Listener Feedback #222

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-533.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-533-lq.mp3

SHOW TEASE: It's time for Security Now!. It's Patch Tuesday. Steve will talk about the latest from Microsoft. Of course security breach after security breach. Talk about all of that, the ProtonMail problem and all that. And then we get to 10 fabulous questions from you, our viewers. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 533, recorded Tuesday, November 10th, 2015: Your questions, Steve's answers, #222.

It's time for Security Now!, the show that protects you and your loved ones online with this guy right here. He's the Explainer in Chief, Steve Gibson. And a good day to you, Steve. How are you?

Steve Gibson: Great, Leo. Great to be with you again. This is 533 episodes on the day before what we think will be the iPad Pro release. And if nothing else, tomorrow is 11/11, so that's kind off fun.

Leo: Yeah.

Steve: So this is our Listener Feedback episode, #222.

Leo: Wow. Even that number is getting big.

Steve: Yeah. Lots of interesting stuff. We have news of China having a new hiring

problem, brought to us, I'll warn our listeners, by The Onion, but it's hysterical. An update to Firefox with some news. Lots of news about sort of various ransomware and Internet extortion which has come to light. Some certificate authorities issuing banned certificates. Microsoft has announced in a blog posting that they're giving serious consideration to changing their own famous SHA-1 cutoff date in lieu of the recent concerns about SHA-1 integrity moving it forward. We'll talk about that.

And I actually have an overflowing cornucopia of fun miscellaneous stuff. Some software tool recommendations, too. Some things I realized I've been using, I've been really happy with, that I want to make sure our listeners know about.

Leo: Good. Good, good, good.

Steve: So lots of great news. And then, of course, let's not forget, 10 interesting ideas, suggestions, thoughts, questions from our listeners.

Leo: All right. Security news, always a thrill.

Steve: Always an adventure.

Leo: Always an adventure.

Steve: I will refer our listeners later back to the Picture of the Week, which is...

Leo: I can show it now, by the way. My system is back.

Steve: Well, okay. This is a screenshot of a utility that will I think be of extreme interest to Windows 10 users who are concerned about the monitoring features built into Windows 10. And of course we've heard that Microsoft intends to port these back into Windows 7 and 8. So this is from people we know well, the Spybot Search & Destroy people. They've got a new utility, Spybot Anti-Beacon. That's hyphenated.

Leo: Oh.

Steve: A-N-T-I hyphen B-E-A-C-O-N. It's now at v1.2. And so, for example, it lists all of the things that it does on its status screen. So, for example, telemetry hosts, all blocked. Telemetry services, all blocked. Telemetry group policy, all blocked. And just to make a note, you know, group policy is sort of the underlying sort of super policy that the machine uses, which generally gives much finer grain and much deeper enforcement of things that you see at the UI level. So telemetry group policy, all blocked. Consumer experience improvement program, that's CEIP, group policy, all blocked. Consumer experience improvement program scheduled tasks, all blocked. Application impact telemetry group policy, all blocked. Steps recorder group policy, all blocked. WiFi sense, and then they have in parens (hotspot sharing) group policy, all blocked. Apps use of advertising ID, all blocked.

And finally, something that we actually didn't talk about because I just didn't think it was a big issue, although there's a lot of furor out on the 'Net, and that's the peer-to-peer Windows Updates outside of the local network, all blocked. Some people were concerned, they just didn't - they were annoyed, essentially, that Microsoft was creating a peer-to-peer network, basically to offload the demand on their servers, for issuing all of these updates to the ever-growing number of Windows systems. So they said, eh, let's do peer-to-peer. So that if, you know, the point being your system could be called on to send some of its updates out to other Windows users. And that just annoyed some people. I don't think - I'm sure Microsoft locked it all down so it isn't a way to obviously, in some easy fashion, inject malicious updates. But this lets you turn it off.

So basically, and we'll cover this again later, but it made a great Picture of the Week. I also have a fabulous one for next week that someone tweeted me, and I said, oh, I've already got a good picture for this week. But oh, boy, I can't wait. Because we actually have results from whether tinfoil hats help or hinder.

Leo: The official headgear of Security Now!.

Steve: Yes. MIT, no one less than MIT has done the research that we've been waiting for. What degree of shielding is provided by the tinfoil cap?

Leo: It's a Faraday cage for your brain.

Steve: We'll know next week. In the meantime, speaking of Microsoft, it's Patch Tuesday. And the only thing annoying about the podcast on Tuesday, which I do like as opposed to Wednesday, I'm really happy with this day of the week...

Leo: Thank you, thank you.

Steve: Except that it is when Microsoft is releasing. And they sort of do it in the late morning. So I kept checking and checking and checking. And finally I fired up my Win7 box that I Skype from about an hour ago. And it initially said, no, nothing new. Then, oh, look, I've got 13 patches. It's like, okay, fine. So then I had to go find out what they were, just in case there were any showstoppers. There are not.

Only three of the 13 are flagged critical. The others are important. And the critical ones are not surprising. One you may not need to worry about much, and that's Windows Journal. But that's one. But then the two browsers, Edge and IE, not surprisingly, both have problems that you need to patch. And then there's just a bunch of other stuff that I haven't had a chance to look at because it just happened. So I'll survey them. But, you know, so standard operating procedure is you probably should update as soon as you can. And if you're not using Edge or IE and Windows Journal, then nothing critical apparently.

Leo: What is Windows Journal? I don't even know what that is.

Steve: Yeah. So sometimes these things do relate to core components that other apps use. So again, we've got a really important story we'll get to in a second about the problem with not keeping yourself up to date that's a little chilling. So everyone knows they want to do that.

Now, The Onion brings us an important newsflash from China. The title: "China Unable to Recruit Hackers Fast Enough to Keep Up With the Vulnerabilities in U.S. Security Systems." There are just so many, Leo, there are so many problems over here that they can't get enough hackers in China to take advantage of all the vulnerabilities that exist. They're falling behind.

Leo: They're falling behind.

Steve: We've got unexploited vulnerabilities in the U.S. systems, despite China's best efforts to get in there and exploit every one possible. It's a manpower shortage. So this comes to us from Beijing: "Despite devoting countless resources toward rectifying the issue, Chinese government officials announced Monday that the country has struggled to recruit hackers fast enough to keep pace with the vulnerabilities in U.S. security systems. Quoting them, that is, the Chinese government: 'With new weaknesses in U.S. networks popping up every day, we simply don't have the manpower to effectively exploit every single loophole in their security protocols...'"

Leo: Shocking.

Steve: "...said security minister Liu Xiang, who confirmed that the thousands of Chinese computer experts employed to expose flaws in American data systems are just no match for the United States' increasingly ineffective digital safeguards." Quoting him again: "'We can't keep track of all of the glaring deficiencies in their firewall protections, let alone hire and train enough hackers to attack each one. And now they're failing to address them at a rate that shows no sign of slowing down anytime soon. The gaps in the State Department security systems alone take up almost half my workforce.' Liu complains." That's just a shame.

Leo: The Onion. Don't write to us. The Onion.

Steve: They're busy.

Leo: They're working hard.

Steve: "At press time, Liu confirmed that an inadequate labor pool had forced China to outsource some of its hacking work to Russia." Wow. That's such a sad day for China.

Leo: It's funny because it's probably true.

Steve: So, Firefox 42. I received a dialogue announcing, I think it was yesterday, that,

oh, 42's available. Would you like to restart? So of course I said yeah. And the first thing I noticed was that the menu bar that used to take up some space had moved up into the title bar, which is sort of interesting. I kind of like it up there. So, you know, to give me a little more vertical space.

Just a segue, too. I noticed people talking about Firefox for iOS. And we do have a story in our Q&A about Firefox for Android and the great success one of our listeners has been having with it. But I went looking, I thought, wait, finally, you know, we heard it was coming? It's not available in the U.S. If I were in Finland, apparently, I could get it, and some other places where I'm not. So I went looking, couldn't find it, wouldn't come up. I went back to Mozilla's own report of the countries where it's available. And I don't understand why it's not available here. Do you know anything about iTunes apps and country? Like who cares?

Leo: Well, people do. I mean, every iTunes store is associated with a country. I think it has to do with payments. But even the free apps. So you can, on iTunes, you can go down, and you can change the country of origin and see what the Chinese iTunes store has. I don't know if you can download it or not, but you can...

Steve: There was, there was a dialogue that came up and offered for me to change the country to New Zealand. And I said, ah, you know, I've got to do a podcast.

Leo: That's how things - that's often the case. That's how they roll it out. There are a variety of reasons why you might want to do that.

Steve: So, okay. So Mozilla would be presumably letting countries at a time start using it, see how it goes, and maybe...

Leo: Phased rollout, yeah.

Steve: Right. And then, you know...

Leo: Does it require, I mean, does the new thing require servers of some kind, not just the download servers, but like is there some server component? No?

Steve: Just the web browser. It's Firefox.

Leo: Have you ever seen them do this before? I don't remember doing this before.

Steve: No.

Leo: No.

Steve: Yeah, so...

Leo: I don't know.

Steve: Anyway, we do have on our desktop platforms, available globally, even in China, maybe they can find some problems, is the new version 42 of Firefox. And their big deal, I got a whole page that came up after I restarted, introducing me to the new tracking, the built-in - and this is what's key - built-in tracking protection for their private browsing feature. So when you click on the menu - and they show, like, a little pair of sort of black raccoon mask Mardi Gras disguise goggles as their symbol for private browsing. You click on that, and now what they're doing is they are using the Disconnect database, as are many other extensions. But this is native Firefox, to block the web elements that could be used to record cross-site behavior.

So this is not blocking web content, per se. It's blocking tracking. It's blocking profiling and building a history of your past travels across the Internet when you're in private browsing. Apparently it's enabled by default because mine was on. So under Options > Privacy > Tracking, there is "Request that sites not track you." Of course I had that on. So that's the DNT, the Do Not Track header, which we haven't - the industry's not completely given upon. It's having a rough go of it. But with all of this recent adblocking, sort of the idea of, okay, well, maybe we'll consider honoring that, says the ad industry, even though initially we were just laughing at you. So fingers crossed.

And the other option is use tracking protection in private windows. You can turn it off if you don't want that. But that sort of seems to go along with private browsing is being nontrackable. So, yay for Firefox 42. And they explain: "Tracking refers to the collection of a person's browsing data across multiple sites. The tracking protection feature uses a list provided by Disconnect to identify and block trackers. A shield icon will appear in your address bar whenever Firefox is blocking tracking domains," which is to say we just painted a shield there because we're not going to show that. "To see which resources are being blocked, you can open the web console and look for messages under the Security tab." So that's there now.

