Listener Feedback #216

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-517.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-517-lq.mp3

SHOW TEASE: It's time for Security Now!. Yes, I'm back. Steve Gibson's here, too. We're going to talk about the latest security news, including that horrific story about hijacking a Chrysler in mid-ride. We'll also talk about Microsoft's zero-day update, just shortly after its Patch Tuesday, and answer your questions. It's all next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 517, recorded Tuesday, July 21st, 2015: Your questions, Steve's answers, #216.

It's time for Security Now!, the show where we protect you and your loved ones online with this guy right here, the Explainer in Chief, Steven "Tiberius" Gibson, who is living long and prospering because...

Steve Gibson: Prospering.

Leo: ...not only does he have a salubrious diet, he also is a secure fellow. Hello, Steve.

Steve: Hello, my friend. Welcome back from your three-week hiatus.

Leo: It was fun. And thanks to Father Robert for filling in. He did a great job.

Steve: Yeah, we produced some of the longest podcasts we've ever made because he engages me when I'm, like, ready...

Leo: Right, that's why I shut up.

Steve: Well, and so, yeah, so I've calibrated these over the years for, like, the length that I know we're going to go. And I'll be through with a topic, and he'll say, well, wait a minute. And then, you know. And I'm watching the clock, and we're 30 minutes in, and we're still on the first topic.

Leo: I've got to fill him in on the plan here.

Steve: You know, it all worked. We did some good podcasts.

Leo: Oh, no, it was great. In fact, all the comments I got was we really love Robert's interactions with Steve. And, you know, he really is - and I can interact with you more. I mean, I don't have a problem with that, I just - my observation was you kind of get a head of steam up, and I'm not going to get in the way of that train.

Steve: And how many times have we heard you say that, I mean, I've heard you tell other people that, if you interrupt me or interject, it throws off my...

Leo: I can see it happen.

Steve: Yeah.

Leo: Your eyes start to spin.

Steve: [Laughs]

Leo: So I don't want to throw you off. Well, Robert did it right, though. He waited till you were done, and then before you went to the next topic he would ask a question.

Steve: Oh, yeah, I mean, and it was fun because last week I realized I'd never had a chance to bring him up to speed on SQRL.

Leo: Yeah, good.

Steve: And it's been 92 weeks since the first mention of SQRL on the podcast. So I thought it'd be fun to engage him in that. And so I appreciated, like, being able to, like, spend some time and have him, like, grok the concept.

Leo: Good. Good, good, good.

Steve: Yeah. So it was great.

Leo: Well, I had a very nice vacation. It was a very - it was fun to be able to get away and relax. And I tell you, if you ever want to relax, a river cruise is the best way to do it. There's absolutely nothing to do.

Steve: And I've heard you saying that that's what you guys are going to do in the future. It's like, that was a win.

Leo: Well, I like ocean cruising. There's more to do. In fact, we're going on an ocean cruise, I think, for New Year's. And since we're taking Michael, who's 12, we're going on a ship that has more going on.

Steve: Right.

Leo: Because you don't want to bring a kid on a river cruise. They'd go nuts on you. They'd escape.

Steve: And did you have connectivity?

Leo: Yeah. Well, you know, you're not at sea. So I had a T-Mobile phone with me, and I had T-Mobile connectivity. We're in Germany, after all, most of the time. And then the boat has its own WiFi. It wasn't great connectivity. It wasn't enough, for instance, for me to listen to all the shows and things like that. But it was enough to answer emails and a few things.

Steve: And stay in touch with the world.

Leo: Yes. And I tried to. But I have to say, that's one thing I really miss when I'm not doing the shows is I just - the shows, like this show, keep me really up to date with what's going on. And when I don't come in every day and do a show with you and the rest, I kind of lose track. So did anything happen while I was gone?

Steve: Let's see. I think you know about most of the things. We know that I lost my T1 lines that I've had forever.

Leo: Yeah, tell me about that because - did you talk about that with Robert already?

Steve: Yeah, I did.

