SECURITY NOW!

Transcript of Episode #549

Listener Feedback #229

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-549.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-549-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We'll talk a little bit about the Apple thing. Testimony's going on right now. We've had Apple's response. Steve will talk a little bit about that. But there's lots of other security news. And yes, finally, your questions, Steve's answers. We've got 12 of them, coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 549, recorded Tuesday, March 1st, 2016: Your questions, Steve's answers, #229.

It's time for Security Now!, the show where we cover your security and privacy online. And we say it every time, but we're never going to run out of material, are we, Steve.

Steve Gibson: It never gets old, Leo.

Leo: Steve Gibson is here, the guru at GRC.com, which has been up now for a week.

Steve: Yeah.

Leo: Guy moved on. Did he ever send you an email?

Steve: Never got an email. I got five emails from other people who enjoyed having an email address for me. As you commented last week, I've never given an email address out because I just can't. Sue and Greg are my frontline filters, and they handle support and sales questions and so forth. And of course I respond to Twitter, I read the feed, and I'm in the GRC newsgroups, so I have a presence. But what I've found is it's just necessary to have some barrier.

But, yeah, everything has been great, and I'm appreciative that I can get on with working on SQRL. I'll talk a little bit about how I lost my weekend to trying to install Windows 7 on some old laptops, and what I learned. And I hadn't intended to burn my weekend that way, but I'm back focused on SQRL, so I'm really glad for that. And today we're going to do a Q&A. We haven't for a number of weeks because we've had one thing or another coming up. And there was one that was kind of a quasi Q&A, but I thought, nah, okay, let's...

Leo: Let's do a real Q&A, yeah.

Steve: And I had 639 pieces of email waiting for me in the Security Now! mailbag, so plenty to draw from. We need to talk a little bit about the news of the week on the Apple versus FBI deal. Apple has filed a formal reply that I want to - I found four, just four, out of 65 pages, four paragraphs that beautifully sort of sum that up. As we're recording this, there's testimony now in front of Congress. And ultimately I think everyone's pretty much agreed that the FBI's going to lose this, that this was a real stretch trying to use this All Writs Act, and that what's going to happen then is that we're going to need Congress to generate some legislation, some law. And of course that always scares me.

Once upon a time I would accept jobs being an expert witness. But I did that for a few trials, and I was so distraught over the outcome. First of all, I would only testify for the people who I thought were right, of course, because it's like there's no way I'm going to support the wrong side. And so I saw, like, these judges who were just technically incompetent. And of course I was being asked to testify about technical things.

The famous one was the NEC MultiSync Monitor, where they were advertising that this is the last monitor you would ever need because it's so smart about the way it handles the horizontal and vertical sync. And of course, as the developer of the Light Pen, which runs on horizontal and vertical sync as the way it counts scan lines and determines the Light Pen's position on the horizontal scan line, I knew this stuff upside down and backwards. And I can also explain things. And so they figured, hey, Gibson's like the perfect expert witness to explain why this indeed is the last monitor you'll ever need.

What happened was the PS/2 came out, the IBM PS/2 computer, and it used different horizontal and vertical sync, which the NEC MultiSync had no problem with. And so, indeed, this monitor did work on these new machines. But there was another company, Princeton Graphic Systems, that was trying to sell a new PS/2 monitor for the PS/2. And so they got upset that NEC was making the claim that nobody needed a new monitor. Anyway, the point is NEC lost. I mean, it was like, okay, I'm done. I'm not going to spend any more time trying to convince anybody of what I absolutely know and buy into.

So anyway, the point is that I'm a little nervous where, like we're just watching John Conyers, who, I don't know - actually, in that particular case, the judge had to pause testimony every so often to take a deep whiff of his oxygen from his mask.

Leo: Literally? Really?

Steve: I'm not kidding you. He had a green tank next to him. And so, but judges are lifetime appointments, and he was in no hurry...

Leo: There's a visual metaphor; right? Huh? Wow.

Steve: He was in no hurry. And so he was fascinated, and he thought I was wonderful, and he asked me questions. And I thought, okay, great, you know. And then, wham, he ruled, I think because the opposing counsel was prettier. And so it was like, oh, okay, you know, she was flirting, and I wasn't, and so it didn't matter whether the...

Leo: We've all watched "The Good Wife." We know how unusually the wheels of justice turn.

Steve: Anyway, so we've got that. I've got a comment that you were making before the show I want to strengthen.

Leo: Yeah.

Steve: And that is the notion about iPhone passcode length.

Leo: I have a Gedankenexperiment I want to go through with you. So maybe I'll be the first of the questions in the Q&A.

Steve: Okay. And we've got RSA's conference happening. And so some papers released already, but probably more coverage. In fact, next week's podcast is already named, and I forgot the name now. But there's two - there's a brand new horror about HTTPS and SSL or TLS. Actually, it is SSL because it's some servers still support v2. And a very clever hack for contemporary servers that make the mistake of not having completely shut down v2, just brilliant hack. And then a weird cache timing attack on OpenSSL. Even constant-time RSA, which we were talking about, constant-time encryption solves the problem of, well, some of the problems of side channel. This is a different side-channel attack.

So those are our two big topics for next week, for anyone who wants to tweet me about - it's not DAWN. It's not - it's a five-letter word, DROWN, DROWN, the DROWN, D-R-O-W-N. And unfortunately, the last word of this abbreviation is actually encryption, but D-R-O-W-E didn't really work, so they used the "N" from encryption, the second letter of the last word, rather than the first letter. It's like, okay, you're kind of cheating on that, but fine. And some miscellaneous stuff, and then of course we've got actually a dozen because there was one fun long one, but a lot of sort of shorter questions. And so I think a great podcast.

Leo: I know a great podcast. Not the least of which, I know your eyes will be turning toward CNN in about 20 minutes when the first results from Super Tuesday come in.

Steve: Yeah, when - I know.

Leo: So it's a busy day. It's a busy day.

Steve: Yes, it is. It's going to be. Although I already know what's going to happen. I've been following it closely enough that probably it's a fait accompli.

Leo: Well, you never know. It feels like there's lots of surprises.

Steve: Well, and the details are fun. For someone who is as engaged as I am, I mean, I just don't want to look at the final score. It's fun to watch it happen. So, yes, TiVo is sucking it in, and that allows me to do some commercial skipping.

Leo: Good.

Steve: So late last week Apple filed their formal reply to the FBI's demand under this All Writs Act from 17 something or other [1789] that they create software - last week we talked about what it was the FBI wanted, which was that the "10 strikes and you're out" wiping of the decryption key would be removed; that any additional delay deliberately imposed by the OS and therefore under software control be removed; and that they be given an electronic means for rapidly entering their guesses in order to perform essentially a brute-force attack on the password that had been set into that phone. I expect that this week will be our - we will not be talking about this every week because pretty much until...

Leo: I hope you're right.

Steve: I hope. Until there's a decision on this case, and we'll certainly mention what that is, but then I think it'll be some time until there's some congressional action. And, I mean, who knows? We're in an election year. I don't know if this would, you know, like where the executive branch stands relative to Congress, what sort of a partisan divide there is. But as we know from the sudden death of the justice last week, everything is sort of up in the air. So maybe this gets punted. Who knows? Anyway, what I wanted to do, the Apple response is 65 pages of legalese stuff. But there are four paragraphs that beautifully state their position that I just want to put into the podcast. And as I said, I think this will be the last coverage we give it for a while.

So Apple, explaining their case, wrote: "There are two important and legitimate interests in this case: the needs of law enforcement, and the privacy and personal safety interests of the public. In furtherance of its law enforcement interests, the government had the opportunity to seek amendments to existing law, to ask Congress to adopt the position it urges here. But rather than pursue new legislation, the government backed away from Congress and turned to the courts, a forum ill-suited to address the myriad competing interests, potential ramifications, and unintended consequences presented by the government's unprecedented demand. And more importantly, by invoking 'terrorism' and moving ex parte behind closed courtroom doors, the government sought to cut off debate and circumvent thoughtful analysis.

"The order demanded by the government compels Apple to create a new operating system - effectively a 'back door' to the iPhone - that Apple believes is too dangerous to build. Specifically, the government would force Apple to create new software with functions to remove security features and add a new capability to the operating system to attack iPhone encryption, allowing a passcode to be input electronically. This would make it easier to unlock the iPhone by 'brute force,' trying thousands or millions of passcode combinations with the speed of a modern computer. In short, the government wants to compel Apple to create a crippled and insecure product. Once the process is created, it provides an avenue for criminals and foreign agents to access millions of iPhones. And once developed for our government, it is only a matter of time before foreign governments demand the same tool.

"The government says: 'Just this once,' and 'Just this phone.' But the government knows those statements are not true; indeed the government has filed multiple other applications for similar orders, some of which are pending in other courts. And as news of this court's order broke last week, state and local officials publicly declared their intent to use the proposed operating system to open hundreds of other seized devices, in cases having nothing to do with terrorism. If this order is permitted to stand, it will only be a matter of days before some other prosecutor, in some other important case, before some other judge, seeks a similar order using this case as precedent. Once those floodgates open, they cannot be closed, and the device security that Apple has worked so tirelessly to achieve will be unwound without so much as a congressional vote.

"As Tim Cook, Apple's CEO, recently noted: 'Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks - from restaurants and banks to stores and homes. No reasonable person would find that acceptable.'" End of Tim's quote.

"Despite the context of this particular action, no legal principle would limit the use of this technology to domestic terrorism cases. But even if such limitations could be imposed, it would only drive our adversaries further underground, using encryption technology made by foreign companies that cannot be conscripted into U.S. government service, leaving law-abiding individuals shouldering all of the burdens on liberty, without any offsetting benefit to public safety. Indeed, the FBI's repeated warnings that criminals and terrorists are able to 'go dark' behind end-to-end encryption proves this very point.

"Finally, given the government's boundless interpretation of the All Writs Act, it is hard to conceive of any limits on the orders the government could obtain in the future. For example, if Apple can be forced to write code in this case to bypass security features and create new accessibility, what is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user? Nothing."