They also added an indicator to tabs that allow pages that play audio to be muted with a single click. So if that's a problem for people, this update of Firefox addresses it. And then they did also make some WebRTC and Login Manager improvements. Then a ton of - they're moving forward. They've added some more support for ECMAScript 6 stuff that we were talking about last week, some more HTML5 support, and then a whole bunch of developer features and some security improvements. So that's the tune-up on Firefox.

So we've talked often about ransomware because that's the new big thing. The first time we encountered CryptoLocker, it was very clear that there was going to be more of this. I said it the first week, I said, oh, boy, you know, this makes too much sense. For a decade we've been getting along with viruses that seemed mostly there to be mischievous, to prove that they could. They weren't horribly malignant. Sometimes, increasingly, they were remote-access trojans, or they were bots, so that they just - but even then they were just wanting to use your bandwidth to play king of the hill on IRC chat and so forth. Now, with the advent of encrypting someone's files, it of course famously occurred to these people that they could get some money, so ransomware was born.

Well, the new target of ransomware are not individuals, but websites. Brian Krebs reported the discovery from the Russian AV company that calls itself Dr. Web, that there

is something called Linux.Encoder.1, sometimes called Linux Filecoder and similar names. When Brian reported it, it was almost undetectable by any of the existing AV tools as shown on VirusTotal. If anyone's interested, I have the link in the show notes, and now it's jumped to about 50-50. So the various detection tools are catching up very quickly.

As the name implies, this thing targets Linux web servers. It gains a foothold through using known vulnerabilities in site plugins or third-party software. So this is not a problem with Linux itself or with Apache, which is oftentimes, or maybe Nginx, the web servers that run on the Linux OS. This is a problem with sites that have added other stuff. And of course once this gains a foothold on a server, the malware encrypts all the files in whatever home directories it's able to find, as well as all backup directories and most of the system folders that are typically associated with website files - images, pages, code library scripts and so forth - so basically hoses your web server.

Then, looking at a specific case, which is why I was referring back from the issue of Braintree, a specific site that wasn't disclosed in the reporting that I saw was recently infected and completely encrypted through an unpatched vulnerability in a shopping cart add-on. The software and the company are both called Magento. It's used by - I have it in my notes here, I'll come to it in a second, but as I remember, hundreds of thousands, thousands at least of sites to handle their ecommerce payments. This company was so big and successful that eBay purchased them back in 2011. So this Magento is an eBay-owned company.

So the story is, or the timeline here, Check Point, the security firm, discovered the vulnerability earlier this year and notified eBay - I'm trying to get the time right - notified eBay to let Magneto know about the problem, and they provide them with the necessary remediation and patches. So Check Point, writing about this, said: "Check Point researchers recently discovered a critical RCE (remote code execution) vulnerability in the Magento web ecommerce platform that can lead to the complete compromise of any Magento-based store, including credit card information as well as other financial and personal data, affecting" - oh, here's the number that I was looking for - "nearly 200,000 online shops."

Leo: Wow.

Steve: Yes.

Leo: By the way, Magento does not equal Braintree. Different company.

Steve: Correct, yes, do not confuse the two.

Leo: Yes.

Steve: "Check Point privately disclosed the vulnerabilities together with" - and this is Check Point's writing in their blog posting - "together with a list of suggested fixes to eBay prior to public disclosure. A patch to address the flaws was released on February 9, 2015." Okay. So February 9th was Magento's release of the patch to fix 200,000 online stores.

Leo: I just want to say one thing.

Steve: Yeah.

Leo: Because Magneto is one of the X-Men. It's Magento is the store. Just so you understand. It's like the color magenta.

Steve: Oh, I mis...

Leo: Magneto, I love Magneto, but he's a bad guy. So I just don't want people to - it's Magento, I think. Isn't it?

Steve: Well, that would be M-A-G-E-N-T-O.

Leo: Yeah, ecommerce software and commerce platform.

Steve: Oh, my god. Oh, misspelled it every - I was so sure. You're right. Thank you very much.

Leo: [To the tune of the Farmers Insurance jingle] We are Magento, da da da da da da da.

Steve: Yeah, the Check Point link says "Analyzing Magento vulnerability." Thank you, Leo.

Leo: Yeah.

Steve: So erase all of that. Elaine, please [crosstalk].

Leo: Don't say Magneto.

Steve: Oh, my lord. Okay, Magento. Okay. So Check Point privately disclosed the vulnerabilities. Okay. So they disclosed, they talked to Magento through eBay early in the year.

Leo: This is Magneto. Different.

Steve: Thank you. Yeah, I do know the difference. I just I got it wrong the first time, and then I just replicated it.

Leo: And I was listening, you know, I mean, yeah. I was just going along with it.

Steve: Okay. So Check Point did the responsible disclosure thing. So they waited more than two months. The patch was released to 200,000 Magento online shops on February 9th. Check Point went public on April 20th, so February, March, April. "Store owners and administrators," writes Check Point, "are urged" - yeah, no kidding - "to apply the patch immediately if they haven't done so already." And of course Check Point is saying this more than two months after the patch was available, so they should have done so already. Thus the whole point of responsible disclosure. You wait till everybody's fixed it before you tell the world, hey, we're brilliant, we found a problem.

"The vulnerability is comprised," writes Check Point, "of a chain of several vulnerabilities that ultimately allow an unauthenticated attacker to execute PHP code on the web server. The attacker bypasses all security mechanisms and gains control of the store and its complete database, allowing credit card theft or any other administrative access into the system." And now we know they can also be used, one way or another, to execute arbitrary code because this is how this particular ransomware got in. And then Check Point finishes: "This attack is not limited to any particular plugin or theme. All the vulnerabilities are present in the Magento core, and affects any default installation." So nevertheless, that site, like so many, was behind on updates for third-party applications, including their Magento shopping cart software.

Okay, now, there is a little bit of good news. In case any of our listeners know anybody who has been affected by this, the BitDefender gang discovered that there was a flaw in this particular Linux server ransomware. It has a predictable encryption key, and that's of course one of the core lessons of this podcast is you have to have good random numbers in order for cryptography to work at all. There are exceptions, like, well, no, I was going to say Diffie-Hellman key encryption. But that also depends upon each person, each party generating a really good random number. I have to think about it. Maybe there is no exception to the fact that you absolutely have to have a source of high-quality entropy.

So BitDefender's posting says: "The AES key is generated locally on the victim's computer. We (BitDefender) looked into the way the key and initialization vector are generated by reverse-engineering the Linux.Encoder.1 sample in our lab. We realized that, rather than generating secure random keys and initialization vectors, the sample would derive these two pieces of information from the libc rand() function, which is seeded with the current system timestamp at the moment of encryption. This information can be easily retrieved by looking at the file's timestamp. This is a huge design flaw that allows retrieval of the AES key without having to decrypt it with the RSA public key sold by the Trojan's operators."

And they went as far as, because of the pervasiveness of this - now, let me separate these things. This is the ransomware. And what I was talking about with the Magento was one particular server that did not update its Magento ecommerce package, and a forensic analysis determined that was the route in for this ransomware. So the good news is this ransomware is brand new. The bad news it is infecting Linux machines. No doubt it's doing a scan of the 'Net, looking for other Magento installations, if it hasn't already found them all, in order to get into Linux servers through any other ecommerce shopping carts that haven't been updated. Of course the problem is immediately upon this defect being found it'll be fixed because it's trivial to do a much better job of getting cryptographically strong random numbers. You just have to care. And so...

Leo: Yeah. We've got to get bad guys listening to this show. I think that's the message of that.

Steve: Yeah. And so the bad news is this will get fixed, and there will be then a better ransomware that doesn't have this flaw. But for now, the BitDefender guys did create an automated decryption tool that is available from them. So if anyone's Linux server is hit by this ransomware that gets in through any means whatsoever, not just Magento, but this is targeting vulnerable third-party add-ons that are behind in patching, or maybe with zero-days that can't be patched because no one knows about them except these guys. And we know of course that unfortunately archives of those exist that are available if you want to pay enough.

So now, essentially, ransomware has turned to servers. And of course the reason is that you can probably extort much more money. And speaking of extortion, the final twist on this is, in the wake of the damage done to Sony by the publication of the data that was exfiltrated from their network, the companies behind these web servers that are encrypted are told - and they're normally being asked to pay hundreds of thousands of dollars or euros or whatever currency. If they don't, in order to get their data back, then not only will their data stay encrypted, but the bad guys will decrypt it and post it publicly. So there's also the twist of the data that we've got from you will be published. You will be blamed. So you'll have that egg on your face, in addition to not getting your data back. So, boy.

And the problem is, whereas once upon a time we were, I mean, for years we talked about how sort of paradoxical it was that viruses weren't doing worse, that they weren't doing more damage. I mean, there were exceptions. There was the one that I've talked about that would, like, overwrite your BIOS so that your motherboard would no longer boot. There was the one that wiped out the first meg of a hard drive, and so I wrote a free utility to restore that because I had the knowledge to do that from SpinRite. And so there have been really destructive viruses. But by and large they just sort of seem to want to propagate and, then, more recently, do more. But we're in the era now where it's about money. And the problem is that creates a deeper level of incentive for people to want to exploit. And as unfortunately Beijing has just reported, you know, they can't hire enough people.

Leo: Yeah, yeah, just use that libc, you'll be good. Good stuff. We talked about that years ago, didn't we, the PRNG and libc being [crosstalk]?

Steve: Oh, yeah, I mean, yes. And the problems with lack of entropy, I mean, you know, that was one of the presumed backdoors with that dual random, what, the dual elliptic curve pseudorandom number generator that the NSA seemed to be pushing?

Leo: That's right, that's right.

Steve: And in fact they paid RSA to put it in and then make it the default.

Leo: Right.

Steve: And so it was like, ooh, boy. Yeah. So random numbers are crucial. And we did a podcast about, what, a year and a half ago called "Harvesting Entropy" [SN-456], which I did after I developed a very good, arguably true random number generator, not pseudo, because that implies that you're able to recreate the sequence, this one you really can't, for the SQRL client, which like all of crypto needs a good source of randomness.

So Comodo, the certificate authority that has been in the dog house a few times, over the years their name has come up, once because they were issuing - they were caught issuing fraudulent certificates. They were also the software behind Superfish. And so it's like, okay, that seems a little unsavory. Well, but they're a popular certificate authority, and they're trusted by all the browsers. They recently performed an internal audit and uncovered eight certificates that should never have been issued. And these were certificates for the "domain" mailarchive, as an example, and help. Not mailarchive.com or help.com, but just those words. And...

Leo: What?

Steve: Yes. And Comodo also warned that "quite a number," in their words, of unnamed competitors have committed similar violations. So this is a violation of a so-called "baseline requirement" of...

Leo: You've got to have a TLD.