Leo: Oh, good. So you don't need to repeat it.

Steve: Yeah, because it was the first podcast with him that I didn't have them, and I was nervous because the one thing that T1s give us is I'm not sharing that connection with anyone else. So it is, in theory, it should be very low dropout and very low jitter. Whereas with cable, you know, my entire neighborhood is on the same cable segment that I am, or probably even a larger space than that. But on the flipside, it is 1:30 in the afternoon. And even if anyone came home for lunch, they're going now. And so I pretty much have the cable to myself while I'm doing the podcast with you. So we've seen, in fact I asked Elaine, since she focuses on the audio, I said, "Let me know how it sounds." And she said, "If anything, it's better than it was over the T1s." So I think...

Leo: Yeah, I mean, the difference between T1s and cable is the T1's more consistent, but it's a lot slower. It's less than 1.5Mb.

Steve: 1.54 each, and I had a pair.

Leo: Yeah. So, I mean, you probably have 10Mb up. What did you get?

Steve: I got the top-end Motorola modem and the Ultimate package, just because I didn't want to - I wanted to unthrottle it. So I think it's 150 down and 50 up. Although - and I have seen, when I was doing a Windows 10 catch-up after a couple days on my Windows 10 "let's see what this is all about" machine, I got about a hundred. So it's like, okay. It's like, it's actually there. But normally I'm not seeing that because they're not delivering that kind of bandwidth at the other end.

Leo: Well, that's one thing you learn when you get super bandwidth, is that you're faster than everybody on the Internet, so you don't really get any benefit to it.

Steve: Doesn't help much.

Leo: I think that the sharing versus the unshared bandwidth is overblown. I mean, I don't think a well-provisioned cable provider is going to have a lot of problems.

Steve: I agree. And that was also my feeling is that Cox is now selling home security, telephone, Internet connectivity, and video, all over the same connection. So if you've got phone service, we have bad power in this area. And there's a Cox van down at the corner immediately setting up generators in order to keep their local repeater running if power in the neighborhood goes out. So they understand having this up is not optional. Whereas Cogent was sort of, you know, scratching their butts, saying, okay, what's your account number again? It's like, okay.

Leo: Yeah, there are pros and cons on both sides.

Steve: Yeah. So the good news is, actually it was weird because during the Father Robert episodes we were just slammed with news. That was when the Hacking Team stuff happened, and all the zero-day exploits, as people dug through that 400GB of storage that got loose from them. And, I mean, it was - in fact, we were due to have a Q&A, and we had to punt it, as you and I have many times, because there was just too much news to talk about. However, this last week there were several high-profile events; but in general, just not a lot of paraphernalia.

So we're going to talk about this really sobering Chrysler problem that was found by some people that we've been following. Well, Charlie Miller, who's like the Pwn2Own king for years. Remember that two years ago we sort of - the way you could discount his auto hacking was that you needed a connection. He had the laptop set up on the fender of the car with, you know, it's like, well, yeah, but you have to have a connection. Eh, no more. Now you can hack Chrysler automobiles anywhere in the world, over the Internet. So that's...

Leo: Over the - oh, you don't even have to be proximate.

Steve: No. You just need the IP address, and you can scan for those. So we'll talk about that. Microsoft had an emergency update just days after, I mean, last Tuesday was their Second Tuesday of July, and they surprised everybody yesterday with, uh-oh, here's one more thing. And now we know that that was discovered from another Hacking Team zero-day exploit.

Leo: And what's most embarrassing is it affects Windows 10.

Steve: Well, yes. Well, it's in - this is, you know, one of the problems with OpenType is that basically it is...

Leo: Everywhere. It's everywhere.

Steve: It's Adobe. It's descended from Adobe's Postscript.

Leo: Right.

Steve: And it's an actual execution environment. So, I mean, it's a little interpreter that draws outlines of fonts. And it's interesting because some people have been moved to go back and look to reverse-engineer the binary. And just looking at it they have, like, enumerated all these flaws, which they then informed Adobe and Microsoft of. And back in March and April and May, they were quickly patching these. Well, this was one that wasn't found that way, that our friends at Hacking Team knew about, and who knows who else they'd sold it to.