So I think that puts Apple's position very clearly. And the assumption now, I think, in the industry is that they're going to lose. And in fact what just happened yesterday was that there was a ruling on a different case regarding an iPhone 5s which was seized by the DEA in 2014. This started being worked through the courts last October. And there was a judge, James Orenstein, who said: "For the reasons set forth below, I conclude that under the circumstances of this case, the government has failed to establish either that the AWA" - which is that All Writs Act - "permits the relief it seeks; or that, even if such an order is authorized, the discretionary factors I must consider weigh in favor of granting the motion."

And so essentially the government in this case lost an essentially identically founded case, and Apple prevailed. So it's not clear whether this judge's rulings will affect the one pending that we've been talking about. They're different cases. There's no terrorism component and so forth. This was a drug-related case. But this is an example of what Apple was talking about, other cases that are - and this was, they said, this was their response, Apple's response late last week. This just happened yesterday. So this is one of those pending cases that was also attempting to use the All Writs Act. And this Judge Orenstein said, eh, no, that doesn't do the job.

Anyway, so my guess is this current case will be similarly decided, and it will be then necessary for us to go the legislative route. And certainly next week I'll put a link in the show notes, and in fact I will tweet it once we're done, a link to the testimony that is underway right now in a committee hearing of all sides about this. This is the beginning of the process of these gears turning.

Leo: This is an awesome opportunity, though, for people to remember that there's an election coming up in November, and it's not just for President. Half the House gets reelected, a third of the Senate. And this is an opportunity to consider this when you choose the candidate you vote for because I do believe Congress will be taking this up, probably not till after the election might be my guess.

Steve: Yes, yes.

Leo: And so, while no one issue should determine who gets elected, I think, but this may be a pretty important part of your calculus on who you're going to support. And it won't be across party lines. I doubt it will be. And you may not have a choice in many districts. But if you do have a choice, it's important.

Steve: It doesn't sound, it doesn't feel partisan. It feels like...

Leo: No.

Steve: You know, like we need to decide, I mean, and as we've been saying on this podcast, we've been seeing this collision coming for a couple years, I mean, you can see both sides. And the FBI chose this case because it was contemporary and terrorist-related, which generates extra heat for it. And it's the problem of math being unbreakable. And the problem, of course, as we discussed, is that the math is already out. It's escaped. And so if Apple and Google are not allowed to deploy this kind of encryption by default in their base platforms, then people who really want it can get it. And in fact, in the testimony we heard someone talking about telegraph. He called it, yeah, the worst tool that's available.

Leo: Telegram, really?

Steve: No, actually "telegraph" is what he said. And I don't know if he meant Telegram.

Leo: He's talking about Telegram, I'm sure, yeah.

Steve: Yeah. Anyway...

Leo: You know, I guess the thing that we should stipulate is, A, if you're smart, you can use encryption, and you could probably do a fairly good job of protecting your privacy. We're going to talk about my experiment that I did with the iPhone to see how much I could lock it down. But what really this is all about is the normal person, and something easy and convenient for a normal person to use. And but that's where my thought experiment's going to come in because I'm also of the opinion that the normal person should know, that really, in my opinion, I want to know what you think, nothing is going to be - nothing's going to be both convenient and truly secure.

Steve: Yes. I don't know if the normal person has any awareness. Our podcast...

Leo: Well, that's our job. And that's my job on the radio to tell normal people. So I want to know what to tell them.

Steve: Right. Okay. Yeah. So, for example, we've talked often about Threema. Threema is my favorite messaging app, which I have no need for because there's nothing I'm doing except deciding, like scheduling when my friends and I are going to meet for margaritas somewhere. And if the FBI cares about that, hey, fine. But if I absolutely needed security, I would use that. And I would arrange to securely exchange private keys, and then it doesn't matter what platform I'm on. But it's not...

Leo: Well, it does because, if you're on a platform that has a keystroke logger on it, you can use Threema all you want.

Steve: Yeah, that's true.

Leo: So really the last line of defense is the operating system. And you probably saw the Ars Technica article which I think makes a really good point that there is a fundamental backdoor in all operating systems which is called the update facility. We saw it with Sparkle, which was a Macintosh updater, and people were using it incorrectly, and it was easy to do a man-in-the-middle. But if the government can force Apple or Microsoft or Google or any company to put rogue firmware on a phone, all bets are off; aren't they?

Steve: No.

Leo: Okay. That's the thought experiment. So we'll get to that. I don't want to get you out of order here.

Steve: Okay. So there's been a neat forensics tool developer, Jonathan Zdziarski, who's been very active in this whole, well, he's been tweeting like crazy and blogging. And he proposed a nice formal definition of a backdoor. But then even more recently he tweeted, just yesterday afternoon, something that I got a kick out of. And his tweet from 1:35 in the afternoon yesterday, he tweeted: "The first uses of my iOS forensics tools were in terrorism and kidnapping cases. Not long after, cops were using it for girlfriends' phones."

Leo: Right.

Steve: And therein lies one of the problems, is that you have a tool like this, and it is just - it's human nature. You mentioned "The Good Wife" earlier, and the NSA is back to listening in on Alicia Florrick's phone, and we're having some good fun with all of that. And the problem is, you know, and Snowden talked about naked pictures that were being passed around the NSA from the eavesdropping.

Leo: It used to be really easy because any law enforcement officer, many of them had a device in the car when they pulled you over that they could connect to your phone, and within a minute, while they're checking your license, suck everything off of your phone. A lot of people just said yeah. "Can I see your phone?" "Yeah, okay, Officer." But that's the point, that's why Apple put encryption on there, to prevent these kind of casual scooping up of everything in your phone.

Steve: Right. So Jonathan goes on, and he worked to formally define "backdoor." Now, even in Apple's document, I read most of the 65-page legal...

Leo: They used the word "backdoor."

Steve: Yes, they did. And it's two words, actually, "back" and "door" with a space in between. So it's like, well, okay. And it was ill-defined, which as we said last week, there's no definition for backdoor. So Jonathan, who is in a position to come up with a good definition, he wrote: "A backdoor is a component of a security mechanism where the component is active on a computer system without the consent of the computer's owner, performs functions that subvert purposes disclosed" - wait. It "performs functions that subvert purposes" - it must be not disclosed, I must have forgotten a "not" in there - "not disclosed to the computer's owner, and is under the control of an undisclosed actor."

So that's very broad, but I think it's a beautiful definition of backdoor. And that's the way we've always used it. We've, when we see it being used in the press and, lord help us, in Congress, it has no meaning. It just means something the FBI wants and Apple doesn't, whatever, you know, it's a big blurry cloud. But a backdoor is exactly what Jonathan said. It is something that is secret that is under somebody else's control, that in some way subverts the security of the system that is the backdoor's target. I think that's our formal, useful formal working definition. And that has nothing to do with this case. This is not a backdoor that the FBI is asking for. It is an improvement of brute-forcing the password is what they're asking for. And from the beginning, when I heard that, I thought, oh, that's kind of clever. I mean, like somebody at the FBI figured out what to ask for that was doable and that...

Leo: But in a larger sense it's a backdoor because, if the FBI can compel Apple to create custom firmware for a phone, that firmware really is in that sense a backdoor; right? It's putting something on the phone to change the phone's security behavior. And now in this case the terrorist is dead.

Steve: Well, okay. So...

Leo: So he doesn't know. But you know what I'm saying? It's a backdoor. The larger thing is a backdoor, which is the idea that a company can modify the firmware.

Steve: But they can, well, yes, except that Apple also has hardware that can presumably not be modified. So, for example, and that takes us right into the next point in the show notes, which is complex iPhone passcodes. What we discussed in March of 2014, so exactly two years ago, I noted that the old PDF I had downloaded was on the 11th of March. And this was the iOS security whitepaper which was dated February of 2014, from Apple. So Apple published that first really comprehensive whitepaper two years ago, and we gave it multiple podcasts. One of the things that it makes very clear is that they deliberately did a high-repetition count PBKDF, password-based key derivation function, which cannot be sped up. Nothing can speed that up. And that's 80 milliseconds per guess and is not subject to being changed by the firm - it isn't in firmware. It's in hardware. So what I wanted to amplify for our listeners is that that's slow. I mean, 80 milliseconds...

Leo: Well, if you have a 16-character random password, that's millions of years is what it is.

Steve: Exactly. Exactly. And so I wanted to quote what we had covered. It's funny because when I opened that PDF and scrolled to that location, I had highlighted this block, which we looked at closely. And you'll remember this word, Leo, because they used this again. They made up a word that I gave them some heat over two years ago. So they wrote, under passcodes, they said: "By setting up a device passcode, the user automatically enables Data Protection," which we know is the whole device encryption using a randomly chosen symmetric encryption key so that all of the storage is always encrypted.

Apple goes on: "iOS supports four-digit and arbitrary-length alphanumeric passcodes." This was then. We know that they increased it by two digits to six since then. "In addition to unlocking the device, a passcode provides the entropy for encryption keys, which are not stored on the device. This means an attacker in possession of a device cannot get access to data in certain protection classes without the passcode.

"The passcode is 'tangled.'" And that was the word. I said, what? What the heck does "tangled" mean? They just pulled that one out of the air, tangled. "The passcode is 'tangled' with the" - and we think they mean hashed in some way because they say "'tangled with the device's UID, so brute-force attempts must be performed on the device under attack. A large iteration count is used to make each attempt slower." And so even if this were done in software, you can't ever short-circuit a large iteration count. There's no way to short-circuit it. And it is designed to be acceleration-proof.

So continuing, they said: "The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. This means it would take more than 5.5 years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers." And they go on, but I won't because this makes the point. So what the FBI is asking for is for - or actually they did say here, skipping a paragraph: "To further discourage brute-force password attacks, the iOS interface enforces escalating time delays after the entry of an invalid passcode at the Lock screen."

That's one of the three things the FBI has asked Apple to remove is the removable, the escalating, software-imposed, whoops, you didn't guess right so we're going to make you wait longer and longer each time. But that 80 milliseconds cannot be short-circuited. Now, and again, we lack definitive design specs. So it's not clear what's being done in hardware, what part the Secure Enclave has. But we really are seeing a proactive design attempt from Apple to limit their own ability to crack phones.