Steve: Well, except that the reason this has been done is for Intranets because, for example, mailarchive might be a server name on a corporate Intranet, and they want to be able to create a secure connection to their internal mailarchive server. So it's understandable that companies might ask certificate authorities for such a certificate. They have a need for it. But the problem is this protects - this is then a certificate for all mail archives everywhere, that is, anything named "mailarchive" would...

Leo: Oh, so it's a wildcard.

Steve: Well, it has the equiv- well, yeah. See, so what we, when you think about it, what we get with the domain, the classic public domain name hierarchy is uniqueness. We have a set of top-level domains, then second-level domains, and then machine names or additional domains. But the point is that dotted name hierarchy absolutely refers to a single unique entity. The problem with mailarchive or help is that it doesn't. It could, if you name your server "help," then anyone who has a certificate for the help domain is able to intercept communications and spoof and get up to all the mischief that you can if you've got a maliciously generated certificate.

So the baseline requirements for the CAB Forum, the CA Browser Forum, absolutely states that these certs are not okay. Nor are certs for the private IP space. So a cert for 192.168.1.1, there are some certs that have been issued in the past for that and shouldn't have been because, once again, anyone who had such a cert could - because, again, that's not unique. It probably exists in most of our local Intranets that are behind consumer routers with the 1.* suffix on 192.168. So anyway, a spin on this comes up later in our Q&A.

But this is another reason, I mean, I remember in the early days of this podcast I was annoyed by certificate expiration. I was wrong. And I've said so several times in the last couple years. I get it now because, as the world has expanded, the idea of expiring certificates was a brilliant piece of foresight because that solves the problem. As long as no new issuances are made, then even these that we wish that didn't exist, well, they will die of their own date and timestamp, within a couple years at the worst. So the system has the effect of sort of continually cleaning up its debris, which is really a benefit.

So for all the faults that this hierarchy, the public certificate hierarchy has, much as it chafed when I was having to pay hundreds of dollars, back in the old - I think it was like $900 a year a decade ago. The prices have come down. And of course we'll soon have domain name validation free from the Let's Encrypt project. So the world is changing. But, boy, expiration dates, they really do come in handy.

Leo: Yeah. As kind of a footnote, I always wish now that I had set expiration dates on my PGP keys because I have lots of old keys, and I get email from people using old keys, and I don't remember what the password was or anything, and I don't have the key anymore. So even with a PGP key or a GPG key, you probably should set an expiration, just every few years. Make it one.

Steve: The only place I'm glad I have a far-out one is I use certificates to secure my OpenVPN endpoints, rather than username and password. They're certificate based. And there you don't want them expiring on you because you're out traveling, and your server certificate expires. It's like, ooh, because you can't fix it without getting connected.

Leo: Yeah. Yeah, that's a good point.

Steve: So I do have long expiration. But those are exclusively private certs, and they're never being publicly shared; whereas server certificates are sent to the browser to validate, and so they're definitely publicly shared.

Leo: I'm wondering why you wouldn't just use a self-signed cert for an Intranet like mail, you know.

Steve: Yeah, I agree. I completely agree. Why need to go get...

Leo: It's not public.

Steve: Well, okay. So the self-signed cert would not be trusted by the browser by default.

Leo: Yeah, so you'd have to have a corporate CA or, you know, that you'd add to the browser.

Steve: Well, if you had a corporate CA, then that's really what you want to do. The right

way to do this is to have a corporate certificate authority that issues certs for the corporation.

Leo: Right.

Steve: Then all of the devices trust that CA, in addition to the other thousand public CAs that are trusted. Then you can have your internal group issue. But maybe the explanation is the sort of, I mean, that's very sophisticated. It really requires management and oversight and a team. And it's certainly easy to ask a public CA, hey, give me a public certificate for mailarchive. And then everything trusts your internal server.

Leo: Right.

Steve: Even though, unfortunately, that's really prone to abuse. So here's a note to our listeners. If you're unfortunate enough to get hit by the Windows Power Worm ransomware, do not pay the ransom.

Leo: Why not, Steve?

Steve: Not because they will decrypt your files if you do, but because they can't.

Leo: Oh. Oops.

Steve: Turns out Power Worm has a bug. It was badly coded, and it locks the data away forever. It infects Microsoft Word and Excel files, that is to say, encrypts them. But the latest version of its update goes after many more types of files that it finds on the victim machine. A malware researcher by the name of Nathan Scott discovered this variant and uncovered the mistake its creator made when updating it. Nathan believes that errors arose when the creator tried to simplify the decryption process, so that is, you know, encryption, decryption. So he's trying to simplify that second phase, the you pay him the money - not Nathan. You pay the bad guy, the Power Worm people the money, and then they provide you with the key to decrypt. They tried to make it use a single decryption key, which, yeah, obviously, so apparently they're not very good. But they mangled the process of generating that decryption key.

As a result, there is no decryption key created for the files it encrypts when it compromises a computer. Lawrence Abrams on the Bleeping Computer website that we refer to often because they've got a great forum there, and they have great pages for helping people with ransomware, he did a post saying: "There is unfortunately nothing that can be done for victims of this infection. If you have been affected by this ransomware, your only option is to restore from backup."

Leo: Customer service has just really gone downhill in the hacker community, I think.

Steve: It really has, you know? You can't even - they encrypt your machine...

Leo: And they can't unencrypt it.

Steve: And you pay them your money, and they say, oh, we're sorry, you got the buggy version of the encryption ransomware. We really did, you know, we want to get paid. We're unhappy now that we're suffering reputation damage.

Leo: Yeah.

Steve: Because now no one's going to pay us because we screwed their data up, and now we can't unscrew it. So...

Leo: Shocking.

Steve: That's the way it goes. So, yes, get hit by Power Worm, don't pay, just restore from your backup. And we know you have one.

So Microsoft recently blogged, in a follow-up to all of this recent concern about SHA-1, we've talked about it several times over the last few weeks, the fact that a collision was created in part of the full 80-round implementation of the core part of SHA-1, not the whole hash. People are still feeling, you know, SHA-1 itself hasn't had a collision. But this scared everybody. And this is the way, as we know, crypto happens, is that somebody makes a bit of a breakthrough that weakens it to a point where, ooh, this is ahead of schedule. And so what happens is you move your schedule up for moving past that crypto.

So Microsoft's blog posting was "SHA-1 Deprecation Update." And they said: "In a previous update on TechNet, we announced that Windows will block SHA-1 signed TLS certificates starting on January 1, 2017." Okay. So that's a date we've talked about many times because what was annoying was when Google stepped in and said, eh, we're going to do it sooner. And many people were upset. In fact, we were just talking about how there are corporations that are saying they need SHA-1 certs, new SHA-1 certs issued after the first of next year, that is, the first of 2016, because they can't stop using them. And here we're talking about the expiration of the certs at the end of 2016, January 1st of 2017.

So anyway, now Microsoft is saying that: "In light of the recent advances in attacks on the SHA-1 algorithm, we are now considering an accelerated timeline to deprecate SHA-1 signed TLS certificates as early as June 2016." So they're going to split the difference. They're going to go midyear of next year. Their browsers, their properties, Windows and servers and browsers, everything will just say, nope, SHA-1, no good after middle of 2016.

And Microsoft finishes, saying: "Mozilla recently announced a similar intent on the Mozilla Security blog. We continue to coordinate with other browser vendors to evaluate the impact of this timeline, based on telemetry and current projections for feasibility of SHA-1 collisions." And this is an interesting note, and you heard me say "telemetry." And we've talked about - and in fact I heard you mentioning it on a podcast recently, Leo,

that like the telemetry is something, eh, fine, you know, if it helps Microsoft, then that's good. And here's a perfect example. It helps Microsoft to get a feel for where and how much and how often SHA-1 certs are today being used, and to look at that history trend over time because that allows them to say, you know, I mean, Microsoft is a company that doesn't want to hurt anybody or upset anybody. They don't want stuff to be broken and incompatible. They're all about it just works.

But if their telemetry is demonstrating that servers are rapidly phasing out SHA-1, then that gives them the confidence to make a commitment date of no longer accepting it at all, knowing that the number of people that they will be upsetting will be minimal. And that's been my own personal strategy. GRC, you know, my certs are SHA-1, and I will take them offline a day or two, to make sure I have time if something goes wrong, before the end of the year, and replace them with SHA-256 certs. I already have them. DigiCert's provided them to me, and they were nice enough to provide me with early expiration SHA-1 certs.

I'm doing it because there are still people who need SHA-1, I mean, there have been all year, people who need SHA-1 in order to get to any secure website, and you can only get to GRC over TLS. So, but at the end of this year, I'm saying enough of that, I'm switching to SHA-256. And then six months later Microsoft, having moved their deadline forward by half a year, saying we're not going to play ball either.

And Mozilla, I wanted to follow up Microsoft's mention to Mozilla. And they posted, and this was on the 20th of October: "In our previous blog post about phasing out certificates with SHA-1 based signature algorithms, we said that we planned to take a few actions" - now, this is browser-side, of course - "with regard to SHA-1 certificates. One, add a security warning to the web console to remind developers that they should not be using an SHA-1 based certificate." That they've done.

"Two, show the Untrusted Connection error whenever an SHA-1 certificate issued after January 1st of 2016 is encountered." Okay, so that's after the beginning of next year, because those should not be issued any longer. Everyone has said, I mean, that was that whole - remember we talked about the voting that went out among the CAB Forum members, should we allow short expiration certificates to be issued after the first of next year. And it was while that vote was in process that the news of this 80-round collision to the core of SHA-1 came up, and everyone backed off, saying, okay, forget it. Forget we mentioned it. We retract the vote. So that they've done.

Then the final thing that they will start doing with the next version of Firefox, 43 - we were just talking about 42. With next major release 43 they will show the Untrusted Connection error whenever an SHA-1 certificate is encountered in Firefox after January 1st, 2017. So that's not issued, but seen after the end of the year. That's what they had said. Now Mozilla says: "In Firefox 43 we plan to show an overridable Untrusted Connection error whenever Firefox encounters an SHA-1 based certificate that has ValidFrom" - which means the start date - "after January 1st, 2016. This includes the web server certificate as well as any intermediate certificates that it chains up to. Root certs are trusted by virtue of their inclusion in Firefox, so it does not matter how they're signed. However, it does matter what hash algorithm is used in the intermediate signatures, so the rules about phasing out SHA-1 certificates applies to both the web server certificate and the intermediate certificates" - which of course certificate authorities issue - "which sign it."

And so then they finish, saying: "We are re-evaluating when we should start rejecting all SHA-1 SSL certificates, regardless of when they were issued. As we said before, the current plan is to" - be essentially synchronized with what Microsoft was originally doing.