So, and some news about RC4, the still being deprecated cipher suite. And we know from recent coverage that many banks still have RC4 as their first choice. There are some reasons that that really needs to get moved down. We've got a bunch of miscellaneous tidbits. And we're going to do a Q&A. We've got a bunch of great observations and

questions from our listeners.

Leo: I have them all here. All right. Let's get into the top stories here.

Steve: Okay. So this is - we're going to see several instances today of the standard security wisdom that attacks never get worse - well, worse in the sense of less capable. They only get more capable. Attacks evolve. And, I mean, and we've talked about this, for example, in the case of a buffer overrun, where when initially encountered, by default it crashes the computer because the attacker has managed to do something that the code wasn't prepared for, and it just goes off into never-never land. And then that offers a clue for the attacker then to start looking more closely at what route it took off into never-never land and begin to discipline that in order to achieve some nefarious end.

So similarly, two years ago, in 2013, Charlie Miller and Chris Valasek - who is with IOActive. And Charlie is a well-known reverse-engineer. He wins Pwn2Own competitions regularly because he knows how to look at existing systems and find vulnerabilities. They started looking at, let's see, two years ago they bought two cars - a Prius and I think a Ford, I don't remember now exactly which, but two cars - and using some DARPA-funded money to look at exploit prevalence. And they began plowing into these.

At one point, as part of this sort of officially DARPA-sponsored project, they sent questionnaires to 16 different car makers, asking them about their security practices. Based on the answers they received, they said, hmm, you know, Chrysler seems not to be really on the ball here. So let's take a closer look at their technology. To make a long story short, they will be, unless they're sued into oblivion and locked up before mid-August because, I mean, they're planning to demonstrate...

Leo: Oh, is this for Black Hat?

Steve: Yes, for the upcoming Defcon Black Hat security conference in the middle of...

Leo: We always look forward to this time of the year because that is a whole bunch of stuff. And these guys all save it up. They save it up. They know.

Steve: Yeah. So they notified Chrysler some time ago. Chrysler - and there it is. This is the guy's brakes not working. His brakes have been disabled. Meanwhile, those guys were at home on the couch, doing this over the Internet.

Leo: And that's what's really scary to me.

Steve: Yes. They did a scan, and they found on the order of 471,000 Uconnect-vulnerable vehicles. So here's the takeaway for our listeners and any friends you have that you care about. This thing is called "Uconnect," so you probably know if you have a Chrysler vehicle equipped with Uconnect. It is, you know, this is the bad stuff that we've, on this podcast, I've been saying for years. This is a bad idea. It's like, yes, everybody wants features. But there's no - we haven't proven yet we know how to do this securely. So what these guys found is a way to connect to the car over the Internet and get to

some firmware modules which are rewriteable. And they rewrite the firmware on the car, which gives them access to the CAN bus. And as we know, the CAN bus is this bus that, you know, CAN is sort of like, you know, we have an Ethernet bus, and we have a USB, and we have a Firewire...

Leo: Wait a minute. They put their picture on his car? Is that one of the things they did?

Steve: Uh-huh. Oh, yeah, they completely took over his instrumentation.

Leo: Oh, this is horrific.

Steve: Changed the channel. Turned up the volume. Disabled his volume control. There he is, trying to turn it down, and it won't go down.

Leo: Now, we had two other guys on the show talking about similar vulnerabilities. Is this the same or different?

Steve: This is different. But this is, I mean, this is the same genre. This is the same problem.

Leo: Because the CAN bus is on everything.

Steve: Yes. The CAN bus is the universal glue among - oh, and they also killed his engine. They disabled his transmission - he went into neutral - then cut his engine. And this was all over the Internet, remotely.

Leo: Wow.

Steve: Yes. So...

Leo: I mean, the demo that they gave us when they were on was not over the Internet.

Steve: Correct.

