8.1 is a big improvement. But I've played with 10 for some time now, and I kind of like it.

Steve: Good.

Leo: Bob Covello, @BobCovello on the Twitter: Steve, do you think an Altoids box lined with a static prevention bag - one of those mylar bags - would stop the keyless entry hack? And he put a Twitter pic up on there.

Steve: Yeah, of his putting up that mylar bag.

Leo: You know, when I got the FasTrak for going through the toll, it comes in a mylar bag. And they say if you don't want to be charged, put your FasTrak in the bag before you go through the toll. So presumably that's the kind of thing it protects against; right?

Steve: Well, except that what he's talking about is a static prevention bag.

Leo: Oh, that's different?

Steve: And they do not block radio.

Leo: Oh, okay.

Steve: What you need is essentially a zero-resistance container so that it shorts out the radio waves.

Leo: Can I show you my baguette? You were talking about your baguette? I found one.

Steve: Oh, yeah, yeah.

Leo: This came from ScotteVest, and they sell this on their site. And you see this material inside?

Steve: Yup.

Leo: It's a metallic material. So I'm guessing this is like a Faraday cage; right?

Steve: It is.

Leo: And then I put my fob in there so that nobody can stand - because I realized I park in the garage next door all the time, and I just fear that that's a little too close for comfort. So...

Steve: Nice, nice.

Leo: ...it's right there. And it's a cute bag. It's like, you know, it's got Velcro on it. You can squinch it. That's my baguette.

Steve: Yeah, it's very much like my little baguette that I got for $7 on Amazon.

Leo: Yeah.

Steve: Anyway, many people have asked about static prevention bags. They don't work because they are a high resistance. They're not zero ohms, the way an Altoids box is, nor are they infinite the way a plastic bag is. A plastic bag creates static, very much like the old experiment in high school of running a hard rubber comb through your hair. You generate a lot of static because there's nowhere for the electrostatic charge to flow, so it can build up. But if there's any conductivity, the charge will bleed off. So the static, the antistatic bags are a high, but non-infinite, resistance. Yet they're high enough resistance that radio sees them as transparent and goes right through them. So for those who - many people asked about antistatic bags. And I just wanted to say, unfortunately, that will not help. And I have heard that Altoids isn't working for some people. So it needs to be a sealed box. Or, as you found, a little bag does the job.

Leo: This one works great.

Steve: And so you have verified that you can walk up to your car...

Leo: Yup.

Steve: ...with your key in that bag...

Leo: Yup.

Steve: ...and it doesn't know you're there.

Leo: It doesn't know I'm there. Yup.

Steve: Nice, nice. And, yeah, good.

Leo: By the way, the Senate has approved the bill to reform the NSA domestic surveillance programs.

Steve: Yup.

Leo: That just happened a few minutes ago. The vote was 67 to 32.

Steve: Did they get any amendments on them? Probably not, if they passed it through that fast.

Leo: Let me check. Yeah, because that was one way that Mitch McConnell wanted to modify it so that...

Steve: Right, right.

Leo: Let's see. I'm looking at the CNN report. I don't see what - if they've modified anything.

Steve: So the way things were under 215 is that the NSA received all of the metadata. The way things will be now, under the so-called USA Freedom Act, is that the telco providers are being asked to keep that data and then provide it as needed to approved NSA requests. Those who argue against this being strong enough, who say that it's not enough, say the problem is - I thought this was really interesting. The problem is the law does not require telcos to retain the data. So they could start using their non-retention as a commercial selling benefit. I thought that was, I mean, so the idea being - and then this really demonstrates that there's an awareness that the public does not want to have this dossier built on who and when they call, even at the metadata level.

The fear is that phone companies will be saying, we're only retaining your data for a week, or we eliminate it as soon as we send out your monthly bill, or who knows what. But they would be seeing it, they'd be using non-retention as a competitive advantage. So the way the law is, that's what the USA Freedom Act does is it just says, instead of it all streaming to the NSA's massive database in Utah, the individual telephone companies, who are already retaining it for some length of time for business purposes, would make that available as required.

Leo: It's a minor improvement, but it's better than nothing. And apparently...

Steve: I sat and watched C-SPAN2, a.k.a. paint drying, on Sunday. And Rand Paul was of course there, and Ron Wyden was making, you know, they both made their points and basically ran out the clock and prevented there from being a vote on just the simple renewal of the Patriot Act. So now we have a modified one. Which everyone knew this was what was going to happen.