"The current plan is to make this change on January 1, 2017. However, in light of recent attacks on SHA-1, we are also considering the feasibility of having a cut-off date as early as July 1, 2016." So, and presumably that's what Microsoft meant. They said June 2016. They may have meant June 30th. And so essentially half a year. So looks like SHA-1 will soon be another signature that no one uses, much like MD5 and MD4 and basically the historically older hashing algorithms.

This is out of the blue, well, but it's on topic, from my own experience. This is the Security Maintenance Tip of the Week.

Leo: I like this. You should do this every week.

Steve: Yeah, well, I don't always have them, but this is one. Log into your Twitter account on the web and look through the apps you have given access to. I did this last week. I don't know why I went there, but for some reason - because normally I don't use the web interface of Twitter at all. I use clients. I went to the apps. And it was like, first of all, it was a little nostalgic for me.

Leo: Right, right.

Steve: You know? But that's the point. I had hundreds of permissions on apps that I haven't used, that I haven't seen, like, because they don't go away. And this is a mistake. They ought to expire in the same way that certificates do. That permission ought to have maybe a one or a two-year self-expiration. Maybe you get a notice. Maybe it just dies. And you go, oh, and then you reauthorize it, if you're still using it. But it's just - so anyway, Security Maintenance Tip of the Week: If you're a Twitter user, you're into this social networking, you're using apps, you have incrementally given this or that and the other app permission. They're all there forever unless you go and remove them. And so I had a field day. I cut it down from, like, I don't know, pages of them to a handful that I'm actually still using today. And it felt good to just yank those permissions away.

Leo: Yeah, yeah, yeah.

Steve: So I know our listeners will get a kick out of that, too. Okay, and this is the Quote of the Week. I just got a chuckle out of this, and this is geek time, but what the heck. Quote of the Week, this was from Chris Keller, who tweeted this to me, mentioning, you know, using the @SGgrc, he said: "My password is the last 15 digits of Pi."

Leo: Nobody'd ever guess that.

Steve: Yeah, that's a safe one. Yes, choose the last - it doesn't matter. Well, it does matter. You don't want...

Leo: Any irrational number would be good; right?

Steve: Yeah, I was going to say. But you don't want to use the last digit of an irrational number because unfortunately there aren't many combinations of those. There's, you know, 10. But the last 15 digits, and pick your...

Leo: [Crosstalk], yeah.

Steve: Yeah, you could, you know, pick your irrational number and go for it - pi, e, rho, whatever.

Leo: Avogadro's number, [crosstalk].

Steve: That's right, that's right.

Leo: Okay. Okay.

Steve: Some miscellaneous things. Sunday's TWiT podcast, oh, my god.

Leo: Uh-oh. Bad or good?

Steve: Leo, it was a world-class, conference-level discourse.

Leo: Oh, yeah, yeah. Well, when you have Om Malik and Ben Thompson, Steve Kovach, that's pretty good.

Steve: I'm wanting to tell our listeners, you already know, this is what you would pay thousands of dollars and travel thousands of miles to go sit in a room and listen to. As it happened, I was doing some non-semantic work, as I call it, working with my hands, so I was able to listen at the same time. I can't read or write when someone's talking, but this I could do. I was just stunned by topic after topic after topic of just informed, interesting, you know, I mean, it's completely different than this podcast. I know our listeners have - we've developed this format of techie, deep, you know, bullet bullet bullet bullet bullet, and that's what works here. This was sort of rambling, really philosophical and interesting industry veteran stuff. And again, I just - I can't recommend it highly enough. It was just - there was no nonsense. And, literally, it's what you pay thousands of dollars and travel thousands of miles to get...

Leo: Thank you, Steve, thank you.

Steve: ...what you can get just by clicking a link and listening for a couple hours. It was really good.

Leo: I basically sat back because, yeah, when you get these guys on, especially Om and Ben, they are really deep.

Steve: Yeah. And, I mean...

Leo: And they go off of each other, and man, you just go...

Steve: And there was pithy stuff. And the Om guy, what I liked about him was he had no fear about telling the truth if it was negative.

Leo: Oh, yeah. Om's got nothing to lose, yeah.

Steve: If it was negative, you know, normally people pad because they're not comfortable just saying to someone, "Oh, that's nonsense," or "You're completely wrong," or "I absolutely disagree." It just came right out. And it was wonderful.

Leo: Thank you.

Steve: So, yeah, bravo.

Leo: TWiT.tv, find Episode 535.

Steve: Good, 535.

Leo: Thank you, Steve.

Steve: It's really good.

Leo: And don't sell yourself short. This is a master class of security every week. And I in fact know many universities that use Security Now! for curricula, and lots of experts in the field who listen regularly. So this is a pretty good show, too.

Steve: I think many people, you know...

Leo: It's an awesome show.

Steve: I'm getting plenty of positive feedback, so I know we're doing the right thing. Okay. Windows users. I found a stunning piece of free software. I started using this a couple months ago, back after I switched over from the pair of T1s over to the cable

modem. It's from a company called SoftPerfect. They make a bunch of free stuff and some paid stuff. This is called NetWorx with an X, N-E-T-W-O-R-X. SoftPerfect NetWorx. It is free. And it has a stunning feature set. It is a network bandwidth monitor. Runs on your screen, shows you incoming, outgoing, and both at the same time. But it also does long-term aggregation. So it can show you monthly total usages, I mean, everything is customizable.

So you've got instantaneous bandwidth usage, long-term usage aggregation, per-application usage so you can see which of your applications is using how much bandwidth, deeply customizable, I mean, it's just - it's beautiful. And there's a paid one that I tried to buy, that's well known, DU Meter's been around forever, but it wouldn't run on XP. So I thought, well, okay, I'll just hold that one. I mean, I bought it, and then I found out it wouldn't run on XP. So I'll maybe - and then I was thinking, okay, I'll use that when I switch over to Windows 7. No. I'm staying with SoftPerfect's NetWorx for Windows. It is fabulous.

Leo: The only thing I'd mention, though, is when you get to the website, you may be tempted to click the "Get It Here" buttons. That's not the software NetWorx. That's an ad, and you'll download something you don't want. So go all the way to the bottom, where it says "Download NetWorx." I hate it when people do that, but obviously this is why it's free. They're trying to monetize.

Steve: There's somewhere, zip up to the top, there's like a page that lists their apps.

Leo: You can just go to the tab that says Download. That might be the best way to do it, yeah. Because then you can get the other ones, too. There's a whole bunch of these. Look at that. Yeah.

Steve: Yeah. So they have a bunch of free things and a bunch of paid things. Anyway, people, free is easy, and this thing, they nailed it. It's what you want. And I'm not paying for the amount of bandwidth I use over time, but some people may find it interesting, and some people it may be important. So, yay. I was just - I wanted to let everybody know about that.

Leo: I want to get it right now.

Steve: And then the second thing for Windows I referred to at the top of the show, when I read off an itemization of the things it fixed. And that's Spybot Search & Destroy. People have been around for years. One of the better early spyware-removing tools. This is their Anti-Beacon, Anti hyphen Beacon. It runs on Windows 7 through 10. And there's an installer version. You can download a portable version and a standalone. They wrote: "Spybot Anti-Beacon for Windows 10 is a small utility" - and I can vouch for that, it's only a few meg, so I was impressed with that, as well. I mean, it shouldn't be that big, but many things that shouldn't be are. It is small - "designed to block and stop the various tracking, a.k.a. telemetry, issues that come with Windows 10. Seeing the bunch of incomplete or broken scripts to disable tracking in Windows 10, and the tools that install adware or worse in exchange for their function, we wrapped disabling tracking up in a small tool that's free and clean. With the upcoming news about telemetry in Windows 7 and 8.1, Spybot Anti-Beacon has added support for those, as well."

So again, not for everybody, not if you're not concerned about Windows 10, if you are like with Paul Thurrott, who thinks there's nothing to worry about, fine, not a problem. But if you're somebody who would like to use Windows 10 sort of the way we used to use an operating system, then looks like these guys have done a great job. And they'll be keeping it up to date. We're already at version 1.2, and they've had a bunch of incrementals as they've added...

Leo: This baffles me because you're trusting Spybot, but not trusting Microsoft.

Steve: That's correct. So let's be clear about that. That's absolutely right.

Leo: You know these guys at Spybot? I know that you actually kind of empowered them in the early days with Spybot Search & Destroy. But you know these guys? They're local guys? You trust them?

Steve: No. And, see, it's that people don't want to be sending telemetry back to Microsoft.

Leo: I understand. But you're putting some random software on there that claims to do all this. Who knows? Maybe it just channels it all to the Spybot server. Right?

Steve: No.

Leo: No. Okay.

Steve: I mean, maybe, but no.

Leo: Okay. I'm just saying. Just understand, everybody, what you're doing. You're transferring the trust from Microsoft to Spybot, effectively. Right?

Steve: Yeah.

Leo: Or you can do what Steve does and use Windows XP.

Steve: You're just, yeah, you're just saying I don't want my operating system to be generating metrics on me and sending them to Microsoft. So I'm going to turn all this off. And, I mean, what they're doing is straightforward. They're using a group policy manager to shut this stuff down, and doing it in a better way. So, but you're right, I mean, trust isn't...

Leo: It's closed source; right? I mean, you don't know what they're doing.

Steve: Well, everything is closed source that isn't open.

Leo: Oh, I know, I know.

Steve: And so...

Leo: Okay.

Steve: Okay. So for iTunes, I've never been happy with the built-in apps for reminding me of stuff. And there are sometimes things I need to be reminded of. I found a fabulous free piece of software for iOS called Alarmed, A-L-A-R-M-E-D. I think it's free initially, and then I think you do something, and unfortunately there isn't a good audit trail for that. But it is really feature complete. Pop-up reminder alerts with robust repeat scheduling, a flexible snooze and full customization. They've got - when I say it has all the bells and whistles, I mean that literally. It comes with a huge array of really good reminder sounds. And I like to have different sounds for different things.

You can use Siri to create reminders and import from the Reminders app into Alarmed. It iCloud syncs and backs up, so all of your iOS devices are updated when you set a reminder. You can create categories. A hundred and 40, they said, high-quality custom sounds. Oh, and it's got both timed and location reminders. So you can set a reminder on a location so that, when you go somewhere, it reminds you of what you wanted to do there.

Anyway, I've been using it now for a while, and they nailed it. I'm super happy with it. So if I paid something, it was a couple bucks to enable advanced features or something. But, I mean, and this is the kind of software you want, where one guy has spent a lot of time listening to feedback, evolving this over time, so that it does anything you can imagine. I mean, it's got advanced tabs for all this stuff, if you want to drill down and make exceptions and which day of the week you want things to happen. And anyway, Alarmed, A-L-A-R-M-E-D for iOS.