Leo: Yeah, but nobody's going to - I've tried this, by the way. I had a nice, long, strong password on my iPhone. And it's such a pain in the ass, nobody's going to do that. You can.

Steve: Correct, correct.

Leo: But it's not convenient.

Steve: So I wanted to make sure that our listeners know. Well, okay.

Leo: It's there. It's there. You can do it.

Steve: Yeah. And also remember that...

Leo: And by the way, you should turn off automatic updates; right? Because you don't want them pushing some firmware on your system. Right? And I would turn off the fingerprint reader because I don't - there's issues with that. You know, you can be compelled, for instance, to use it. So you can't use the fingerprint reader. You have to use a long, strong password, which is a pain in the butt to type. And you have to do it every time you unlock your phone.

Steve: Right.

Leo: And you cannot accept firmware updates of any kind because you don't know if they're okay.

Steve: Okay. So what we just covered, though, prevents - it indicates firmware cannot short-circuit that 80 milliseconds. So if you do have a long, strong password...

Leo: No, no. But they don't have to. If you've modified the firmware, yes, the FBI is asking for this dopey modification, this front door brute-force thing. But why bother? Just modify the firmware so that, while the person's using the phone, you transmit the unencrypted data out of the phone. Do a background backup. Because we know by the - oh, incidentally, you have to turn off all iCloud backups because we also know Apple has access to those.

Steve: Right.

Leo: At this point, you've got a secure phone no one wants to use. A bad guy will do that because he's motivated.

Steve: Right.

Leo: The rest of us will not.

Steve: Right. Well, and we do know, as we discussed last week, that five weeks, or I guess it was six weeks before the last use, that phone had been backed up to iCloud, and the FBI had that. But what they wanted was, for whatever reason, whether they actually want the phone...

Leo: No, it's a precedent, is what they want.

Steve: Or, yes, or they believe they would be able to achieve what they want.

Leo: And remember the precedent right now is making it easy for them to do the six digits. Or four digits, probably. The precedent, though, would establish precedent to get at - the real precedent is Apple will write firmware to help us get into a phone. And should that happen, are you saying to me that I can prevent Apple from getting my data? No, because, right, if I've unlocked the phone with my long, strong, good, entangled password, the phone is now unencrypted; right?

Steve: Correct. Correct. Then, while it's unlocked...

Leo: In the background it goes [whining sound].

Steve: ...the symmetric encryption key is in place, and the phone has access to your data.

Leo: And they can start sending stuff out of my phone, yeah.

Steve: Yup.

Leo: So that's the real precedent, I think. I don't think it's about the brute-forcing.

Steve: Right. So my point was that a long passkey or passcode, passphrase, whatever you want to call it, does thwart the brute-forcing. But you make the point that, if Apple has been compelled to access a phone while it's in use, it's unlocked. I mean, it is decrypted. Yeah, and your comment about the keyboard interception is the same.

Leo: Right.

Steve: I remember we all noted when Apple allowed custom keyboards to be added to iOS, that they replace...

Leo: They warn you. But they don't have to warn you.

Steve: They warn you, and...

Leo: They could do that with Apple's keyboard.

Steve: They take the measure of using their keyboard if they detect that it's a password that you're entering.

Leo: Right. So you have to trust Apple. And once there's a precedent that the federal law enforcement can compel Apple to do what they want, which they frankly can, Apple can't really say, oh, we can't do that, because they can. They always can; right?

Steve: Right.

Leo: So all I'm saying is it's just like locking a door. You can make a law that says you can't cross that lock, but anybody can break in. Locks do nothing. What the lock does is establish a line in the sand that you cross it, now you're breaking the law, and we can use the law to prosecute you. But the law itself can be subverted by a bad actor, whether in government or out.

Steve: Yup.

Leo: So I'm just saying it's really - all of this is a lot of hand waving. But ultimately, the idea that your phone could be secure is a long shot.

Steve: Yeah.

Leo: Okay. I just wanted you to say yes.

Steve: No, I completely agree.

Leo: Because I think that that's, I mean, what we're talking about is a good thing. We should have laws against it. And we shouldn't allow government to do this. It's the Fourth Amendment, et cetera. It should be very clear, Congress needs to make a very clear statement that this is going too far. Doesn't mean it won't happen. And it may not be government that does it. I mean, it could be a bad actor at Apple.

Steve: Where did we leave off with the FISA court secret letters...

Leo: There you go.

Steve: ...that were undisclosed?

Leo: They still - that's in the Patriot Act.

Steve: Yeah.

Leo: You are not allowed to - and Apple almost - remember Apple's first reaction to this FBI issue was seal it. We'll help you. Just seal it. We don't want a precedent. Doesn't mean they don't help. They do help.

Steve: Well, and they have stated that they want to be helpful.

Leo: Yes.

Steve: I mean, they absolutely want to help law enforcement where they can. For example, they made the iCloud backup immediately available, the last backup that they had of the phone. It's like, yeah, here you go.

Leo: Here. We got the keys. No problem. So you can secure an iPhone pretty well, if you're willing to put up with a lot of inconvenience, and never getting updates.

Steve: Well, and this does come back to the point you also made earlier about convenience because it is four things like what if the user absolutely forgets everything that they know, yet their device is backed up in the cloud? There has to be some means for key recovery. Well, if there is, that creates a weakness in what could otherwise be absolute security. Thus it isn't actually absolute because you have to provide those features.

Leo: Anymore than that lock on your door really keeps anybody out. It's social convention. It's law. It's policy.

Steve: Yeah. You know, when you forget a password on a website, and you say "Send me a password recovery link," well, that password recovery link comes through email, which is really not safe, easily interceptable. Somebody gets it and clicks on it before you do, they're recovering the access to your account. So here we have a situation where the email, which is really not secure, is the fallback for all of the other security that we have with our big fancy long passwords. It's like, yeah, except it's not really that secure in practice.

Leo: You know, the truth is it's so hard to really be secure that only somebody strongly motivated will be secure.

Steve: Yeah. And as you said, you give up a huge amount of convenience.

Leo: Yeah.

Steve: If you really, really, really lock everything down, suddenly there's lots of things that don't work and that you can't do and can't use.

Leo: And ironically, you might even be more insecure because you're not taking updates, which means there may be zero-day flaws that aren't patched. So, you know.

Steve: Yup.

Leo: Okay.

Steve: So at the RSA conference, which is ongoing, and I'm sure we'll have other interesting papers arising from it, there was one that I just sort of wanted - it just popped up, and I wanted to share it. This is not super news except one particular statistic that sort of stood out from all others was interesting. And there's a company, Avecto, which has a booth at RSA, that has analyzed the security bulletins, the Microsoft Patch Tuesday security bulletins from all of 2015. And actually they compare it to all of 2014 also. What they found was that, on average, 85% of the critical Microsoft vulnerabilities would be mitigated by removing administrative rights from the user. They also noted that in 2015 there was a 52% increase in the total volume of vulnerabilities compared to 2014. So, yes, this podcast will hit triple digits before we run out of stuff to talk about.

Okay. So what I found was really interesting, though, is that, when they break it down, one really stands out, and this connects into one of our Q&A points that we'll be getting to later in the show. Their key findings were, of the 251 vulnerabilities that were in Patch Tuesday security bulletins in 2015 with a critical rating, 85% were concluded to be mitigated by removing admin rights. And again, there's been a 52% year-on-year rise in the volume of vulnerabilities since 2014, which is to say half again more in 2015. 86% of the critical vulnerabilities affecting Windows were mitigated by removing admin rights. And here's the one that stood out, though: 99.5, almost 100%, 99.5 of all vulnerabilities in Internet Explorer were mitigated by removing admin rights. And this will...

Leo: Just stop using Internet Explorer. Then it's 100% of all...

Steve: Exactly, exactly. So, and then there was Office, remote code execution, critical vulnerabilities in Windows 10, and essentially they were all in the 80 percents. So essentially, what's sort of funny about this is that the technology was built into Windows. I don't really know that the early, the Windows 3.1, 95, 98, ME, I don't think that group had strong security. But NT had the notion of admin and non-admin users because, of course, it came along well after Unix.

And Unix had established this concept of root privilege because Unix was a multiuser operating system. It had terminals connected to it. And people without root privilege, absolutely without root privileges, all over a campus, would be logging in with terminals into a Unix machine. So this notion of clearly delineated rights between users at terminals, who ran jobs through their terminals, and the administrator of the OS, that was absolutely distinct.

The problem was then we got personal computers, where the owner of the computer was both the user and the admin. And there were things that, back in the Unix days, I remember using a Unix terminal when I was at UC Berkeley. And there were things you couldn't do that annoyed us, especially we computer people. But there were lots of things that were off-limits. And it was annoying that there were directories we couldn't see. We knew they were there, but we couldn't see. There were directory rights and file rights that we were unable to change.

And so what happened was, with the advent of the PC, that distinction blurred because you own the computer. You need to be able to install software. You need to be able to do whatever you need to do. The problem is the right of installing software under your account means that malware can also install software by impersonating you with your account's rights. And so we sort of went through this awkward period where, well, the advice was you should not be an administrator. But everyone kind of winked and said, yeah, I know; but I tried that, and it's just no fun. I want to be an administrator so I can push all the buttons and do whatever I want to do. And the problem was the malware was having a lot of fun at that.

Then of course Microsoft continued to struggle with this with version after version of Windows, making it first way too onerous, which is really what happened with Vista, where it was just a horrible problem. You couldn't do anything without the screen going dark and a dialogue popping up and saying, confirm that you really want to do this. It's like, yes. And they had this notion of split rights, where your account had admin rights and non-admin rights, and you would normally run as a non-admin, but then you'd be able to elevate, temporarily elevate your rights in order to get something done.