Leo: Looks like no amendments managed to make it through. There was, you know, the House said, if you amend it, of course, it's going to back to the House now for reconciliation, and it's going to be a poison pill. It's going to kill it. So apparently did because the CNN report says the bill now heads to the White House. So that's good news.

Steve: Oh, and I don't know if you saw, it was in the news just today, independent security checks of the effectiveness of the TSA agents, they failed all but three of 70-some tests.

Leo: Oh, I saw that, 95%.

Steve: Yes. I mean, and we're talking guns successfully brought through the scanner. Turns out if you put them on your hip, on your side, the scanner won't see it.

Leo: Oh, great.

Steve: And it's like, okay. Well, now everybody knows that.

Leo: This confirms what Bruce Schneier said, which is that it's basically...

Steve: Theater. Theater.

Leo: ...security theater. And now we know that the actors are not very good.

Steve: I tweeted yesterday, it was, I'm trying to think what the site was. Anyway, it's in my Twitter feed, a link to a lengthy multipage horrifying story written by a TSA agent about his fellow TSA agents laughing at the images of people's bodies that they're seeing in the I.O. closet. And, you know, and how in some cases couples who were dating, who were dating TSA agents, would go in together and get their jollies. So, wow, very damaging. And, you know, annoying. But I'm TSA PRE, so I'm now, where it's supported, I don't have to do that. I recommend that to everybody. Get preapproved.

Leo: Question 3, Nathan in Kansas discovers a worrisome approach to ad blocking: I'm a computer technician. I was installing a new Cisco RV110W VPN firewall router. Because the business's network had been expanded, the old router was locking up due to traffic load. I first updated the firmware, disabled insecure features, and set up wireless appropriately. A quick test of the firewall at ShieldsUP! showed all was secure from the outside. Now, being security conscious, as always, I disabled the VPN passthrough on the router since no one was using a VPN. I guess that would be a VPN inside the office; right?

Steve: Right.

Leo: The next day I received a phone call from the customer wondering why his Apple smartphone will no longer connect to the Internet. His phone showed that the wireless was connected and had a valid IP address. So I had him check the other network settings on the phone, and the phone had a VPN connection. I asked if he was paying for a VPN service. He wasn't. I had him try to disable the VPN connection. He couldn't get it to disable. So I returned the next day, by which time he figured out it was a free app to block Internet ads. I recommended that he ignore the ads and not use that app. I explained the app was taking all his smartphone's Internet traffic and routing it through some other distant network. But he wanted things to work the way they did before. So I reenabled the new router's VPN passthrough to allow the free ad blocker to function. I wonder, some days, is it even worth the trouble to try to secure things? <Sigh> I enjoy the podcast. Thanks for the information every week.

Steve: I just wanted to share that. I thought, oh, my lord. So there's some app that is offering ad blocking, and they do it by automatically reconfiguring your phone to reroute all of your traffic to their VPN endpoint so that they can do filtering, and then your traffic goes out over the Internet.

Leo: Yeah. But that makes sense because otherwise it couldn't block ads on SSL; right?

Steve: No, because the SSL connection would still go through the tunnel. So they can't block ads on SSL unless they also put a certificate in your phone.

Leo: Well, that's what I'm saying. Wouldn't an ad blocker need to do that to block ads on SSL?

Steve: Yes, to be completely effective.

Leo: Right. That's why we're going SSL, so you can't block our ads. No, we're going SSL because Google kind of is making us.

Steve: Yeah. It's making the world.

Leo: Yeah. But Steve, that's going to make ad blockers ineffective. Won't it?

Steve: Correct. Correct. Well, no. Ad blockers that are in your browser see the post-decrypted data.

Leo: Oh, yeah, yeah, yeah, yeah. Oh, of course. But the ones that work by...

Steve: Intercepting.

Leo: ...intercepting, huh, which this one obviously did.

Steve: Yeah. Yeah, I had enough things to talk about that I didn't get to it, but there's a fabulous report that I will share next week on some statistics that came from the Mozilla tracking protection feature. We talked about it quite a while ago. It's available in the about:config for Firefox. If you go about:config, hit Enter, you know, in the URL, and then put "tracking" in the little search bar, it eliminates the ridiculously long list to six, and you can manually turn it on. They haven't yet surfaced it in the normal configuration UI, so you have to go through all that while it's sort of in this stage. But the statistics in this research are amazing. They found some sites that loaded 150 tracking elements that had nothing to do with the site contents. And in some cases they were loading JavaScript libraries to support a few lines of JavaScript code, all just being sucked in, and of course using up bandwidth and slowing down the display of pages. It feels like it's getting out of control and that we're going to have to strike some new balance here pretty soon.