Leo: They had to be next to the car; right?

Steve: Correct. Well, what happened is Chrysler said, oh, let's allow people to do Internet crap. Who knows what you can do with this.

Leo: Well, my car does that, too. I have a T-Mobile SIM in my car, and I have 3G access.

Steve: Yeah. Well, these guys use Sprint, so this is a Sprint system. And all the cars on the road are broadcasting their location.

Leo: Oh, geez.

Steve: These guys know where they are, how fast they're going, where they're located, what kind of car they are. They're able to, by changing the firmware, that gives them Internet access to the car's CAN bus. And then it's just a matter of how much time they've spent hacking. So they can kill the engine, cut the transmission, disengage the brakes, or abruptly put on the brakes. They've got steering override in reverse so far on the Jeep. And they can track the car by GPS, measure its speed, and even drop pins on a map in order to trace its route.

Leo: Ay, ay, ay.

Steve: So anyway, so I wanted to say, for people who have Uconnect-based Chryslers, the good news is there's a patch. The bad news is Chrysler cannot patch it over the air, which I think is crazy, I mean, for them not to have a means to do that.

Leo: You have to do it yourself, by hand.

Steve: Yes. You can download it and use a USB thumb drive to patch your own car, or you can take it to a Chrysler dealer. So what you want to do is go to driveuconnect.com/software-update. So again, www.driveuconnect.com/software-update. You put the VIN number of your Chrysler vehicle in, and it will tell you whether your vehicle needs this patch. And you're able to download it and apparently do it yourself.

Now, what this of course means is that we know what small percentage of users are ever going to - or drivers are ever going to know about this. Our listeners will, and all of their friends will who know that their friends have Chryslers with Uconnect. But the problem is, I mean, this is a big problem. I mean, this is, I mean, these guys are planning to talk about it in less than four weeks. I think it's the 12th through the 14th. Oh, no, that's the USENIX Conference. But it's around the same period of time is the August, mid-August...

Leo: I know this because you're coming on The New Screen Savers the following Saturday.

Steve: Right.

Leo: To tell us what we have to watch out for.

Steve: To talk about what just happened.

Leo: Oh, man.

Steve: So, yeah. So this is as bad as it gets. It is scannable over the Internet. These guys, once they knew what to look for and what IP address block the Chrysler Uconnect vehicles have, they're able to scan for them. And they were, like, picking them off all over the country. If anyone's interested, I've got the link in the show notes. You can probably - it's a Wired article. The Wired article was titled "Hackers Remotely Kill a Jeep on the Highway - With Me in It," is the Wired article. It's a great article. They go into a great deal of detail and depth.

Leo: And that's where the video that we were playing comes from.

Steve: Right. So forward that to anyone you know with a Chrysler vehicle. This is not - these guys, because it tends to be vehicle specific, that is, the actual exploit of the defect that they have found, they focused on Jeep. But they were finding all kinds of other Chrysler vehicles scattered around the country by scanning for them and were able to determine that there are, eh, about a little less than half a million of these, 471,000 Uconnect-vulnerable vehicles.

Leo: And I should say this isn't really a Sprint issue. That's just how they're connected.

Steve: Correct.

Leo: This is an issue of how the car software works.

Steve: Correct. Sprint is the carrier that Chrysler made the deal with in order to put those...

Leo: Right, just like I have T-Mobile in my Audi. It's just, you know, just what they use. Now I'm worried about my Audi.

Steve: Well, I mean, it's really a problem. I mean, we were talking about airliner hacking a few months ago, and the question about whether the entertainment system was firewalled.

Leo: Was there an update to that, by the way? Did I miss anything?

Steve: No one ever - no, we never got clarity. It seemed like the guy was exaggerating.

Leo: Or making it up.

Steve: Exactly, and also just synthesizing, you know, prevaricating. So, but, I mean, it raises the issue. Now, there's no question, apparently the way in is through the car's entertainment system. So there is a linkage. The problem is the auto manufacturers are trying to minimize their cost. So they did not set up disconnected networks. And in some cases, some of the features that they want to offer require that the car's internal systems have access to the Internet. Clearly this has not been done securely.