I mean, they, to their credit, really tried to work around what was a fundamental problem, which is the person who owned the machine didn't want to be told there was something they could not do, and arguably had to, if it was really them, do things. But then how do you prevent malware from impersonating? So anyway, we're still fighting that today, although I think that it's very clear that, I mean, and for years, when we go over what Patch Tuesday brings, it's oh, yeah, this doesn't have a problem. No problem here if you don't have admin rights. So now we've got some numbers from this analysis saying, yeah, especially with IE, almost none of the problems that affected IE were able to do anything from inside the browser if it wasn't running with admin privileges.

I got a tweet. And this could have gone back in the Q&A, but actually it came in late, and I'd already assembled the Q&A and had already two extra questions and made the PDF. So I thought, okay, I'll just stick this in because I think this is of general broad interest. And so this was Christian Turri who tweeted: "Hey Steve, here's a quick question for the Q&A podcast. ShieldsUP! is great, and I use it all the time, but do you have any tools you can recommend to do internal port scans? Basically I want to do internal port scans on some IoT devices to see what they're opening. Thanks."

And I thought, boy, you know, that is a great question. We haven't talked about this at all except we've been talking about the three dumb routers, the need to isolate IoT devices. But we are at a stage now with so much stuff in our LAN, in our local area network, whether we've got one or segmented or whatever, that being able to probe ourselves makes a lot of sense. And as I have mentioned several times, ShieldsUP! is stopped at the border, which is what we want. ShieldsUP! is looking at your router's ports. But all of your LAN is hidden behind it. What's going on there?

Well, immediately I was put in mind of a tool that a friend of ours who used to participate actively in the newsgroups a long time ago, Robin Kier, he worked for a company called Foundstone, where he produced a whole bunch of utilities. Foundstone was purchased by McAfee, which was purchased by Intel. So he developed a nice, very capable Windows internal network port scanner. And actually there's nothing to keep it from being launched to do external scans, although you can get yourself in trouble if someone sees you scanning the 'Net, so I would recommend you just leave it to scanning your local area. But it's called SuperScan.

The last version he worked on was SuperScan v3.0. Well, I should explain, he did a 4.1 because he was excited about the use of raw sockets when they became available. But then of course Microsoft removed their access with Service Pack 2, I think it was, maybe it was 3, of XP. And in the SuperScan v4.1 notes, it mentions that some of its capabilities were neutered by the lack of raw sockets in Windows. And I should mention, I'm assuming Christian wanted a Windows-based port scanner. Nmap, of course, is the famous scanner that is available for Unix and Linux-based systems. But if you just google, you could google "Foundstone," F-O-U-N-D-S-T-O-N-E, and then "SuperScan," or probably just "SuperScan v3.0," you'll find it.

And there's also, because I had some fun poking around, there's a little directory hierarchy at the top of the page. And if you bounce up a level or two, they've got just a long scrolling page of all kinds of interesting utilities, that is to say, McAfee does - some McAfee, some from Foundstone that McAfee acquired when they acquired Foundstone. But I did think, I think the idea of scanning your own network, who knows what you'll find? And you're able to put in a range of IPs. So you would put in 192.168.0.1 to 192.168.0.255 and tell it to do all ports on all 255 IPs, and press Go, and see what it chose. I think people will have a lot of fun seeing what ports they find on devices that are open within their own network, sort of a cool exercise.

And I already mentioned at the top of the show that next week we would cover the DROWN attack, that's D-R-O-W-N, Decrypting RSA with Obsolete and Weakened eNcryption. And then also the CacheBleed attack, which just happened today, so I haven't had any chance to look at it.

A couple miscellaneous things: I did note with some sadness that SlySoft, that was the maker for I think a decade, since like maybe 2004, so that's more than a decade, who made AnyDVD, was shut down. Actually, they became a little problematical for me a few weeks ago because the certificate they were signing their code with was no longer being accepted. Probably it was an SHA-1 certificate, and they hadn't updated it. But they had been under attack by essentially Hollywood. And I haven't really had any occasion to use them for quite a while because I haven't had any need to rip my own DVDs. But there were some occasions where I wanted to rip it in order to transfer it to an iPad if I was going to be traveling so that I could watch a movie, sort of like before the advent of everything now being available online as it is.

So it's not as big a loss as it would have been 10 years ago, when they began. But I've always felt - and I know that, Leo, you're sympathetic - that material that we purchase and own for our own use, we should have access to use as we choose. And so I certainly never used it for piracy, and I would never advocate it that way. But anyway, we've lost really my favorite utility for doing that.

With all of the activity over the last couple weeks, I hadn't had a chance to mention where things stood with the Zeo, the EEG brainwave monitor. So I just did want to mention that GRC's Zeo page has got a lot of updates over the last month with essentially user tips. We ended up, this URT outlet company that purchased the surplus stock ended up selling more than 2,500. They sold out all their auctions. They sold out, that's the final 1,600-unit auction. More than 2,500 of our listeners purchased these. And I've been seeing tweets from people having a lot of fun with them and being glad to have the opportunity.

So I did want to make sure people knew to take a look at GRC.com/zeo.htm. There's some more recent activity that I just haven't had a chance to add links to, and I will. There is a Zeo CSV utility which its author has updated just recently, both in the Google Play Store and the Amazon App Store, which allows you to export your entire accumulated database in a comma-separated-value (CSV) file, which you can bring up in a spreadsheet. Or there is something called the Zeo Viewer, which you can find if you just google it, and I will put links on GRC's page. It's a Java-based application, so it's multiplatform, which gives you essentially much better viewing capabilities.

For one thing, the Zeo actually has five, or I'm sorry, has 30-second resolution of the sleep state you're in. But the Zeo app only shows five minutes. So this gives you, what, 10 times more slices, that is, that are in the CSV file, which the Zeo Viewer Java app, the Java application does show you. So anyway, I will update the page the moment I'm through with the podcast, before I get back to working on SQRL, so that anyone hearing this can go check out the page if they want a little more flexibility.

Leo: Do you want to talk about your cocktail yet?

Steve: Probably not yet.

Leo: I'll just give you my results. Steve has a little sleep cocktail, doesn't involve alcohol. So first night I took the minimum dose that your friend's been taking, and nothing.

Steve: Right.

Leo: Second night, I took your dose. Whoa. Yes, I slept soundly through the night. And then I didn't take it last night, just to see, because I don't want to get dependent on it. It's all just supplements. It's not, I mean...

Steve: Well, actually it's all - I call it the "healthy sleep formula" because not only is sleep healthy, but all of the constituents are healthy.

Leo: Okay, I'm going to trust you on that because I don't know. Lisa said you should tell your doctor because it's like five different things.

Steve: It is.

Leo: And I trust Steve. He's a doctor. He's like a doctor.

Steve: Well, I've done - I will - I've got to get SQRL back up and running.

Leo: More important, much more important.

Steve: But I really, really, my sister had the same experience, Leo. She and her husband both had the best night's sleep they've had, like, forever. But I'm so excited. So anyway, you said the second night, which would have been last night, you didn't take it.

Leo: Yeah, and I didn't sleep well. In fact, I slept worse. So I'm just, I'm afraid. I don't want to become dependent on this. But I guess it's harmless to do so.

Steve: The reason you slept worse is that you had, I mean, is that there are many things that happen to us as we age.

Leo: Yes.

Steve: Cortisol, the stress hormone, is one that becomes dysregulated. So that first thing, the Seriphos, what that does is it simply sensitizes the - it's going to get too - it's going to get really deep in the weeds.

Leo: And I don't know if we want to because I don't want to do this prematurely. I think...

Steve: Yeah, I just, I cannot...

Leo: You should save it for a time that you can do it right, you know.

Steve: I've got so much on my plate now.

Leo: But let's just say this. Steve has come up with something that really helps you sleep better.

Steve: Yeah. A number of people in the newsgroup, I think everybody who's tried it in the newsgroup has, like, had the best sleep they've ever had. It solved my problem. It solved my friend's problem and my family's problem. It's a collection of five available...

Leo: Herbs and spices.

Steve: Yes.

Leo: It's Colonel Gibson's Secret Formula.

Steve: Individually, they're either endogenous, that is, they're already in us and synthesized by our bodies, but you just need a little bit of a kick at the right time.

Leo: It's melatonin and stuff like that; right? It's not...

Steve: Yeah, exactly. The one that isn't is L-theanine, which is the predominant, overwhelming, more than any other amino acid in green tea. That's the relaxing component of green tea. And so what I've been doing is, for the last - I've been working on this since October. And I can't remove anything without it collapsing. I haven't succeeded in reducing a dose without it collapsing.

Leo: But now you have to take it every night.

Steve: Well, but the problem is - so the reason you slept worse is that, with such a fabulous night's sleep...

Leo: I didn't need as much the next night.

Steve: ...the sleep pressure was reduced.

Leo: Yes. My sleep pressure was reduced.

Steve: Yes. And so, yeah, I mean, I don't think, I mean, again, I'm a supplement taker. I take six grams of Vitamin C. I take a bunch of magnesium. I take a whole bunch of things already. And so I guess I'm - the idea of taking something to sleep doesn't put me off at all.

Leo: It's like a little vitamin pill.

Steve: Yeah, exactly, it is a vitamin cocktail. It's amino acids and phospholipids.

Leo: If you just made a little shaker, and I could put it in my tea...

Steve: Well, actually Doctor's Best is just down here, like a stone's throw away from me. And I'm thinking, if this thing ends up taking off, maybe we could get someone to formulate a...

Leo: Doctor Steve's Secret Sleep Mixture.

Steve: Anyway, I'm so glad. Thank you for letting me know that it worked for you.

Leo: Yeah. I'm going to be taking it tonight, I can tell you right now.

Steve: And let me tell you, one of the things that I want to have time to document is how important sleep is for health.

Leo: Well, that I know, yeah, because I don't sleep well at all anymore.

Steve: For example, you should be much less hungry after a long night's sleep.

Leo: Yeah, yeah.

Steve: Because leptin, which is the hormone that our adipose tissue produces, it does so while we sleep. And growth hormone is released, which is very good for you.

Leo: I don't want to grow.

Steve: And that's being released.

Leo: I'm done growing. I did enough growing sideways.

Steve: Anyway, thank you for letting me know. I'm delighted. I was...