Leo: Yoctoville; right? That's the one?

Steve: Yes, you're looking at it. Green icon with a guy with his index finger with a string tied around it.

Leo: Do you ever use your Echo for timers? Because I use it all the time for timers.

Steve: You know, I forget that it's there. Sometimes I do. I'll just kind of call out to her.

Leo: I do it for tea timing. But then now I've realized, because we have one in the bedroom, I can say, "Hey, Echo, set an alarm for 7:00 a.m."

Steve: Yes.

Leo: It's by far the easiest way for me to set an alarm because I don't normally have to get up, but occasionally.

Steve: Yeah, and it's sort of a nice soothing sort of alarm when it goes off.

Leo: [Inexplicable noises]

Steve: Yeah, yeah, yeah. And I find myself thinking, wait, what sound is that? And I go, oh, and the little blue ring is fluctuating.

Leo: [Inexplicable noises] All right. I'm going with it. Alarmed.

Steve: I really, I know that you're in transition. Are you heading back to - you have an Android phone you're in love with.

Leo: Yeah, I wasn't at first with this Nexus 6P. But I had to - I think I had some software on there that was causing problems. Anyway, it's [crosstalk].

Steve: Because I heard you yesterday saying you were going to really - or day before, you were not going to put anything on there that you didn't absolutely need.

Leo: And it worked fine. And then I slowly put stuff back. I think I tracked it down to an IRC program I was using called IRC Cloud. And it was just tying up the processor by constantly watching IRC and notifying me when anybody mentioned my name, which is great, but does kind of tie the phone up. So I run it on the - iOS doesn't seem to have the same problem with it, by the way, so I run it on my iOS devices.

Steve: A real quick note, I saw "Spectre" on Friday.

Leo: Ah. No, it's gotten some bad reviews.

Steve: Has it? I...

Leo: You like it?

Steve: I just wanted to say I loved it. If you're not a Bond person or a Daniel Craig person, I understand that. But I thought it was everything you want from a Daniel Craig Bond movie.

Leo: Apparently the opening sequence is the best ever. Because you have Bond...

Steve: It was, yeah.

Leo: Before the credits there's always - and going back to "Dr. No" there's always an event, and then the [sings four-note Bond sting]. But, so, yeah, apparently this one was pretty amazing.

Steve: Yeah, it had that. And of course the credits, the Bond movies are famous for their title sequences. And this was just astounding. Just, you know, they must have spent - who knows what they spent. But Charlie Rose did an interview of Daniel Craig and the director. And there was initially some strange press saying that Daniel Craig was sick and tired of Bond, and he never wanted to do another Bond movie.

Leo: I don't blame him. It took them two years to make this movie.

Steve: And that's my point, is that, yes, they spent the money. This was all on location. He did the stunts. And someone in the press asked him immediately upon it being finished, when would he do...

Leo: He was exhausted.

Steve: Yes. The last thing he wanted to think about.

Leo: You don't ask a novelist when they just finished, rip out the last page, oh, when are you going to send the next one? The first thing they're going to say is "Never."

Steve: Right. Which is what he said. And Charlie asked him about that. And he sort of shrugged. And that's where I understood. He said, look, they asked me when I had just finished filming. I spent two years of my life. I haven't had a life. I've been doing this. The last thing I wanted to think about was another one. And Charlie said, "So, will there be one?" And he said, "Yeah, when it's time."

Leo: I'm sure they gave him a lot of money.

Steve: "Skyfall" made, well, a billion dollars.

Leo: Yeah.

Steve: It was a billion dollars. And so these movies do pay.

Leo: He just has to say, "Ten percent of the gross, we're good."

Steve: Yeah.

Leo: We're good.

Steve: And I already did mention Paul Thurrott's tweet and link. If you want to click the link and show the picture, I just got a kick out of it. It's Paul Thurrott on the iPad Pro, which of course we believe goes on sale tomorrow. He doctored the photo.

Leo: Thin. Light. Pointless. Oh, he's just jealous. I'll have one by next week. I'll let you know. And you will, too, hopefully.

Steve: I will, too, hopefully. So I did get, when I was going through the mailbag, a fun note, something I'd never - an analogy I hadn't run across before in all these years. And the subject was "SpinRite Oil Change." Barry Brown in Arizona, oh, Barry Brown who's in Arizona in the winter and Washington in the summer.

Leo: Okay.

Steve: He said: "Steve, I've been using SpinRite monthly, for many years, on my eight-year-old HP 9500 laptop. I have the original drive that came with the laptop still in use as the D: drive, where I store data. About four years ago I upgraded the C: drive to an SSD. And needless to say, I've never had any trouble with either of them. If you want your internal combustion engine to last, you change the oil. If you want your hard drives and SSDs to last, you run SpinRite. This laptop has not led an easy life," he writes. "I use it as my portable desktop. It's been all over the world, and even fell out of the overhead bins a few times. SpinRite brought it back, time and time again. Barry."

Leo: Nice.

Steve: So, Barry, thanks for the oil change analogy. That's a...

Leo: That's a great analogy, yeah.

Steve: ...good way to look at maintenance, which drives could use, even though they don't tell you that.

Leo: If it's got moving parts, it needs maintenance.

Steve: Yeah.

Leo: Continuing on. We've got questions. You want answers? We've got 'em. Steve's the king.

Steve: Cool. And we've got great listeners who are on the ball and offering ideas, sharing their experiences, and every so often asking a question.

Leo: I love 'em. Starting with Question 1 from John in Cinci. And he has a prime example of doing it wrong: One of my clients uses a secure email service to send secure, private messages to their customers. That sounds good. What could be wrong with that? The system works by allowing the sender to enter an email message into the site, then sending the recipient a link that takes them to a web page where they can securely read the message.

Steve: So far, so good.

Leo: Thus the message text never transmits in the clear, over the public Internet, and the company that provides the service appears to be doing everything right by providing end-to-end encryption with the customer in control of the keys. But then, when troubleshooting an issue of why a recipient couldn't access a secure message, I found that the recipient's company web filter was blocking access to Facebook when the secure message was being displayed. Turns out the secure message viewer web page was loading JavaScript code and single-pixel images from several third-party sites including Facebook, also Google Analytics and DoubleClick - DoubleClick is Google, so that's not surprising - and several others.

I couldn't believe what I was seeing. This is a service for accessing messages privately, and it's telling everyone about it every time a message is read. Not to mention allowing a third party's script to run on a page that's meant to be secure from third parties. Doing this obviously puts the user's privacy at risk and has no place here. At minimum, it lets these third parties know when the message was read, where, and the referrer URL, from which the sender and recipient can be found. Oy, that is kind of a leak, isn't it.

Steve: Yeah.

Leo: Add to that the tracking - it doesn't show the message, but, boy, that's a lot of other metadata. Add to that the tracking info these companies may have on the user, and then there's their control of the JavaScript. They're definitely doing it wrong. I did get them to remove the Facebook. Why would they put a Facebook bug on there? Took them a month, and they are resisting removing the others. Very frustrating, since they make all these claims about security and privacy on their

website. And you know what? No one would ever see these, so no one would ever know.

Steve: Yup. Yup.

Leo: Thanks for the show and all the great info. Long-time listener since the first episode, saver of countless hard drives thanks to SpinRite, and PiDP-8 owner. You know, I ordered one of those kits. I haven't gotten it yet.

Steve: Oh, you should have. I got my three.

Leo: Uh-oh.

Steve: Yeah, it's been months ago.

Leo: Oy oy oy.

Steve: Yeah. Yeah, yeah.

Leo: I ordered it assembled. Maybe he's just - maybe that's...

Steve: Oh, that could very well be. He might, yes. And I'm glad you did because then you can just put it behind you and...

Leo: Yeah, I'm not going to solder it together.

Steve: Yeah.

Leo: Hey, did you see the - we didn't mention it, but the ProtonMail DDoS [crosstalk] secure email.

Steve: Good point. I did, it fell off of my list just because we went - there was so much talking about...

Leo: Yeah.

Steve: Yeah. And it was like multiday, five days.

Leo: Man, 10 gigabits, it was huge, 100 gigabits.

Steve: Oh, yeah. And that's the state-of-the-art flood now is just - it's unstoppable. And...

Leo: They said because of the size it had to be a nation-state doing it, a governmental actor.

Steve: So that seems odd. But again, it's very difficult to track this down because you've got traffic streams coming in from all over the world that probably infected clients that are under control of a remote access trojan, that are all pulling pages from that server. I noted that there are some services now which advertise DDoS protection. But of course those are not free.

Leo: ProtonMail said about $100,000 to do that.

Steve: Exactly.

Leo: So the $6,000 ransom they paid was a deal.

Steve: Yes, yes. And of course nothing keeps the bad guys from coming back except maybe there's honor among thieves, who knows.

Leo: Oh, yeah, right.

Steve: Yeah.

Leo: Yeah, right. Question 2. We're done with the answer; right?

Steve: Yeah.

Leo: Just bad news, yes.

Steve: Yeah, I just thought that that was a really interesting, you know, the idea that you would go to all the trouble of creating - and this is so typical. I mean, the web just seems to be irresistible for people to do things wrong. But you go to all the trouble of creating a secure end-to-end email delivery transit management system, where they don't have the keys, the end-users have the keys. And then the page that comes up has trackers on it. It's like, my god. It just boggles - again, just because it's on the web. Something about the web, this stuff seems irresistible. Or maybe they used some drop-in toolkits, and that's where the trackers are is in some third-party thing that they're not

even aware of.

Leo: Watching a CNN story about the TSA let a guy get on a plane with a suspicious bag. They noticed it later. They stormed the plane. It's got dental tools in it.

Steve: Wow. Well, everybody's on edge these days.

Leo: Question 2, Steve in Walla Walla, Washington wonders about malvertising - I love that - versus user-generated content: You've spoken a lot on Security Now! about how bad guys buy ads as a means of loading their malicious content on unsuspecting users' browsers. But why don't we hear about malicious payloads in user-generated content sites, like some blogs or YouTube? Anyone can upload an image or video to many sites out there. So why are these not used heavily as vectors of attack? Is there something inherently different about loading a video or image on YouTube or a blog than an advertisement?

Steve: So, yeah. A couple things. There's been enough history of malicious games being played from user-supplied content, you know, famously Johnny Drop Tables. And for so long the backend PHP or SQL interpreter would be involved in the content being displayed. So bad guys figured out they could easily get up to mischief from user-generated content. This is old enough now that pretty much any system which is going to be hosting user-generated content filters it heavily on the way in, really scrutinizes it. And those things generally don't need the features, for example, JavaScript, you don't want a user submitting JavaScript.