And, I mean, this is a disaster for Chrysler. Again, I'll be surprised if there isn't an injunction to prevent these guys from making their presentation. They're not going to share the reverse-engineered code, which is a key portion to this. I mean, they needed to reverse-engineer a processor's firmware, which they did, and then they wrote their own firmware. What's shocking is that, with no contact, they're able to upload replacement firmware through this patch. Which makes you think that Chrysler ought to be able to fix this over the air, too. But they're just not equipped to do that.

Leo: They're not as sophisticated. Oh, man.

Steve: Yeah. They don't know as much as the hackers do about their own technology. So, I mean, I think this means they're going to have to do a recall, and they're going to have to send people, you know, in the old-fashioned way, take your Uconnect vehicle into your service center immediately.

Leo: No, they need to do that. And if they don't, they'll be forced to, I think.

Steve: Yes, yes. There would be a class...

Leo: Yeah. Because you said exactly the right thing, which is no one's going to do that. They're not going to know.

Steve: Well, and imagine if even the bad guys didn't want to hurt anybody, but wanted to be nasty, they could brick the autos. There was an instance where - remember that there was a story we covered a couple years ago about a disgruntled employee who used a system which was in place to kill cars that were behind on their payments. And he killed about a hundred cars that way, just bricked them.

Leo: Yeah, right.

Steve: So they wouldn't work anymore.

Leo: But that was aftermarket stuff added by the loan company.

Steve: Right, the leasing agency.

Leo: For this very, yeah, for the very purpose of getting a deadbeat. And they even said, oh, we would never do this when the car's moving, although I don't know if there's any way of preventing that. But they would never do it while the car's moving. Just, you know, they brick it when it's sitting outside the house.

Steve: Yeah. So imagine if half a million Chryslers just were dead.

Leo: Well, and already members of Congress are tweeting, we're going to make a law, there ought to be a law. I don't know what the law would be, but there ought to be a law.

Steve: Well, and look at the Office of Personnel Management. One thing you probably caught while you were on vacation, Leo, was that of that 21.1 million records, which was the latest count from the second of the two breaches, there were 1.1 million fingerprint images that were stolen, that is, 1.1 million individuals' fingerprint images were among the data stolen. So their biometric data was part of this. So, you know, no one seems to be able to secure anything.

Leo: Yeah. Yes, that's kind of the bottom line, isn't it.

Steve: Yeah, it really is.

Leo: No one can do crap about this.

Steve: And you know, remember the famous mistake, it was Ford and the Pinto, where it came to light that Ford understood that, if you rammed, if you rear-ended the Pinto in a certain way, that the brake lights could short out and cause the gas tank to explode. And the bean counters calculated that, well, it would cost so much to recall all of these Pintos that, frankly, we're better off just dealing with the individual suits which arise from those that do actually explode.

Leo: Criminy.

Steve: And unfortunately, this comes down to economics. It's very much like the code which is used for mission-critical space shuttle stuff is so expensive to produce because the cost of failure cannot be tolerated. But it really is incredibly difficult, which means expensive, to produce code which is mission-critical. And the fact is there's really no pressure on automakers to do this. They're pushing features to market. Their engineers say, oh, of course, it's completely bulletproof, don't worry. But what software engineer at

Microsoft didn't tell that to Steve Ballmer? And when has Windows ever not had a month full of patches?

Leo: It's bulletproof, Steve.

Steve: Yeah. Remember XP? It's the most secure operating system we've ever produced. Yeah.

Leo: Somebody's pointing out in the chatroom, by the way, that this Uconnect firmware download is on a nonsecure site. No problem there.

Steve: Okay, yeah. So meanwhile, we Windows users got a surprise patch after last Tuesday's. It wasn't very eventful. There were some things, I mean, it was like, yeah, it's a good thing to patch it. There weren't any huge problems. But this, we got another one yesterday which patched the entire range of Windows. And I got a tweet from somebody who applied the point-of-sale patch to his XP SP3. It, too, was patched.