Leo: Yeah. So at some point we'll reveal this secret formula to the world. But we should point out Steve's not a physician. You should ask your physician.

Steve: I'm just a health hobbyist. And so far people are not getting sick during the wintertime because they're taking Vitamin D.

Leo: Vitamin D, thank you.

Steve: And how many husbands and wives told you that they lost 50 pounds each after experimenting with no carbs?

Leo: It almost killed me. The ketosis almost killed me. That one I might disagree on. But the other stuff, fine. The other stuff's good.

Steve: Cool.

Leo: So I just wanted, I wanted to fill you in on that.

Steve: Thank you.

Leo: Nice. I got a mystery package, you know, from Steve, like a couple of days ago, with five vitamin bottles in it.

Steve: It arrived on Saturday.

Leo: Yeah.

Steve: And I said, Leo, this is the healthy sleep formula.

Leo: But I need your dosing because the mild dosing didn't seem to do anything.

Steve: Yeah. Two of everything and one of the last.

Leo: Your dosing, I just - I was out. And as you said, when I woke up, I'd wake up and go right back to sleep.

Steve: That's the key, yes. Because many of us will, see, sleep is inherently cyclic. And so it may well be, you know, sometimes we wake up because we have bladder urgency.

Leo: Yeah, I have to get up every night, you know.

Steve: Yeah. And but what's cool is you wake up, and this, you're able to go back to sleep, rather than just being like, oh, I guess it's time to go visit my friends at Starbucks.

Leo: Or worse, which most of us do, oh, where's my phone? I want to spend a few hours staring into it.

Steve: Yeah, yeah. Good, I'm so glad.

Leo: Not good for your sleep at all.

Steve: So a real quick tip for anyone setting up Windows 7 systems. As I mentioned, I don't remember if it was before we began recording or not. But Greg's ThinkPad Lenovo, actually it might not have been a Lenovo, I think it's an IBM ThinkPad T60, which he's had for, I don't know, like 10 years, it's beginning to get a little wonky. So he said, hey, you know, I really like this. All the new laptops are flimsy. What can we do? So we got a couple refurbed ThinkPad T60, actually a T61 and a T61p, off of eBay for a couple hundred bucks. And I said, you know, I'll put Win7 on them. I pay Microsoft for the privilege, $2,500 a year to be a developer. So I have licenses.

Oh, my lord. What a challenge. And here is what I learned. This is the tip I wanted to pass to our listeners because I know there's a lot of people who are staying with 7 because they don't want to go to 8 or 10. What's happened is Windows Update has changed a lot since the last service pack of Win7. So when you're installing a new Windows 7 system, you're installing Windows 7 with Service Pack 1. The problem is, even that is so old that it gets confused when you tell it to use Windows Update to bring the 250 things that have been updated since.

So what you have to do, and it doesn't seem to be - two systems, the big one I mentioned building recently, that didn't have a problem. But the laptops, one was a 32-bit, and one was a 64-bit Win7. They both got lost. The secret is go and get the update to Windows Update manually off of Microsoft's site. You can just - you can download it. In fact, I downloaded it with my main Windows XP system, and Microsoft showed me a warning, wait a minute, you can't use this on this antique operating system you're using.

Leo: How dare you, yeah.

Steve: And I said, I know, I know, just let me have it anyway. So I got that after another fresh install of Windows 7. Oh, and you have to take it off the Internet. Don't let it touch the Internet because it'll start trying to sniff Windows Update and get confused. So after it first boots, with it off the Internet, you manually install the update to Windows Update. That then brings it current, and then you can let it run from there. So just a little tip, for those of us creaky old farts who refuse to go forward because, gee, Windows 7 works just fine. It holds our files. It runs our applications.

Leo: It's still supported. I mean, they haven't stopped supporting it, so you're okay.

Steve: Yeah, true, true.

Leo: Soon.

Steve: I think I'm going to skip that one because I'm getting tired, and we're running out of time. So I did want to mention SpinRite. This is a fun story, another kind of a - the subject, "Oddball SpinRite Story," comes from Rick Harvey in Melbourne, Australia. He said, "Hey, Steve and Leo. Did you know that SpinRite can save your power bill? Yes, this is bizarre. But I'll let you try to work out why." And actually I know why. But he says: "I have an old, sentimental testing laptop, a Dell Studio, that pretty much spends its day idle, sleeping between test runs. But annoyingly, it's always running the fan. Task manager shows the CPU barely getting off the baseline. I've never even tried reinstalling the OS." Oh, no, he says "I even tried reinstalling the OS. No difference. Just noise and heat. Not so great during the summer.

"I bought a copy of SpinRite last year, just to support your show and give you the pleasure of a yabba dabba do. So it finally occurred to me to give that machine a spin, also because I'm curious about your SpinRite powerhouse fitting into just 170K of code. So I created a boot USB, and off SpinRite went on Level 4. When it finished, everything was green. I rebooted, and all was quiet. Oh, my god. No more fan running. The icing was a comment by my wife, who hadn't realized the screen was blanked. She quipped: 'So, you've finally turned off that heap of junk?' Shhh. Let's not tell her. Awesome show, yada yada. Best regards, Rick."

Leo: That's awesome.

Steve: And of course the reason is that SpinRite fixed the drive, and drives generate a lot of heat when they are - just by seeking. The act of accelerating and decelerating the head, and moving around, having trouble, causes heat to be generated. So it actually is very often the case that systems run cooler, and we hear this all the time, after you run SpinRite on them.

Leo: Systems run cooler after SpinRite. Just that's good, Steve. We're getting some slogans here for you. We're getting them all in order. All right. Let me get the questions, and we will start. We haven't done one of these in a while.

Steve: We haven't, I know, we've just been busy.

Leo: A listener who shall remain nameless wanted to revisit browser containment, like a nuclear plant. You want to contain it: Hello, Steve. Several months ago I heard an interesting tidbit on one of your episodes about using a browser inside a virtual machine to surf the web so that you wouldn't need add-ons such as NoScript to protect your host system. This was also just after it was revealed that running a browser inside Sandboxie was not a viable alternative since it doesn't prevent the browser from reading potentially sensitive data from your disk and then sending it out to the Internet. Dang it. At the time, you were looking for a lightweight guest OS to run the browser in, and I believe you asked listeners for suggestions. Did you ever find one? What's your current solution for browsing the web?

Steve: So as I said earlier in the podcast, I would be referring to this question of the browser being the single largest problem that we have for security. And we talk about this all the time. We've, of course, famously in the past, NoScript was our solution for blocking scripting. But as sites became increasingly dependent upon scripting to do anything at all, I found myself having to create so many exceptions to NoScript, allowing scripting on this site, allowing it on this site, that finally it's like, okay, this is, you know, not having scripting, while, yes, it's really strong security, unfortunately scripting has become as critical as HTML is to the way the Internet works.

Leo: Yeah. I was telling you that.

Steve: So then, yeah, so then uBlock Origin is sort of the next add-on that we came to, to at least deal with the non-native-to-a-site things, the third-party stuff that a site brings in, being somewhat intelligent, using curated lists of things that we want to not have the browser instantly go and get by default in order to further enhance security. Sandboxie we've looked at, and this listener asked about, and also the idea of putting browsers in an entirely separate virtual machine. The problem with Sandboxie is that it's still in the same OS. And it's got that problem of people being very clever about working around the attempt to enclose it in some way. I'm just - I'm concerned that the sandboxing isn't strong enough to count on. And in fact what Sandboxie was explicitly doing was preventing anything from being written out of the sandbox into the OS.

But what we covered at the time was an exploit where the browser was reading from the OS and sending it off to the Internet. So it's like, whoops. Here's a different exploit. So suddenly it's not that we want to prevent something from modifying the operating system, we want it blinded to the operating system. So then I think where we go is a virtual machine. And one of the problems I have, and this is just me because I'm still running a 32-bit OS, is Windows only gives me access to 3GB of the address space, the 4GB address space. And the various OSes and VMs take up enough of that RAM that it's uncomfortable to try to do a lot of other things at the same time.

My new system has 64GB of RAM, and I went crazy with RAM specifically so that I could have multiple virtual machines, give them each 4GB and still have lots of RAM available, although I don't intend to use that as a browser solution. I do think that a more formal virtual machine which by default creates containment around the browser, that both read and write access makes the most sense. But you still need then a means for moving things in and out of that container, that is, when you want to, because we're downloading things from the Internet all the time. They're going to be in that virtual machine until we move them out. So I don't have a good solution. We've looked at a ton of different solutions through the years.

Leo: There's Qubes. Have you ever looked at Qubes OS? I mean, it's a non-Windows OS, but...

Steve: Right. I have, and it's not clear whether it would be a host of Windows and others. I mean, I guess I'm looking for something more lightweight, something easy to add, rather than, like, changing the fundamental architecture of the whole system.

Leo: Yeah, I mean Qubes, it's my impression that Qubes sandboxes every process entire. I mean, it's just...

Steve: And that's of course Joanna's project, whom we've talked about a lot, Rutkowska, I think it is.

Leo: Rutkowska, yeah, yeah, I think so, yeah.

Steve: Yeah. And she's continued to...

Leo: You know, this is an obvious avenue, and there's a lot of interesting work being done. I've been putting Tails, which is a secure Linux, on a USB key. Or better yet, put it on something that's not writeable, like a CD. It's pretty small, and you can boot to it. And I don't think - I think you can make it so it doesn't have access to the internal hard drive. And then, you know, but again, it's always security versus convenience, isn't it.

Steve: Right. Well, and I forgot to mention one thing that I am doing, and that is I am using DropMyRights.

Leo: Ah, good idea, yeah.

Steve: Whenever I launch Firefox - which is still my go-to browser, mostly because it lets me have 400 tabs open. But when I launch DropMyRights, I'm actually executing DropMyRights through a shortcut which then launches Firefox, the Firefox process, with reduced rights. So if something misbehaved, it would have lower rights on the system. And exactly as we were talking about at the top of the show, what you really want is the process to have as few rights as it can possibly get away with. So that really is a good option for browsers running in an environment that have more rights than they need. Running through DropMyRights can give you a lot of security.