So JavaScript has a half-life of a microsecond, if you try to upload it onto some server that is going to host it. Whereas ads are linked to third parties that, as we know, can host JavaScript by design. When we talk about a web page with megabytes of JavaScript coming from third parties, sometimes those are non-advertising application libraries. But often they're ads themselves that are permitted to run JavaScript and Flash, for example. So, for example, YouTube is phasing Flash out in favor of native HTML5 video playback. So Flash is leaving YouTube. And user-generated content doesn't have the flexibility, doesn't need to have the flexibility, and deliberately blocks the flexibility that web-based ads have.

And finally, it's about volume. If you can get an ad on The Wall Street Journal or The New York Times or the Huffington Post, and of course the Huffington Post has had problems with this recently, you're getting an amazing number of eyeballs. And while it's true, some YouTube videos get played when they hit millions of times or tens of millions or hundreds of millions, most of them are maybe, you know, a few thousand. They're much more modest counts. So these guys are going for volume of opportunities to infect and then the ability to run their stuff. And unfortunately, malvertising is the sweet spot for all of that.

Leo: Just block Flash, baby.

Steve: Yeah.

Leo: It's almost always Flash; right? I mean, I guess it could be theoretically JavaScript. But it...

Steve: It's normally JavaScript that invokes something in Flash.

Leo: It invokes something else, or like Flash or a reader or something.

Steve: Right.

Leo: Donn Edwards in Johannesburg, South Africa has a drive encryption question: Steve, if I create a mountable encrypted volume - for example with TrueCrypt or VeraCrypt - and then fill the entire drive with a file containing only zeroes, how much easier will it be for someone to figure out my encryption key or password? I ask this because some utilities allow you to do this with the free space on your drive. Is that leaking information?

Steve: So that's an interesting question. We've never talked about the details of encryption of hard drives. I don't know how it escaped us, but there was just always so much else to talk about. What the drive encryption technology uses is something known as a "tweakable cipher." And you know we've never talked about it because I'd never used the term "tweakable cipher" before. But the idea is that you don't - you have this large region of space with numbered sectors. And for security you want essentially different keys for every sector, or maybe every cluster, depending upon the granularity. And so what has been developed are something known as "tweakable ciphers," where the tweak factor is the linear number of the sector or the cluster, probably the physical sector, if you're operating below the file system level for this encryption. And it has to be very fast.

So with that foundation, what Donn's talking about, with the idea of like we know this is all zeroes, how does this help us? Well, that's the known plaintext attack, as opposed to, for example, the chosen plaintext attack, where the attacker can cause something to be encrypted and then examine the results. This is the known plaintext because you know, if you're wiping regions to zeroes for presumably extra security, or to fully, like, do a secure erase or a secure delete of a file, you want to actually zero the information. It turns out that these ciphers and other properly designed ciphers are fully hardened against known plaintext attacks. So the bottom line is, with that background, nothing to worry about. You can use a secure deletion tool in an encrypted drive without that helping an attacker in any substantial way.

Leo: Just checking to see where my PiDP-8 is. I sent Oscar a note.

Steve: Yeah, do send Oscar a note. He was really responsive. He was really great. And I've talked to lots of people who've received them and built them. A bunch of them were saying, hey, your programs for the machines behind you run too fast. Well, because I used...

Leo: There's a Raspberry Pi in there; right? Or something like that?

Steve: Well, there's a Raspberry Pi. But the emulator is of a PDP-8. I used - I needed something that was slow. So I used the teletype output, the delay in sending a character to the teletype, in order to create a fixed slow time quanta which my software then uses. So I had to use PDP-8 instructions. So I thought, what can I use that's usefully slow? And so I actually used the "send a byte to the teletype" as a delay factor. But it's not emulated in Oscar's implementation. So my code needs to be slowed way down.

Leo: You just put some goto subs in there; right? Go subs. Go sub. Count to 10, go sub. Count to 10...

Steve: Yeah, well, remember it's all machine language.

Leo: Oh, well, same thing; right?

Steve: Yeah, well, no, because the PDP-8 doesn't have a subroutine.

Leo: Right. But you must be able to jump to a memory location repeatedly. Does it even have for while?

Steve: No.

Leo: [Crosstalk] some test; right?

Steve: Leo, it has a...

Leo: You increment a register until it's full, until it's FFFF.

Steve: Three-bit - there aren't registers. Three-bit opcode.

Leo: There's no registers?

Steve: There's one accumulator.

Leo: Okay, increment the accumulator till it overflows.

Steve: Well, so it turned out that my system had requirements. For example, I'm showing the instruction pointer there. So if I'm showing the instruction pointer, I can't

have it busy doing something else. So anyway, so I ended up coding around all of the limitations to come up with this. But it's really just for that particular piece of hardware. So eventually, after SQRL, after SpinRite, I will build my three new PDP-8s, and I'll write new code for everybody who has one.

Leo: Oscar did write to me when I gave him my order back in June and said, "I owe you. You guys are responsible for two thirds of the PiDPs that'll be in existence shortly. If you boot up your PiDP for the first time, it might call you 'Daddy.'" I don't think it can do that, actually.

Steve: I want to see blinking lights behind you for the podcast.

Leo: I want blinking lights.

Steve: Yes, we need blinking lights.

Leo: So I'm glad I asked you because I just kind of spaced out. You know I do that a lot. I order stuff, and I never remember that I ordered it.

Steve: I think, as I remember, he did it on the 8i, and I did it on the PDP-8e. That's why I only have two registers of lights. His has, like, five registers of lights. It's going to be fun. There's going to be lots of blinking lights.

Leo: Is it going to come with software installed, or do I have to download and assemble your code?

Steve: Just give it to one of your - oh, give it to Padre. Padre would love to get it set up for you.

Leo: Oh, I'm sure he would be, yeah, yeah.

Steve: Yeah.

Leo: All right. More questions. This one's from Montreal. John wonders about the wisdom of allowing scripting. He points to a Trend Micro posting which mentions NoScript as a mitigation. Granted, it's not a great way to mitigate the threat unless everybody on your home network, including friends, blocks scripts. I do agree that NoScript is really intrusive; but, on the other hand, it does offer protection. And it pays, in my opinion, to see what third-party sites can mess with you. For example, I routinely access Amazon.com, but I never trust it. That mistrust paid off recently as Amazon started to import stuff from Cloudfront.net, which isn't really a great idea as, in the past months, reports have surfaced of malware finding its way onto people's computers through that service. You agree?

Steve: So the Trend Micro posting was titled, it was like from their Trend Labs Security Intelligence Group, "DNS Changer" - which we've talked about before - "Malware Sets Sights on Home Routers."

Leo: Oh.

Steve: And so this is stuff that somehow gets into a person's network.

Leo: I get it. That's why he says friends and other people in the household could be a problem.

Steve: Right, right. And so it uses the known - and this is not news - the known weaknesses in consumer routers, for example, users who do not change the default username and password to log into them. And so this is - I wanted to bring this up again because when it first happened, we said, okay, we're going to be seeing more of this, and this is what Trend Micro is reporting.

What this does is it's called DNS Changer because we rely on the correctness of DNS to make sure that we're going to the right websites. And even though like a malicious redirect to an Amazon.com won't have their security certificate, you might go to Amazon.com over HTTP. And if you were at the wrong IP, you'd be at the wrong server, and you wouldn't know any difference. And so that server wouldn't be using security. The point is that we don't yet have, as we've talked about recently, good DNS security. DNSSEC, DNS Security, exists. The spec's finished. The various root servers are in place. We've got support in the clients. We're just waiting for it to sort of propagate and happen. But these things take time, as we're learning with IPv6, which is fighting tooth and nail not to happen, despite the fact that it's going to have to now that we're really running shy of IPv4 addresses.

But anyway, I wanted to make sure that people understood that changing your router's login username and password is crucial because you get to your router through a web interface, by your browser polling port 80 or 443, getting a secure or a standard connection. You get then a login page. You fill out the form, and you log in. Well, that page that comes up identifies the router. So the malware doesn't even have to brute force. And everybody knows what the default username and password is. You know, sometimes you forget it for your router. And if you are bad, and you didn't change it, then you go google, you know, default password for Netgear something or other. And then it says, oh, you know, this is the password, the username and password. So anything in your network can do the same thing you do in order to log into your router behind your back and then get up to all kinds of mischief. And you don't want that to happen.

So it's very unlikely that it will do a brute-force attack. It's not beyond the pale, but, like, way unlikely. But still, change it from the default. And why not make it strong? You don't have to log into it all the time. And you can write it on a Post-it note and stick it on the bottom of the router because the malware can't see the Post-it note on the bottom of the router. And, you know, people say, oh, don't write these things down. Okay, so stick it in a LastPass or other password manager vault, as long as you remember that it's there. But it's sure better to change it, make it strong, and write it down and stick it on the router than it is to leave it as the default because you're worried about forgetting what you changed it to because this is something we're going to see more and more. And I will

note that John's commenting about scripts being a problem, and so that's one problem. But anything that's malicious getting in that has access to your network can do the same thing.

Leo: Question 5 comes from in Powell, Wyoming. TZ offers a site and tip: LibraryFreedomProject.org. Most of the resources listed on this site's Resources page will be very familiar to regular listeners of this podcast, but it's always great to have a page to refer to, as well. And this page is Privacy Toolkit for Librarians.

Steve: And weren't you talking about Tor and libraries in...

Leo: So we interviewed the Library Freedom Project on The New Screen Savers.

Steve: Right.

Leo: And we had the inventor of the Onion protocol and the creator of Tor on both The New Screen Savers and Triangulation. Dr. Syverson was way over my head. In fact, I think I asked you to join me, and I wish you had. But anyway...

Steve: Yeah, and I think I had a scheduling conflict, so I couldn't.

Leo: Yeah. Would have great.

Steve: I think it was Tuesday morning.

Leo: Because it was heavy-duty stuff.

Steve: Or Monday morning.

Leo: Monday morning, yeah. It's heavy-duty stuff. But, yeah, I do encourage people who are interested in this, The New Screen Savers interview with the Library of Freedom Project. They're putting Tor nodes in libraries.

Steve: Well, yeah. And I wanted to - the reason this caught my eye was that, I don't know about you, but I grew up in a library.

Leo: Me, too.

Steve: I grew up in the San Mateo Public Library. After school I'd ride my bicycle, and I'd spend the afternoon looking at my wristwatch, annoyed that it was getting close to dinnertime and I was going to have to come home because, for me, it was all of this stuff

that I wanted to know. And I was just voracious. And of course libraries sort of have a different role now. I think now they're sort of a community center. Sometimes they are the Internet access, the only Internet access that people who for whatever reason can't afford their own, maybe their community is connection-starved or who knows. But, I mean, there's a sort of a civic role that they play.