Leo: Yikes, shmikes.

Steve: Yeah.

Leo: Yikes, shmikes, double-mike pikes. That's what my mom used to say. Did your mom use to say that?

Steve: I don't think I've ever heard her say that.

Leo: Think she was...

Steve: You know, my grandfather said, "I opened the window, and influenza."

Leo: Yes.

Steve: So Mom could certainly handle that, if it came to it.

Leo: Or when love - let's see, what was it? When romance comes in the door, love goes innuendo?

Steve: Or it the rain keeps up, it won't come down.

Leo: That's right.

Steve: That's right.

Leo: M. Weber in Southern California - those are Dad jokes. M. Weber in Southern California wonders about juggling NoScript: I've been a NoScript user for a long time, M. Weber writes. It seems as though sites are linking to more and more scripts from other sites. We do. It's analytics. We do a lot of it. As the use of cloud services and content delivery networks grows, it's probably not a mystery why. But it makes it really hard for the security-conscious user to know what to allow and what to block. I know there's no easy answer on this, but interested to hear your thoughts on, one, guidelines for decision-making as a user; and, two, what owners and developers of websites can do to help, at least the ones who respect my right to security and privacy.

Steve: So there's really no pat answer for this. I run with NoScript blocking by default and no notifications. Actually, I'll change that. There's an audible, you can have a little [untranscribable] sort of sound that it makes, and I do that just to remind me that, oh, yeah, it's blocked some stuff. I mean, I never don't hear it, so it's not surprising. But I don't have it do any kind of a popup or visual confirmation. I remember that when you first started using it, Leo, it was, like, coming up all the time.

Leo: Yeah, I gave up.

Steve: And you said, oh, what is this?

Leo: Screw this.

Steve: So what I do, when you think about it, I think a lot of surfing is in the just browsing category. You enter some search terms for Google, it does the best job it can, and then you march through the links looking for exactly what's right. In the process you're going to a lot of sites, pulling all of the content for that page and anything else it references into your browser. That's the time not to have scripting enabled, when you're sort of in that mode of looking through lots of content in a short time. As opposed to going to Amazon or to Wikipedia or to TWiT.tv or a site where, you know, an anchor site for you. Or you find a site that has things you care about, and you notice, like, maybe it's complaining that JavaScript is disabled because I'm seeing that more and more. Sites are recognizing that people are surfing with JavaScript, and so they're saying, hey, turn that on because our site needs it.

So I guess my sense is I'm still a proponent of, by default, having scripting disabled, and then - but being relatively casual about enabling it when there's a reason. Because I really think that, at least in my use of the web, when I'm looking for something, I'm browsing through many sites until I find what I want. I'd like to have my shields up while I'm doing that; and then, once I find something, if it doesn't want to work with scripting on, I don't have any problem then enabling scripting temporarily for that domain. And so that works for me.

Leo: Yeah, I think probably trusting the domain or not is really the key.

Steve: Right.

Leo: And I should - we do run quite a few scripts. If you ran Ghostery, you'd see quite a few scripts. There's analytics so we can keep track of how many people visit. It's going to - our new site is based on Node.js. If you turned off JavaScript, there'd be no site. So...

Steve: Right, right. Oh, no, yeah. So, for example, you'll have to have it on. But there are sites where 150 pieces of code, in fact 80% of the stuff being loaded is script. It's not even ads or content from other sites. It's script from organizations...

Leo: Well, that's kind of what our site's going to - actually, no. You won't, come to think of it, because it's Node, you won't see - you'll see HTML because it generates HTML and sends it to you. So I take that back. It won't be scripts executing on your desktop.

Steve: Probably. Right.

Leo: And NoScript doesn't care about that. If it's server-side JavaScript, it doesn't know.

Steve: Well, and once you say "Trust TWiT.tv," it's never a problem again, yeah.

Leo: Let me make sure I'm not moving too fast here. Yeah, yeah, I scrolled up a little bit here.

Steve: Well, we're approaching a two-hour podcast, so...