Leo: Yeah. Wes, New Jersey, corners Steve - oh, seems like a bad idea, this man's had a good night's sleep, I'd be careful - with a terrific HTTPS man-in-the-middle conundrum. I'm sorry, I lost my confidence for a moment. Steve, I recently started listening to your show, and I thoroughly enjoy it. It helps me keep up on what's happening in IT security and perform my job better. I am a systems engineer for a managed service provider. Network security is a big part of my job.

Something you brought up in Listener Feedback #227 left me with an uneasy feeling. You were discussing how Firefox was having issues with man-in-the-middle proxies issuing SHA-1 certificates. As we know, these devices are used to break

HTTPS connections to allow the inspection of their traffic for malware and other blights. You stated you'd no longer like to see these devices used.

Yet the very next topic you brought up was attackers now using HTTPS sites to host malware. Secure sites for malware. We've set up these devices in the past, and they can be configured to bypass banking and other sites where personal security is a must. If you don't believe these devices should be used, what do you recommend as protection against malware hosted on secure sites?

Steve: So as I said, it's a great question...

Leo: Good point, yeah.

Steve: ...that I really do feel sort of corners me. And so here's the answer. The world is going HTTPS. Corporate networks have, I think, a defensible right to break users' security, that is, break the connection security for traffic inspection. And this puts us back to the discussion we have traditionally had earlier about just the idea of what employees of a corporate network have a right to expect in terms of privacy using that network. And we've talked about companies sticking a label across the top of the monitor, reminding them that they're using corporate property on a corporate property network and corporate property bandwidth, so behave accordingly. So I think where we're going to end up is that these devices, these appliances, are going to be used. Users in a corporate setting have to then be aware of that and alter their behavior, if they choose, with that awareness, not to do things which are sensitive.

Leo: Like your banking.

Steve: Exactly. Do it at home. Wait, you know, wait till you're not on somebody else's computer, by definition your employer's computer, using your employer's network and your employer's bandwidth. It has to be recognized that, for the legitimate needs of corporate security, the traffic is going to be inspected. And so be aware of it, and then modify your behavior. I think that's the right answer.

Leo: There you go. Because, I mean, he makes a great point. It's completely legitimate that they should be monitoring that kind of activity. They have a right and a duty to protect their network.

Steve: Yup.

Leo: Matt in London shares his secure, uh-oh, two-router solution: I've placed my guest network behind my safe network, as you suggested, so I can sniff the traffic of my guest network from my safe network. My safe network is protected by the various attacks you noted because my interior guest network router blocks all outbound traffic except TCP 80 and TCP 443. That's HTTP and HTTPS. So no scan of the middle network is possible except for those two ports. Ping and traceroute, not possible. ICMP is not permitted. And as you have noted, ARP does not cross IP routers. Wow, there's a lot of acronyms in there.

Steve: And that's actually a very clever solution. So what he's done hadn't even occurred to me because I was being so absolutist about this. To the degree that Internet of Things (IoT) devices use port 80 and 443, that is, if they are using HTTP and HTTPS, and I haven't looked, but I'll bet most of them do because those are always available as safe ways of getting out to the Internet. Browsing is like, if there's any set of services, it's your web browser. Even if you can't use your email because your ISP is blocking port 25, you can use browser-based mail like Gmail, for example. But the browser always gets out.

And so, if our IoT devices are using HTTP or HTTPS, and if the interior router has the provision, and you'd have to make sure - and I meant to fire up a blue box, a Netgear router or some standard $40 consumer router, to see because I'm not sure, I haven't looked for a while, what class of routers or how available explicit port blocking, basically you're setting firewall rules, not for what's coming in, but for what's allowed out. So you'd have to have a router that gave you the ability to block all outbound traffic except traffic going to port 80 and 443.

The reason that's so clever is that most users on their middle network, their safe network, aren't going to be running web servers. So they probably don't have any vulnerability there. And you've constrained the possibly worrisome IoT network only to have access to web servers. Which means that nothing in there can scan your network or get up to any mischief.

So anyway, Matt in London, that's a clever solution. It does require a router that provides a kind of firewall which is, I think, less common, which is not inbound blocking, but outbound traffic blocking. But if you've got that, turn off ICMP, block everything except 80 and 443, and see if your light bulbs still work, and other stuff still works.

Leo: So IoT devices usually just use port 80 or 443.

Steve: Yeah, yeah. And so I think this is...

Leo: They're not using some special protocol.

Steve: I think this is so - it's so clever, is that, by tightly constraining what the interior possibly insecure network can do, it can live inside the network you really care about and not get up to any mischief.

Leo: Very interesting. Well, I've put this up on the screen so people can take a picture of it and figure it out for themselves. Debra B. in Cincinnati wonders where, Steve, do we draw the line? When you talk about Internet of Things (IoT) security and the need to create isolated networks for the higher risk, cloud-connected devices, should I include my AV equipment, my Smart Blu-ray player? Yeah, my AV receiver goes online. Anything. TV. Anything that goes online. Or is this an issue mostly for the inexpensive stuff? Or where do I draw the line? Does that include Roku?

Steve: So, okay. There isn't any hard-and-fast rule. I would say, if you don't need to connect to it, then let it go on, stick it over on the IoT network. For example, certainly the Roku needs the Internet. But all it needs to be able to do is get out and connect to the Internet. So unless, for example, you're using it to stream to other devices inside your primary network, your secure network, then, yeah, stick it on the IoT network.

So I guess where we draw the line is that it is better to put those things on the insecure IoT network than not. So if they work there, leave them there. And if you need something from them, or they don't work there, then bring them into your main network. So it's sort of like you've got two places they can go. If they can run over in the sequestered safe zone off of your main network, put them over there. Smart Blu-ray player, probably perfect place for it. Roku, probably the same thing. Light bulbs, definitely.

Leo: Very interesting. Moving on to Question 5, this is a long one. Buckle your seatbelts: Kris Chaplin, High Wycombe, United Kingdom wonders where he should put his NAS drive? Hello, Steve. Thank you and Leo for many years of Security Now!. I have enjoyed many a deep dive propeller episode over the years, and I've been fortunate enough to visit Leo, both at the Cottage and the Brick House. Thanks for your hospitality! Well, you're welcome. Thank you, Kris. Your podcasts have also been a worthy weapon in threatening my kids to go to sleep in the evening. For them there is nothing worse than being subjected to your informative podcasts, and they have been known to fake sleep just to get me and my iPhone to leave the area.

Steve: Oh, I love that. I think that's so funny.

Leo: Here's a little bedtime story, kids.

Steve: The Security Now! sleeping pill. Threaten your children with listening to us.

Leo: Yes. I recently purchased a 3TB Western Digital "My Cloud" NAS hard drive, which I am using as a local backup for my Mac as well as a DLNA server for our smart TV. I've turned off all external access, as that just sends shivers down my spine. Hopefully that and being behind a NAT router is enough to provide reasonable security for our files. I hate to think of the bit-density of that beast of a drive - yeah, 3TB, and how many platters, five, three, four?

Steve: Not enough.

Leo: And I haven't cracked it open yet to see the interface should I need to transplant it into a PC should SpinRite ever need to be used. Hopefully not, but you never know. I have a bit of a fun/odd question for you regarding the location of my backup drive. In an ideal world, I'll be following the 3-2-1 backup strategy - I mention that all the time, that's a Leo, not a Steve, but I'm sure you agree - the idea of having three different copies of everything on two different forms of media, one of them offsite. Indeed a lot of my data is backed up in the cloud. However, some data is just too big and cumbersome to do this with. Yeah, I could store this offsite and should do so. I'll slap my wrists in advance of you reading this and promise to sort it out before I suffer catastrophic data loss. If someone would be kind enough to let me know just before this happens, I would be obliged.

Steve: Yeah.

Leo: I have CAT5e throughout the house - yes, I'm the typical geek you've acquired through episodes of Security Now! - and as such I have a lot of flexibility in the location of my NAS. This has led me to wonder where in the house is the best place to put it? One possible location would be up in the attic - the "loft," as he says. This would have the benefit of being a nice cool space, no disruption, and potentially the last place to catch on fire. Hmm. Out of sight, out of mind. I'm also aware that, if it starts making nasty "I'm about to die" noises, I won't hear them.

Another idea is on a shelf right next to the front door. Yeah, I've even got a socket there. Man, he's really thinking ahead. This would have the benefit of grabability should we be in the house when said catastrophe happens. I could pick up our data on the dash out of the door. But then, so could a thief. The final place, I could put this is in "mission control," where all the networking cables aggregate. This is in the small brick cupboard next to the heating boiler, so I think I'll rule that one out as not a good idea.

Is there an ideal place to put a NAS hard drive in a house for the best chance of longevity? Also, the casing stands the drive vertically. Do you have any preference to how the drives should be oriented, vertical or horizontal? Or does it not matter? Many thanks and regards, Kris Chaplin, proud SpinRite owner, FPGA SoC expert, and general unscrewer of things that are not yet broken. A true geek, in other words.

Steve: Okay. So it's funny, when I first started to read this, it's like, where should I put my NAS drive, I thought he meant, like, where to connect it in the network. And then I realized, oh, no. Like above the fireplace?

Leo: Where in the house, yeah.

Steve: Yeah, exactly. So, okay. Last thing first. Drives that are standing on end always make me twitchy. So absolutely lay it down flat because then it can't fall over.

Leo: Is that the only reason? It doesn't have to do with the sideways drive, thought; right?

Steve: No. And in fact...

Leo: Although I've heard you should format it in the orientation it's going to live in for some reason. I guess that would...

Steve: Yeah, once upon a time. But now we've got servo tracks, and so that compensates for any bias. And the drives are carefully designed by the manufacturers to have no gravity bias. They don't - you don't want to run them, like, longwise up and down. But whether they are flat or vertical, they don't care.

Leo: Good to know.

Steve: And so, but while it's vertical, it could always go flat. And that wouldn't - the drive would not like the bump when that happened.

Leo: If it has a good stand, it may not matter.