And I know that, in one of the interviews you were talking about, libraries, there was a letter that the DoJ sent that chilled a library because they were saying we do not want you to offer Tor browser or Tor services in your facility. And it was like, whoa, whoa, wait, what? It just, you know, it seemed wrong. And so there was, as I remember from the interview, there was a - you know, it's easy to get caught up in one person or one organization or the DoJ logic about oh, you know, how this could be misused. But the flipside is, wait a minute, you know, we want to offer people the freedom of using our service without worrying about them being tracked. Books don't track you.

Leo: They're putting Tor exit relays in libraries. They're showing people how to use Tor browsers. And they have, yeah, this great privacy toolkit. They actually have several. There's a mobile privacy toolkit and an online privacy class. Some good resources in here.

Steve: Yeah. So I wanted to aim our listeners at the LibraryFreedomProject.org. Browse around a bit. And as I guess either he or I mentioned, or what I was thinking was that it is great to have something to just aim friends to. You know, friends are asking our listeners, hey, how do I secure this, and what do I do? Or do you have a checklist, or blah blah blah. And you just say, hey, go here. Look at the privacy toolkit if you're concerned about privacy. And again, none of these will come as a surprise to our listeners. But it's just a nice compendium of useful resources.

Leo: Somebody there must listen to the show, maybe Alison Macrina, the librarian or the founder we interviewed, or others, because they recommend NoScript, and they recommend uBlock Origin and Privacy Badger and HTTPS Everywhere. You know, I mean, this is almost a list of things, a litany - YubiKey - of things that you've recommended over the years. So this is a, yeah, I think you're absolutely right, I mean, I just scanned through it. It all looks right on. So that's great. That's great. Continuing. Thank you, by the way, for the suggestion.

Steve: And we want libraries to survive, you know, and to...

Leo: Yeah. Oh, they'll survive. But we need to give them a little help from time to time, yeah.

Steve: Yeah, yeah.

Leo: Jeff Beaumont in Canton, Michigan solicits advice for a noob: Steve, my 13-year-old grandson is buying a Windows 10 laptop. Well, I know what you're going to say right away, but okay. And I wanted...

Steve: No, no, no, no.

Leo: Well, a 13 year old should be using Linux. Get him some...

Steve: Advice you can't use is not useful, so...

Leo: Okay. And I wanted to give him some security advice to get him off on the right foot. Actually, a 13 year old, I'd say get a Chromebook. But as a longtime listener to Security Now! I think I have a good idea of what to tell him. But as an Apple employee - oh, my - and Mac owner, my Windows-specific advice would be more theoretical than based on experience. My suggestions are never run as admin, use uBlock Origin for all web browsing, don't bother with third-party virus protection, and then the usual advice about not clicking on links in emails and using only trusted download sources. He left out updates.

Steve: Well, with Windows 10 you don't have a choice. So that'll be taken care of.

Leo: Well, but not just updating Windows, but of course the browsers you use and the...

Steve: Ah, yeah.

Leo: And Adobe Flash and Adobe Reader.

Steve: Oh, although the browsers, the browsers - yeah.

Leo: Most browsers do, yeah.

Steve: More and more, of course, yeah. Okay. So what I would add to that, because he asks, you know, what am I missing, I think the most valuable lesson that someone can learn is also more theoretical than platform specific. And it's nothing that our listeners haven't heard before. And that is, and this is, of course, Grandpa talking to his grandson. So explain about social engineering because...

Leo: Oh, good idea, yeah.

Steve: ...that's the key. That's the way - it's not technology, it's one way or another a suckering you into something. And a 13 year old with a Windows 10 laptop, it's all bright and shiny and looks wonderful. You need to understand that, I mean, he understands that bad guys use dark alleys to hide in the city. Well, bad guys also use the Internet to hide. And so you just - you wouldn't, just looking at the computer, there's like a level of abstraction between it and what the browser shows you and the reality and depth of what is connected to it because, when it's on the Internet, the Internet is on it. And

we've spent the whole front end of this podcast talking about really bad stuff that really bad people are really doing on the Internet. And when you're connected to it, it's connected to you. So just this notion of keeping your guard up, which is not anything anyone wants to hear, but it's something they have to hear. I think that's crucial.

And then the one piece of advice, the standard advice that could go in that upper list, never download something you are told you need because that's the most effective and most often encountered piece of social engineering and the way they get you. And the way they get the nave user is you go to a site, and something pops up and says, oh, your movie player is out of date. Click here to update your movie player. So many people are going to do that. And bang, CryptoLocker. So don't download something you didn't go looking for. I think that originally came from Brian Krebs, and that's just - that's pure pith.

Leo: And, yeah, I do agree, social engineering, that is a really good thing to talk about, I think, yeah.

Steve: Yeah, especially for a 13 year old who's just going to be trusting.

Leo: Wide-eyed and bushytailed, yeah.

Steve: Yeah.

Leo: David in Sweden. Oh, somebody's pointing out, by the way, that the interview I did with Paul Syverson on Triangulation, I don't think we published it yet. So if you're looking through Triangulation at episodes and saying, well, I don't see it here, we recorded that ahead of time for later release. I think it's going to come out Thanksgiving week, but I'm not sure.

Steve: Ah.

Leo: So watch for it in the next month. I apologize. I set up an expectation I cannot fulfill. A little later. Dave in Sweden wonders why not a wildcard cert for a top-level domain? Hi, Steve and Leo. If I got a CA to print a wildcard certificate for, let's say, *.se, is there anything preventing me from impersonating ANY website using a .se TLD? SE is Sweden, by the way. Are the TLDs in any way different from a subdomain of a top-level domain, for example, example.se? Or is it up to the CA to prevent these certs from being issued? Just for fun, I went to DigiCert's website and tried. Fortunately they did not accept *.se because it was a TLD. Is it just that they're on the ball, or is this some sort of automatic rule?

Steve: So of course this ties back into what we were talking about, about certificate authorities issuing certificates for domains they shouldn't.

Leo: Right.

Steve: I mean, if a certificate authority ever issued a wildcard for a top-level domain, they just ought to be shot, you know, taken out in the back and shot. I mean, I just can't imagine anything more horrific.

Leo: Yeah, no kidding.

Steve: And I'd be surprised if web servers honored such a certificate. I mean, I'm a little surprised web browsers honor, like, mailarchive, just a simple name like that. But, boy, a wildcard cert, I would think there would be logic. I don't know one way or the other because you're never going to get a *.se certificate, or *.com, or *.net or .org or anything. I mean, just there's - I would hope at every stage of the pipeline, from certificate all the way through servers rejecting it and clients rejecting it, like just that such a certificate would have no chance of even having a brief life within the public key infrastructure. I don't know. I don't know for sure. But I do know that absolutely no CA would...

Leo: That would be calamitous.

Steve: Yes. Oh, boy, yeah.

Leo: Well, you know Google issued a domain for Google.com. They sold their own domain name to somebody who had it for a total of two minutes before Google said, oh, wait a minute. Whoopsie.

Steve: I know.

Leo: So mistakes do happen.

Steve: Yeah.

Leo: Software is imperfect. Man, I'd love to own Google.com. That'd be a valuable domain until you went to jail. Let's move on. Question 8 from Pat Cho in Sacramento. He's wondering about sharing a cert: Steve, my ISP has offered me a free shared SSL certificate as a "thank you" for renewing with them. I don't know if you've ever talked about shared SSL certificates, so it would be nice if you could discuss any security issues with these, and how they differ from a private cert. Would it allow visitors to my website to use HTTPS?

Steve: Okay. So what a shared cert is, is just what we were talking about, the wildcard. But it has some intervening domain names. So, for example, say that there was an organization called hostingsites.com. So they would get a cert, *.hostingsites.com. And many of these sites offering shared certificates will give you - they'll get many different certs for different names, like *.mysite.com, star dot whatever, the idea being that then you choose the name for your site that goes under that, that is, that is the wildcard.

So this is Pat Cho in Sacramento, so it might be like patcho.hostingsites.com. And what this means is that, first of all, this is not expensive for the provider. They have one certificate, or maybe two or three, if they want different base names, like hostingsites or mywebsite.com. So it would be patcho.mywebsite.com. And so they only need a couple certs that can serve all of their customers and, yes, secure all of those websites. So Pat asks, would this mean that visitors to the website would use HTTPS? And that's exactly what it means.

Now, this is kind of new, although it's - remember, in the sense that things change really slowly on the Internet, what was necessary is an additional feature to TLS, back when it was called SSL, known as SNI, Server Name Indication. The reason this was necessary is that the certificate, an SSL or TLS certificate is typically bound to an IP address. That's why you needed one domain name per IP in the old days. Now we're talking about many domain names per IP. Thus we're able to use the wildcard. But the only way to allow this many domain names is for the handshake to indicate the hostname in the handshake. Because the domain name used to be implied by the IP, there was no need for that in the handshake. Now we've got multiple domain names on an IP, so that the actual domain name is no longer implied by the IP. Thus it has to be carried in the handshake.

So at some point in SSL's evolution - and this is 10 years ago, but again, things move slowly - this server name indication was added. It was an additional field that the client's browser could add to the handshake where it would, in the initial handshake, say I'm connecting to this IP, and I'm wanting a certificate for patcho.myhostedsites.com. That would go in the handshake. The server could then check to see if it had either that cert or a matching cert, meaning *.myhostingsites.com, which would satisfy its need, and then it would respond. So almost everything today supports server name indication. Again, it happened a long time ago, but things do move slowly.

So to give you a feel for it, what is not supported, and I pulled this from Wikipedia to get because that's being well maintained, is IE6. Okay, no big surprise. Now, again, you can use IE6 to connect to a non-wildcard domain just fine. But not a wildcard domain. So you could not use IE6 today to get to that. But, boy, you know, IE6, or any IE version on Windows XP or earlier. Safari on Windows XP or earlier didn't get updated. Blackberry OS 7.1 or earlier. Windows Mobile up to 6.5 does not support it. Android's default browser on Android 2.x. And, for example, this was fixed in Honeycomb for tablets and Ice Cream Sandwich for phones. There's a very popular tool, Wget, I use it all the time. And Wget before v1.14 did not support it. Nokia's browser on Symbian, okay, so we're getting into the weeds here.

The point is, yes, anything anyone would be using. SNI has been around long enough that its support is virtually universal, with some only old creaky stuff that probably will never be supported and almost no one is using any longer. So you get security, it costs the hosting provider nothing, nice that they're giving it to you, but don't think that they're doing you a big favor because they already have the cert that they're using with other people. Costs them nothing to make it available to you, as well. Maybe that's something that they normally have an upcharge for, for allowing you to use a secure connection. And so they're saying we're going to waive that fee, which, you know, that is nice. But, yeah, works great. And you can have a secure site.