Leo: Holy cow.

Steve: And also 4:00 o'clock when you need to do TN2.

Leo: I turn into a witch, yeah.

Steve: So feel free to, like, wrap this up whenever you want to, and we'll just do the next questions in two weeks.

Leo: We'll do a couple more.

Steve: Okay.

Leo: Here's Brock Reese in Nashville, Tennessee. He has a question about credit card testing: Just started listening. Love the podcast. Welcome, Brock. I'm wondering if you have any information about how to deal with "credit card testers." I run a small business, and it seems we are flooded with "testers" from Indonesia. Is there a way to proactively block these people from spamming orders on my site? It does end up costing money and time dealing with these spammers. Oh, I know what's happening because it's happened to me.

Steve: Yeah. And tell me about it because I've never had the problem. But when I read his question, I thought, oh, of course. I've talked about how bad guys use credit cards at gas pumps.

Leo: Right.

Steve: Because they're near their getaway vehicle, and there's no attendant nearby to see them or for them to have to deal with in any way. But suddenly, reading Brock's posting, I realized, ah, they're - naturally ecommerce sites would be used as tests to see if credit cards which have been purchased by the underground are still effective.

Leo: They're seeing is this number good. And then of course after that goes through, that dollar purchase goes through, then they go buy, you know, a $10,000 something or other. So I had this happen to me, a couple of charges, like for a dollar to a British charity. And when I talked to the credit card company, the security guy there, he said, yeah, that's really common. They like to do charities because they often don't have the same safeguards online that others do. So it's safer. And it's always a small amount because, you know, they don't want to ring any alarm bells.

Steve: They're just trying to ping the card, essentially.

Leo: Right.

Steve: See if it's there.

Leo: So is there a way to avoid this?

Steve: I can't think of any.

Leo: Don't see how.

Steve: Yeah, I mean, you could block all of Indonesia by IP, but that would be problematical.

Leo: Yeah, what if you have some customers there?

Steve: Yeah.

Leo: And, you know, it's true, and this is going to be more and more of a problem, that the merchant is increasingly responsible for fraudulent charges.

Steve: Right.

Leo: So that's why Apple Pay and chip-and-PIN and all this stuff has to happen quick.

Steve: Yup. And that's a good thing. Unfortunately, what Google - Google's strategy is we need to hold people accountable, or they never will be.

Leo: Right. Want to do one more?

Steve: Let's jump to the end because there was a good one at the end.

Leo: Okay. That's what I was going to ask you, which one. Pick one from the last half.

Steve: Number 10.

Leo: Jim Leavitt, Beaverton, Oregon. He's puzzled about Steve - aren't we all, Jim. Oh, I'm sorry, there's more - and government backdoors: Unless I missed something about government encryption backdoors in your intervening podcasts, I'm having trouble reconciling your enthusiastic endorsement of Matt Blaze's testimony and Jonathan Mayer's note - this was in Episode 506 - with your empathic - or, I'm sorry, emphatic statements in SN-491. He quotes you, and this is where a transcript will get you in trouble: "I want to get correct about the technology because that's what we do here. And everybody's got that wrong. It does not weaken anything to give the government access. That is, it doesn't have to. It shouldn't." Oh, yeah. I remember this conversation.

Steve: Yeah.

Leo: "It's possible to have multiple front doors and for them to be every bit as secure as the security we have now." So you don't like some of these backdoors and key escrow and stuff, but you say inherently, though, having more than one key to an encryption process is not inherently insecure.

Steve: Well, yeah. So here's - and a number of people said, wait a minute, I thought you said this was, you know, it wouldn't weaken security. But you're saying, you know, you're like, yay for Matt and Jonathan for their testimony. So I just wanted to clarify. The math, the raw technology can do this. And I actually don't think there's disagreement on that point. And I think everybody agrees that it's the bureaucracy. It's the managing that technology, managing, for example, the extra set of keys, that's where we're going to get into trouble. And in fact the examples which various crypto experts have used isn't that, for example, multiply keying data is fundamentally flawed. It's that, inherently, having multiple keys increases the management burden on those keys. And all of our experience demonstrates we don't know how to do that yet.

So I just wanted to draw the distinction between the math, the raw crypto technology that does allow in theory the use of, the creation of multiple keys, with - and separate that from how do we manage those. And that's what everyone is afraid of is that it just - there would be all kinds of systemic failures in management of a more complex keying ecosystem.