Steve: Well, yeah. And so the first thing is I would say, given a choice, horizontal, so there's nowhere for it to fall to. And then, secondly, probably nothing is more important than temperature. Of every other factor, you want it to be in a cool place. And I worry a little bit about these external drives and their fans because manufacturers try to have them be silent and try to, like, let them be convection cooled, or maybe just use an aluminum housing where the housing will hopefully be kept cool. So if there's anywhere to put it with a breeze, that would be really good because you really want to take the heat off the drive. And as for not being able to hear it, I think that's secondary.

What you should be attuned to, wherever you put it, is it seeming to be slower in its response? That's the sign, I mean, what we're seeing is drives slowing down is like the pre-SpinRite phase, where someone says, well, you know, the computer's booting a lot slower. They run SpinRite, now it boots fast. Similarly, when these media drives start to slow down, you know, I've been using TiVos for years. And they have big drives in them. And when you start pressing the button, and it takes a while for it to do something, and it didn't used to take a while, almost invariably, if you stick your ear on the case, you'll hear [screeching]. And that's, again, time for SpinRite.

So I would say make it so it can't fall over. If there's any way to give it the lowest temperature environment, hopefully with some air flow around it to take away the hot air that it has heated up and bring in new cool air, and then, thirdly, rather than listening to it because, I mean, you really have to have your ear on it in order to hear anything, I would just be attuned to the performance of the drive, which you'll be able to sense through the network if, like, you know, if your show that you're playing back starts to stutter. It's like, uh, whoopsie, you know, unless Junior is playing some high-bandwidth online game at the same time, thus bogging the network down, it could be the drive that's giving you some early signs of trouble.

Leo: Good to know. William Burlingame in Huntsville, Alabama wonders about firewall subscriptions: My son-in-law is a partner in a two-doctor family medical practice in a small rural Alabama town. Their previous IT consultant had them buy a Sonic firewall unit. The unit came with a two-year subscription that has since expired. They hired a new consultant who was concerned that the subscription was no longer up to date. Why should there be a charge for updates, Steven? It doesn't seem to me that firewalls have the same problems that antivirus programs have. If an update for a firewall is needed, I assume they have a bug in their firmware. Bugs should not require a fee to correct. My question is, is it a catastrophic problem if they don't keep their subscription up to date?

Steve: You know, this reminds me. Anyone who has trademarks, I'm sure you have seen this, Leo, you get letters in the mail from bogus companies, telling you that your trademark is due to expire.

Leo: Yeah, but we can help.

Steve: Yeah, send $860 to this address, and we will renew your trademark. This strikes me as old-school. Once upon a time a firewall was like, ooh, do you have a firewall?

Leo: Fancy.

Steve: Yeah. Is it big? Is it painted red? Yeah. I think William's intuition, listening to the podcast, is right. I'm sure that Sonic would love to have an ongoing subscription...

Leo: All of them do this, by the way. Everybody does this.

Steve: Yes.

Leo: And we pay them. We pay the fees on ours.

Steve: Okay. Now, if it's also doing malware and virus mitigation...

Leo: Which it is; right.

Steve: ...and filtering, then certainly you need to pay in order to get that service. And, for example, Astaro, who was an early sponsor of the show, you could do that, or you could use the free one. And so my sense is, if it's just a firewall, they will still try to get license fees from you, I mean, because, hey, maybe you'll send them a check. Why not? It doesn't hurt to ask; right?

But, no. If it's not doing AV stuff, then - well, and the other thing is, remember that once upon a time a non-TLS intercepting firewall could inspect traffic. If this has been around for a while, it's not even able to see the traffic going by any longer. So it can't filter it unless all of your machines have its certificate, and it's signing and impersonating the websites on your behalf, which is unlikely. Which means it's probably useless even if it was doing AV stuff because nothing's in the clear anymore. So, I mean, I don't want to give a blanket prescription without knowing all the details. But my intuition says, eh, Sonic would love to get a check from you. And it probably does you absolutely no good whatsoever.

Leo: Wow. All right. I'm going to go talk to Russell right now, say stop writing those checks. Emily in Reno, Nevada wonders how IPv6 figures into the IoT NAT routing thing? You know what I'm talking about. Steve, over on the TWiET podcast - that's Father Robert Ballecer's Enterprise Tech podcast - there was a lot of talk about IPv6 actually starting to come to life on the Internet. I think you mentioned 10%, right, of the Internet is using IPv6. But I'm wondering if you could explain how IPv6 and our security reliance on NAT will play out.

It seems that with IPv6 the concept of NAT may be going away because of the huge number of available addresses. I know that NAT was originally designed to help mitigate IPv4 address exhaustion, but now we rely on it for security, as well. Will every IoT device eventually have its own public IPv6 address? That seems like an awful idea. Please help explain what we should expect with IPv6, IoT, and NAT.

Steve: So it's a really good question. I've already seen some discussion of NAT routers not NAT'ing IPv6, that is, for IPv4 they provide the standard NAT and local DHCP. For IPv6, they pass it through. So if a device gets an IPv6 address, it's getting it from the ISP rather than from your local device. Meaning that, in fact, routers are not routing any longer, essentially. They're just bridging the ISP's network into your network and not providing any of the security that we're traditionally used to having. That's a horrifying idea.

Leo: Yeah.

Steve: So we're in the early days. But what we really need is not necessarily NAT, but what used to be called like a "stateful firewall." We went through a phase, remember, when the NAT routers were boasting that they did deep packet inspection or stateful inspection. And it was like, what? It's a NAT. Of course it's stateful. And you don't need anything more than that. So even if this thing, I'm not sure what we're going to call it because it's not a NAT, and it's not really a router. So we're stuck. We're going to need a new term of art here. But this thing that you have in your house that is running on IPv6, it will presumably have the ISP allocating per device IPv6 IPs because you get a block of, typically, a 16-bit block. Maybe it'll do it locally. I mean, a lot of this is unclear. But this idea...

Leo: Do you think it'll ever happen? I mean, are we preparing for something that's never going to happen?

Steve: Yeah. Where are we? We're at Episode 549. Before we reach three or four digits, I don't know, Leo. I don't know.

Leo: I mean, we've got ISP route NAT now, which is kind of eliminating some of that crazed fear. I just wonder, you know?

Steve: Well, our OSes all have IPv6 stacks in them now.

Leo: Yes, yes, yes. We're ready.

Steve: So if you were to put - yes, exactly. If you were to use a NAT router that was IPv6-aware, and your ISP responded to IPv6 DHCP, that is, if it was provisioning IPv6 on that connection, it would presumably come up and run. And so the concern is, are we then relying on our OS's firewall? The good news is Microsoft finally turned them on by default. And the Mac's is on, I think the Mac's is on by default. It must be.

Leo: No, 'tis not.

Steve: I'm glad I asked, yeah, so it isn't.

Leo: Nope.

Steve: Ugh. So, yeah, we need border security. We need something which is stateful, meaning that it sees something outbound to a certain IPv6 address. And it then allows return data from that IPv6 address back to the same IPv6 internal address that generated that mapping in the table. Essentially, NAT without NAT. I mean, no translation, but a stateful firewall is what this would be. And we've never had the need for it before, but we need it now. I mean, certainly the OS firewall provides that. But I would - I'm belt and suspenders in this case. The appliance on the border, it should not allow random scans of, like from Shodan, of the IPv6 known allocated ISP space to penetrate people's LANs and just be poking around at their light bulbs. That just seems like a bad idea.

Leo: There are security benefits to IPv6, though; right?

Steve: Well, I mean...

Leo: Like for instance the DDoSing that we're experiencing. If we were on an IPv6 network, could you do raw sockets? Could that spoofing still happen?

Steve: Yeah.

Leo: It could.

Steve: Yeah. So spoofing still happens. You have a known address. One argument is that scanning the 'Net becomes more difficult because you've got way more than just four billion IPs, as you have in IPv4. On the other hand, the ranges of IPv6 space, which ISPs would be known to be allocating, that would be known. All users contacting websites through their IPv6 address would have their IPv6 address known to the website. So these are secrets that cannot be kept. There is no way to keep your address secret, whether it's IPv4 or IPv6, because it's the address that is the way that...

Leo: That's how you talk. That's your name.

Steve: That's how you get found on the Internet.

Leo: Yeah.

Steve: Yeah. There are other, you know, once it really begins to happen, we'll do a series of podcasts on IPv6 because, for example, IPSec security is built in, instead of being a layer added afterwards.

Leo: Oh, that's nice, yeah.

Steve: And there are a lot of good things that have been done with the move from v4 to v6. Which will happen, or will be good if they happen. So, but, boy...

Leo: Episode 1000 we'll be covering that.

Steve: That's right. That'll be the commemorative IPv6 episode.

Leo: Remember IPv4? What was that, Grandpa? Oh, you don't want to know.

Steve: So simple, I actually knew what my IP address was.

Leo: I knew it. It was only a dotted quad. Bill Russell, no, I'm sorry, I was thinking basketball. Bill Rakosnik near Athens, Georgia wonders about configuring DHCP for three dumb routers. Be a great TV show, my three routers: I don't have any formal computer network training. Almost everything I know about computers I've learned from shows like yours and research on the 'Net. Long ago, after you first mentioned it, I experimented with your three dumb router method. However, it didn't just work out of the box.

After reading some more online, I don't remember exactly where, I turned off DHCP on the two interior routers connected to the primary outside-facing router, and then manually assigned IP addresses to the two interior routers. Once I did this, it did work. By doing this, I believe only the primary router is responsible for assigning IP addresses on the entire LAN. However, I also suspect I'm not getting the security benefits of the three dumb routers. Or as we call it now, "Steve Gibson's Three Dumb Routers." Is that the case?

If that's the case, why didn't it work with DHCP turned on? To get the benefits of three dumb routers, do we have to leave DHCP on and configure each router to be responsible for its own separate segment of IP addresses? By turning off DHCP have I essentially turned my secondary routers into dumb switches? If not, what is the difference between a router and a switch? I've always been surprised that my secondary routers have IP addresses, but switches do not.