Leo: Yay. John in the U.K. wonders about "Let's Encrypt" for email: Hi, Steve and Leo. Long-time listener, since it was feasible to catch up from Episode 1. You can be a long-time listener, as long as you've listened to all the episodes, even if you did it in a couple of weeks.

Steve: That's paying your dues, babe.

Leo: Yeah. I don't think you could do it in a couple of weeks, actually.

Steve: No, no.

Leo: I was wondering if it would be possible to use one of the EFF's Let's Encrypt certificates in an email client to achieve authentication and or encryption? Thanks. J. in U.K. Interesting question.

Steve: It is. And I doubt that it would be supported. Certainly it's not supported today because that's not their target. As it succeeds, maybe that automatic client protocol would be ported into email clients. But you could certainly kind of hack it. That is, you're going to get, from Let's Encrypt, a working certificate for identifying a server. That's the same certificate that an email server would use. So you can probably just import the Let's Encrypt certificate for the web server into the email server, and it'll be able to use it.

The traditional email - so there are two ways that email does security, that is, encryption. The way it has traditionally been is you connected insecurely, that is, on the standard email ports. Everyone who's like a port person knows that SMTP, the Simple Mail Transfer Protocol, was 25. POP, the Post Office Protocol, was 110. IMAP was 143. And then there was like an addition made to the SMTP protocol called STARTTLS, where the client and the server could negotiate a secure connection after connecting to the traditional ports.

The other way of operating is there are now other ports for those same three servers. Rather than using 25 for SMTP, 465 is like SMTPS, you could think of it that way. It's always secure. It assumes, the endpoints bring up a TLS tunnel before they do anything else, and then they do their business. And the same thing exists for POP. Rather than 110, it's 995. And for IMAP, rather than 143, it's 993. So you need things to be configured right.

And an email server won't have a client, at least initially for Let's Encrypt. But the certificate that the server itself gets would work just fine. So use Let's Encrypt for the HTTP server to get its security, and then just import that certificate into the mail server. And remember, I mean, I'm sure the mail server knows about the ports. But you'll want to make those high-numbered ports available for secure connections. And you should be good to go. So basically, yes, Let's Encrypt should work. But not quite automatically.

Leo: I may be - I must have misunderstood the question because I thought he - he says, "in an email client to achieve authentication and/or encryption." I think he might be talking about 509, not, you know, like a PGP or S/MIME style authentication encryption, which you couldn't use that kind of cert for; right?

Steve: Correct. And I guess that's why I was assuming he meant a standard security certificate, like a web server uses.

Leo: So you could use that for a mail server to give the mail server secure TLS-style conversations.

Steve: Correct.

Leo: Which in fact a good mail server will do.

Steve: Correct.

Leo: But obviously you can't use it for - if you mean authentication and encryption for your email, no.

Steve: Correct.

Leo: Just for transport.

Steve: Correct. Very good distinction.

Leo: Yeah, I'm not - it's not clear from the question which one he's talking about.

Steve: Right.

Leo: The good news is there are plenty of places you can get free email certificates, like Comodo I think offers them, and StartSSL offers them, places like that.

John User, I mean, Meuser, in Indianapolis, Indiana wanted to put Firefox for Android on our radar: I know iOS is Steve's mobile platform of choice, and Leo follows the latest tasty phone wherever it may lead, but I figured I would try to bring some attention to Firefox for Android. Which we just talked about, actually. In all of the discussion of mobile adblockers for iOS, I decided to check out the options on Android.

I was messing around with one of them when I realized, hey, it's Firefox for Android with a pre-installed extension and a slightly customized GUI. I've used Firefox for Android a bit, but it was never my daily driver, so I never really delved into Firefox's extension ecosystem. For a while I've lamented that, while we have a robust system of extensions on the desktop in Chrome and Firefox, in which we can tweak our experience to perfection, if you want something other than the default behavior on Android, you have to install separate browsers - LastPass integration, LastPass browser. If you want to prevent tracking, there's a Ghostery browser. If you want adblocking, there's an adblock browser and so on. Then you have to open links in the proper browser based on the behavior you're seeking. And if you get the wrong one, good luck.

All that was before I started exploring what extensions are available in Firefox for Android. I was pleasantly surprised. Steve's favorite adblocker, uBlock Origin, has full functionality, as does the LastPass extension and HTTPS Everywhere. Wow.

Steve: Yes.

Leo: This has motivated to make me run Firefox on my Android device. I thought I'd share my observations. I did not know that. I've been looking for exactly that kind of solution. That's great to know.

Steve: Yes. Yes. And we were talking about Firefox on iOS, where it's still apparently rarefied. But Firefox for Android apparently is universally available and represents a beautiful solution. So this is absolutely great. Thank you, John, very much.

Leo: I had no idea.

Steve: Yeah. And to be able to have on a mobile platform a browser that we know and trust, with an extensive extension ecosystem, that's fabulous. I mean, now we get to have all the goodies - uBlock Origin, LastPass built-in, and what else we want.

Leo: Yeah. Well, I really would - I like LastPass, and I would love to have adblocking. And HTTPS Everywhere is kind of cool, too.

Steve: Yes, exactly.

Leo: So does this support, I wonder, just the standard Firefox extensions? Or do you have to use special mobile extensions?

Steve: I've not dug into it.

Leo: I will let you know next week.

Steve: Yes, and in fact I have my little Samsung tablet here because I'm, like, the moment we disconnect, count the seconds, I'm going to fire this up and put Firefox on it and start poking around because that's a win.

Leo: Very positive reviews, too, for it.

Steve: Great.

Leo: Great. Thank you very much, John Meuser. And now we have completed 10 fabulous questions for Mr. Steve.

Steve: Right on schedule. Coming up on Tech News 2Night on the TWiT Network. And plenty of podcast for Elaine to transcribe. And by now she's finished changing all of the, what was it that was wrong?

Leo: Magnetos into Magentos.

Steve: Magnetos into Magentos, yes.

Leo: By the way, Bleak and others in the chatroom are saying, yes, it uses the standard Firefox extensions.

Steve: Wow.

Leo: Nice.

Steve: Fantastic. Yeah, I think that the extensions are just written in some controlled JavaScript subset.

Leo: Yes, that's right, yeah.

Steve: And so they ought to be portable across platforms.

Leo: Ironically, it's called Chrome. On Firefox. It's in the Chrome. Great. Steve is available at GRC.com for consultations, but you have to go through some special rigmarole. First of all, if you want to email him, don't. Go to GRC.com/feedback. That's where questions go. And he can't guarantee individual answers. Although he's also pretty responsive on Twitter, @SGgrc. And his DMs are open, @SGgrc. While you're at GRC.com, do get SpinRite, the world's best hard drive maintenance and recovery utility. Do check out all the other stuff. Somebody was saying we haven't heard about SQRL lately. What's the latest on SQRL? You're working?

Steve: Yeah. I'm thrown because someone suggested, just two days ago, suggested, wouldn't it be nice if we could use SQRL to log into LastPass because we know SQRL adoption won't be universal immediately. And even ultimately when it is, it'd still be useful to have LastPass as our vault. And the idea of logging into a local app is tricky. And I'm like, I've been thinking about it for a day, and it's like what I'm going to spend - I'm going to sit down this afternoon with my pencil and pad, because I don't yet have my iPad Pro to use with the Apple Pencil, and make sure there is not a way to solve the problem. It's very tricky because you'd want to use a third-party server for SQRL to authenticate to, and the app to authenticate to. And I've got the whole thing solved,

except there's a man-in-the-middle vulnerability that I haven't worked out yet.

And so anyway, the bottom line is the protocol is finally finished. I'm working my way through the protocol description pages. And the crucial one, I'm having to rewrite a lot of it because it's interesting, as I'm reading what I first wrote a year ago, it's like, okay, that's no longer right. That's no longer right. That's no longer right. And but there's a lot of things that are, like, way better. And so it's sort of a little bit of a time capsule for me because it's helping me realize how much work we've done in the last year, actually during this year, in 2015, to really fine-tune and hone this thing. So it's been time well spent.

Once the documentation is done, then there are a number - there's about six other clients, Jeff and five others, that are, like, waiting for the final final so that they can implement. And then I return to mine. There's been some changing of the wording because, again, it's been a while. And there was - for a while I was talking about changing your identity. And someone came up with the term "rekey." And that's such a - it's like the perfect word that fits what you're doing.

So I just have to go back to the UI. We've identified a couple bugs. I need to support corporate proxies that never occurred to me. So that, and so I've got to do a little more work. But we're really close. And all the server-side stuff at GRC is up and running. So once that's done, we'll do the full - I'll take it all public, and anybody who's got Windows or Linux with Wine will be able to download it and start playing with it. And then we're off to the races. So we're getting there.

Leo: I'm installing Firefox, and it's making me feel very old because, you know, if you have a Firefox account you can sign in. And I clicked the wrong button to create a Firefox account. And it says year of birth, and it gives you some choices, and then it stops at 1990. It says "1990 or earlier."

Steve: Oh.

Leo: Well, I guess I'm earlier, then.

Steve: I guess they don't care.

Leo: Earlier.

Steve: And Firefox now has a nice cloud sync. So you could sync your tabs among your devices so that, if you're doing work on your desktop...

Leo: Yeah, they've had that for a while, yeah.

Steve: Yeah, yeah.

Leo: They bought Xmarks, yeah.

Steve: Right. But I'm saying that, like, then you grab your phone, and off you go. And it's like oh, yeah, you're able to keep...

Leo: Chrome does that, too, yeah.

Steve: Yeah.

Leo: If you're over 25, we don't really care. Okay.

Steve: I'm going to have a problem, Leo, when I go past a hundred because it's going to be year of birth, and it's going to be, what, two years old?

Leo: Two digits? Well, they can't say that.

Steve: No, I'm 102.

Leo: 102.

Steve: Yeah.

Leo: Damn straight. That's why zebras don't get ulcers. They're not worried about the Firefox. What else? GRC.com also has, of course, besides all that other great stuff, the Password Haystacks, SQRL, and SpinRite. It's got the show. Steve puts written transcripts up there, also audio, in 16Kb and 64Kb versions. GRC.com. We have audio and video at TWiT.tv/sn. We do this show on Tuesdays at about 1:30 Pacific, 4:30 Eastern. That's 21:30 UTC, if you'd like to watch live. We love that. If you can't, on-demand versions of the show, not only at Steve's site and our site, but everywhere you can get shows. Everywhere, iTunes, whatever. Just look for Security Now!, 533 episodes. Thank you, Steve. We'll see you next week.

Steve: Okay, my friend. Talk to you then.