Leo: Yeah. That's the flaw there. It's not a mathematical or a technical flaw.

Steve: Right. We can do it mathematically. It's just that, then what? You know, then it's like, who do you turn the keys over to?

Leo: Right, right. Yeah, who do you trust?

Steve: Right.

Leo: No one. Did you see, I didn't mention it, but Facebook has allowed people to put their public key into their Facebook account so that Facebook emails to me are now encrypted by PGP.

Steve: Oh, interesting. So you give them the public key, and they encrypt with your public key so that then you're able to decrypt.

Leo: Yeah.

Steve: Very nice.

Leo: Isn't that cool?

Steve: Very nice.

Leo: Yeah. I don't get any email from Facebook, but I did it anyway. I don't want any email from Facebook. But I did it anyway. I'm really thinking it's going to be

intriguing to see how Google - because they said they want to implement this, as well, somehow, in Gmail.

Steve: Remember that the browser can do local encryption. We've got all the technology we need now. JavaScript has matured to the point that it can do encryption. And while a lot of people argue that a browser is a fundamentally bad container for anything cryptographic, compared to nothing, it's better than that. And so you could certainly have a browser interface to Gmail where there's crypto in the browser such that it's encrypted under the recipient's public key and sent to Google, and then Google can say, "We can't decrypt it even if anyone asks us to." So they're just storing gibberish. And so it's browser-based end-to-end encryption. And we saw that, for example, with miniLock.io that a lot of people have adopted and are using now, a very well-designed, browser-based file encryptor, miniLock.io. Same, you know, does the same thing.

Leo: Yeah, I use that, yeah.

Steve: And the beauty of elliptic key technology is that the keys are so small. Unlike the big RSA keys, elliptic keys can be 32 bytes. And so, as is said, you can tweet them.

Leo: Facebook isn't yet using elliptic key, but they said they're going to adopt that quickly.

Steve: Yup.

Leo: But it is using Open - it's actually using Gnu Privacy Guard, which is what I use, which is an OpenPGP implementation.

Steve: Nice, nice.

Leo: Steve, Steve, Steve. We've run through the clock.

Steve: And covered every base.

Leo: Every possible base, including my RF - that's a cute little baguette, isn't it, my RF...

Steve: I'm glad to know that it works. That's very nice.

Leo: Yeah. We do this show live. I have apologized for scaring everybody last week, saying we weren't going to do it live, and we were going to shut down chat. That was wrong of me. I lost my head. Just chalk it up to I'm just a cranky old man. Get

off my lawn. But we are live now and will continue to be live, and the chatroom continues to operate. And what I realized, as I mentioned earlier, the chatroom is not mine, it's the community's. So they're going to police it. We've got great mods. They're going to take care of it. And we just - we've said "whatever resources you need." And they're looking into things like, which I think would be great, a web frontend that would require an SMS text message to validate your identity before you go in, things like that. Which I, you know, we'll see. We'll play with these things. Steve, thank you.

Steve: Always.

Leo: And we'll see you next time, live, Tuesday, about 1:30 p.m. Pacific, 4:30 p.m. Eastern time, 2030 UTC on TWiT.tv. After the fact, Steve has 16Kb versions. And I didn't notice this, I didn't know this before, but you also have the other audio versions, as well, on your website, along with show notes and fully human written transcripts at GRC.com. When you get there, though, pick up a copy of SpinRite. It's like tipping Steve and tipping yourself because it's the world's best hard drive maintenance and recovery utility. Check out SQRL. Can anybody - nobody can do the SQRL test themselves. You have to cooperate with them; right?

Steve: Not quite yet. There's one last feature I'm adding which I'll describe in the future, not to get in the weeds. But the client is almost finished. As soon as it's done, then that'll be a Windows client, and we've got - there's already one for Android, and of course Jeff Arthur's that I just used for the demo, running on iOS devices. But we're getting close. So it's becoming real.

Leo: Steverino, I'm so excited. GRC.com, that's the place to go. Steve's @SGgrc on Twitter. And next week do we know?

Steve: No idea. I've got a bunch of stuff. We'll see what the wind brings us during the week. And I'm sure we'll have something fun to show.

Leo: Good. Let's see what the wind brings us.

Steve: Thanks, Leo.

Leo: Thanks, Steve. See you next time on Security Now!.