Leo: Oh, good. That's that little weird hack that we were sure Microsoft would turn off, and they never did.

Steve: Yeah. Yup. And in fact...

Leo: You say you're not Windows XP, you're Windows XP Embedded. You still get updates. And it fixed it. That's good news, that it fixed it.

Steve: Yup. Well, what this does tell us is this thing...

Leo: Goes back. Goes way back.

Steve: ...has been there from the beginning, from the beginning of time. Yes. And it is a problem such that, if a bad guy arranges to get your browser, your Windows-based browser - I don't know if this is IE only, or if it's - I don't think it is. I think it's any browser that uses Windows to render OpenType fonts, which is down in the kernel. A particularly maliciously crafted font can cause your system to be taken over remotely, just by displaying the page. So user does nothing. This just happens to you. And this was found amid the treasure trove of exploits that the Italian Hacking Team's breach revealed. So anyway, that's something good to patch.

Leo: You pointed out at the beginning of the show that OpenType fonts are really not fonts. They're a program. They're Postscript.

Steve: Yeah.

Leo: But that's true of TrueType, as well. TrueType fonts are also programmatic. And I think all the fonts on your computer, they don't do bitmap fonts. They haven't done that in ages. They're all little mini programs. And we've had TrueType exploits before, too.

Steve: Yeah. And unfortunately, based on the review that I recently saw of the quality of code, the guy that reverse-engineered it just had his head in his hands. Everywhere he looked, without even - he was a white hat hacker who found, just by reading the code, nine or 10 brand new exploits that he then told Adobe and Microsoft about back at the beginning of the year. And they were patching them in March and May.

Leo: Wow.

Steve: And this was just doing a read of the code. It's apparently unbelievable low-quality code from Adobe. Who would have imagined that Adobe would have a problem?

Leo: There's no program we can't break.

Steve: Oh, boy.

Leo: Wow, wow.

Steve: So on the topic of attacks never get worse, they only get better, a paper to be presented at the mid-August USENIX security summit in a month, the paper is "RC4 No More." And there's a site, RC4NoMore.com, where they have an awkward acronym. They turned the "no more" into - I can't read it, but you can.

Leo: I'm sorry. I just ate something. Numerous Occurrence MOnitoring & Recovery Exploit.

Steve: Right. So there we have an acronym. So we've talked about the problems with RC4. Quick review. RC4 is based on an elegant, incredibly simple, but it now turns out a little too simple, random bitstream generator. The actual algorithm is a study in simplicity, two 256-byte arrays. And the key is they're initialized zero to 255 values. And then the key for the cipher, which is actually a key for the pseudorandom stream, is used to prescramble the arrays. And then you say, okay, start giving me pseudorandom data. And it spits out pseudorandom bytes. And the algorithm is then an XOR. You simply XOR this pseudorandom data with your plaintext. And although it's counterintuitive, you just wouldn't think that inverting random bits of this plaintext could produce something that's cryptographically strong, it actually is surprisingly strong. And in fact, if the pseudorandom data was high quality, it would be unbreakable.

Leo: Ah.

Steve: But that's the problem, is it's not quite good enough. So we've been talking about RC4 problems for a while because remember that the original encryption of WiFi used this RC4 cipher, specifically because it wasn't appreciated at the time that it wasn't very secure. And it seemed like it was good enough. Then cryptography got better. We started looking at it more closely. We began to see that there were problems with it. You know, the early WEP encryption had many problems. Only one of the many was its use of RC4, which is why we've moved away from that up to AES cipher, which is substantially stronger.

So when we first started talking about this, the way you broke this was by causing a browser to make an incredible number of requests. And the individual requests needed to be captured. And by analyzing them, you could find the subtle - you could discern the subtle differences from perfect entropy that was being generated by the RC4 cipher.

Leo: Wow.

Steve: Now, when I say "lots of requests," I mean...