Steve: Okay. So I'm responsible for leaving out that important detail when we talked about three dumb routers. I didn't want to overwhelm our listeners. I felt there was already - we were talking about ARP spoofing and ARP broadcasts and ARP not going across routing and bridging and all of this. And I thought, okay, you know, enough for one podcast.

The problem, and I did touch on it later, and I want to make sure because I've seen some more confusion about this, the problem that Bill had, which he solved by turning off DHCP for the router, the interior routers being assigned the WAN IP, is that, as I did mention, we essentially have three networks. We have the network which connects the three routers together, and then we have each of the networks behind the two interior networks.

What is critical is that the IP addresses of those networks, the network IPs, be separate because the router, what it routes is it inherently routes between differently numbered networks. So 192.168.0.1, like from 0.1 to 0.255 would be one network; then another one would be numbered 192.168.1.1 to 1.255; and the third one, 192.168.2.1 to 2.255. The idea being that the networks cannot overlap their address space. That way all the routers know whether the packets are moving around in their own network or whether they're bound for a different network. And if they're bound for a different network, that's when they send them through the router out to the other side.

So the problem with DHCP is it wasn't designed for the three dumb router mode. And it might have been that the main exterior router was assigning IPs to the interior routers' WAN ports that were the same network as those routers were assigning to their interior WANs, I mean their interior LANs. And if that was the case, they would have been confused because they wouldn't have known to send packets out into the world because the network on both sides would have the same numbering. They need to be differently numbered. Then the router knows, oh, this packet goes over there, this one on the inside goes on the outside, and so forth.

So, Bill, to answer your explicit question, that's why it didn't work, why doing what you did fixed it, and your security is perfect. None of this dumbed down your routers or turned them into switches. It just allowed them to know where to send the packets, which is the part that was missing because it probably had LAN numbering that was colliding. And so just giving them their separate, each one, each of the three networks separately numbered eliminates all confusion.

Leo: Some routers, like Apple routers, use 10-dot. And then Linksys and others use 192. Those two shouldn't have a problem; right? They can tell the difference.

Steve: Correct. You could completely use, like, the other - there are three, what is it, RFC-1937, 1937? There's an RFC that...

Leo: Private address. Private addresses.

Steve: Exactly, that lays out the nonroutable, the three now-nonroutable addresses. I use 10-dot both at GRC's internal network and here at home, and then have subnets within that.

Leo: Too bad there's not one more unroutable subnet. Then you wouldn't have to worry about this.

Steve: Well, the problem is...

Leo: Used to be 5.5, right, but you can't use that anymore.

Steve: The question is what do the routers default to. So if the hardware routers themselves use 192.168, and as far as I know they all do...

Leo: Supposed to, yeah.

Steve: Yeah, then you're going to have a collision, and you're going to need to step in and do a little manual overriding.

Leo: Right, right. Jim in Chicago, a great tip for security-conscious Chrome users: In Show 486 - 486, that was a long time ago - you covered how Google proposed that web browsers "change their user interface to display nonsecure origins as affirmatively nonsecure." I think they did this. They were planning to do it.

I'm unsure when Google added this to Chrome, but it is currently available. At the moment it's disabled. Oh, I didn't know that. However, it's very easy to turn it on. In the address bar, enter the following, chrome://flags, and then search for a setting named "Mark nonsecure origins as nonsecure," and restart Chrome. And now, whenever you go to a website that's using a nonsecure connection, you'll get a red "X" in the address bar. You're going to get that soon enough, I think. I think that's the intent. I thought your listeners would appreciate this tip. Keep up the great work. P.S.: Looking forward to the next season of "Mr. Robot" and "The Expanse." Jim.

Steve: So anyway, I just wanted to share that tip. Right now I think maybe is it a little - maybe there's no marking at all on non-HTTPS. I know Chrome complains all kinds of ways about HTTPS certificates it is not completely enamored with. But what this would do is, you know, this would really bring to your attention that this site you were on was HTTP. And so this is like, again, Google staging their security. But I kind of like it as just to - as long as you know that it doesn't mean anything is wrong. The problem would be, and this is why it's not enabled yet by default, is it would scare lots of people, who would think, oh, my god, a red "X," you know, run away, run away. But our listeners know enough to, if they turn it on, it's helping them notice that this is not HTTPS. Which is fine within the limits of what behavior you're asking for from the site.

Leo: Right.

Steve: Nice tip.

Leo: Good tip. One more. You ready? Oh, no, I lied. Few more, but they're short.

Steve: Yup.

Leo: Neal Fildes near Cincinnati, Ohio wonders about ShieldsUP! for IPv6. Have you considered it?

Steve: So, yeah, I've mentioned it a couple times, but lots of people are asking. And I will tell you very honestly, and everybody who's waiting for SpinRite 6.1 will be glad to know, that I will spend no time on ShieldsUP! for IPv6 until SpinRite 6.1 is in everyone's hot little hands.

Leo: And then...

Steve: But I absolutely look forward to doing it. There's nothing I would like more except getting SpinRite out the door. So yes, in the future, no commitment. You've got to know by now that I can't commit to when. But it's definitely on the list of things that I think would be fun to do.

Leo: Good. And Paul Erskine (@paulerskine) tweets this question: @SGgrc Like DVD players, keys to open iPhone are in device, no? I think - this is a tweet, that's why there's missing words - think one could physically access Secure Enclave with expensive tools?

Steve: And so I thought this was an interesting point. Paul was asking, he said, you know, we've often talked about how DVD players are inherently unsecurable because they need to be able to decrypt the DVD.

Leo: Yeah.

Steve: What Paul is missing is that the DVD player is not asking its user to provide a secret that it doesn't have. That is, it's able, and it's not having to go out and contact the Internet to get it or do anything else. Internally, all by itself, it knows how to display the images of the DVD. So it is impossible to protect it.

Where the phone is different is it is relying on information the user provides that it doesn't have. So that's an important distinction to make is that the iPhone, and this of course is why the only thing the FBI can do in this case is guess. It's asking Apple to make it feasible to brute-force guess every possible passcode until they find the one that works.

Leo: Finally, the bonus question. Jason's subject line caught your eye, Steve? It would have caught mine: You would love my wife's legs.

Steve: It was sitting there in my email. I thought, wait a minute.

Leo: Uh-oh, spam.

Steve: I mean, and it's surrounded by "When are you going support IPv6 on SpinRite?" And there's, "You would love my wife's legs." And I thought, what?

Leo: Uh-oh, what? Well, it turns out he's talking about Harry's: I purchased a Harry's razor a few years ago based on your testimonial. I love it, works great on my bald head. Now, my wife had been shaving her legs with rusty butter knives for years, so I offered her a fresh Harry's blade to try. She loved it, and now that's what we both use. Thank you. Her legs are more amazing than ever. She begrudgingly credits you for it, but she still won't let me listen to you guys around the house. She says you sound like Charlie Brown's teacher. Remember the teacher? "Wa wa wa wa wa, wa wa wa wa wa, wa wa wa wa." You guys are the best. Thanks so much. Listening for years. SpinRite. TLDR. And, if you read this on the air, please tell my wife, Grace - Grace? - how bad of an idea it is to log into her email on a public computer in a hotel lobby.

Steve: [Crosstalk]

Leo: But she's got great legs. No? Shouldn't do that?

Steve: Yeah. Good legs, but bad security practices. Nothing worse you could do.

Leo: Really.

Steve: Nothing worse.

Leo: The worst.

Steve: Listen to your husband Jason. You trusted him with his razor, now trust him with the security advice.

Leo: There is a reason why all that "wa wa wa" has been going on in your house for so long.

Steve: That's right.

Leo: So that he could learn these things and protect you. Steve, what a fun show. As always, a great pleasure. You can catch Steve on his newly functional website. I shouldn't - I don't even want to say anything. GRC.com. That's where he stores, not only all that great stuff, SpinRite, the world's best hard drive maintenance and recovery utility, all the freebies he gives away, all the passwords and everything, and SQRL is going to be there. But it's also where he puts 16Kb versions and 64Kb MP3s of the show. He puts really nice transcripts that Elaine Farris writes for us. And so you can see it all there, GRC.com. We, on our site, TWiT.tv/sn, have audio and video of the show. It's great to look at Steve's happy face. And, by the way, he has great legs. Well, they're well shaven.

Steve: No.

Leo: No. Let's not talk about it. I have no knowledge. I have no knowledge of the subject. But TWiT.tv/sn or, you know what, it's everywhere, on all the Internet stuff, including YouTube and all the podcatchers, and of course our free apps everywhere, and paid apps everywhere, and it's just - it's all out there. Just get a TWiT app and listen and subscribe because you don't want to miss a single one of these. They're all valuable. Save them. Save them. Because it's really, it's an education in a box.

Steve: And there is some neat news happening later this month. We're getting a direct flight between my airport and your airport.

Leo: What?

Steve: Which makes it much easier for me to come up and play.

Leo: That is good news, or for us to do the same. That's great. Yeah, we have to fly to LAX when we leave Santa Rosa now.

Steve: Right, right.

Leo: But if we can go - what is your airport?

Steve: They call it, unfortunately...

Leo: John Wayne?

Steve: Yours is - mine is John Wayne, and yours is Charlie Brown or something.

Leo: Yeah, Charles Schultz.

Steve: Charles Schultz.

Leo: The creator of Charlie Brown of "Peanuts" is from Santa Rosa, yeah.

Steve: Yeah. So we'll go from the John Wayne to the Charles Schultz.

Leo: So that's nice because it's half an hour from here. It's easy parking.

Steve: Yeah, I mean, the problem is it's just so difficult for me to get up to Petaluma.

Leo: I'd love to see more of you.

Steve: And so you're going to be seeing more of me.

Leo: That would be - I'll tell Lisa. She'll be thrilled. And we'll start stocking up the cabernet.

Steve: Yeah, I can't carry it onboard, unfortunately.

Leo: No, no, that would be coals to Newcastle. You're coming to Sonoma and Napa.

Steve: Ah.

Leo: Right?

Steve: Got it.

Leo: Thank you, Steve. We will see you next time. Every Tuesday, 1:30 Pacific, 4:30 Eastern, Security Now!. Take care.

Steve: Bye.