Leo: Thousands.

Steve: Back then, 13 times 2^30.

Leo: Oh.

Steve: Yeah.

Leo: That's a lot.

Steve: Yes, 2^30.

Leo: Many, many, many.

Steve: So, yes. And back then, at 1,700 requests per second, it would take more than 2,000 hours. So imagine your browser is spending 2,000 hours doing nothing but generating 1,700 requests per second. Basically it's just slamming these requests. And then they could obtain a 16-character cookie value. And the assumption was that would be the session token, and that would allow them to hijack your session. Okay. What's been improved since then is we're down to 75 hours.

Leo: Oh, they're using the Fluhrer-McGrew biases. Well, no wonder.

Steve: That's true. There are two biases in the RC4 key stream. There's one where two consecutive bytes are known to be biased, slightly biased toward certain values, and a

different bias where a pair of consecutive bytes may be a little likely to repeat themselves.

Leo: Wow. So this is really a very minor missing entropy. I mean, it's not like there's long strings of repeated numbers, as we've seen in pseudorandom number generators. This is like a flip of a coin.

Steve: Right.

Leo: Kind of like a bias towards tails kind of a thing.

Steve: Yeah, where, exactly, if Washington didn't have such a high brow, or, wait, no, Lincoln. Is Lincoln on the copper penny?

Leo: Or a buffalo, depending on how old you are.

Steve: Anyway, yeah. So, yes. Or if it hadn't spent so much time in the vending machine, then it wouldn't - it'd be a little more 50-50. So tiny, tiny, tiny variation away from pure entropy, such that you have to get an incredible number of samples, and then find the bias. But by understanding the nature of the bias, they know what to look for better now than they did. And so they've cut it from 13 times 2^30, all the way down to 9 times 2^27.

Leo: Well. So really, so this is still impractical; right? I mean, wouldn't somebody notice?

Steve: Yeah. This is the meat for, like, research papers. Again, we don't blow them off because these things only get better. They're not getting better very quickly, but they're getting better slowly enough that we have enough notice to move away from this. And as you say, Leo, yes. If something - if your browser is saturating your bandwidth doing nothing, then it's time to close the page because something malicious somehow got in there, and it's causing your browser to make all these - and they're doing it, their 75-hour attack is they've managed to get it up to 4,450 requests per second. So it's just going crazy. It's just making an incredible number of requests in order to decode a few characters that are presumed not to be changing during that period of time. Crazy. Okay. That's all of our news.

Leo: Wow.

Steve: Now, you're probably behind on your "Mr. Robot" episodes.

Leo: I still have only seen the pilot. I have a lot of roboting to do.

Steve: I envy you because you can watch them asking what some people are beginning to ask.

Leo: Ah.

Steve: We know - yes. We know that Elliot talks about, like...

Leo: It's like "Fight Club."

Steve: ...someone like a friend, like he has a - we know that he's in therapy, and he's a druggie. But he also sort of has this other...

Leo: No spoilers.

Steve: Well, but I don't think this is a spoiler.

Leo: If you've been watching it, you're starting to think along these lines.

Steve: You're kind of wondering. And now people are tweeting it. So I figured, okay, it's kind of getting out there. Is the Christian Slater character Elliot's alter ego? And some people that have been tweeting have said, you know, nobody interacts with Christian Slater except Elliot.

Leo: Yeah. And he keeps appearing in what really must be magical ways. I mean...

Steve: Remember that first scene, where he's sort of there on the subway with Elliot, sort of looking at him and talking to him. And then he's like, he seems to be, like, maybe interacting with the people that Elliot thinks might be following him.

Leo: Mm-hmm.

Steve: And it's like, oh.

Leo: Yeah. Even on Episode 1...

Steve: Correct.

Leo: ...I had odd, I had premonitions of something going on there.

Steve: Correct.

Leo: Because either that - and this is a problem when you watch a new show. You don't know if there's magic in this universe. Because it would have taken magic for Christian Slater to appear and disappear as he did.

Steve: Yup.

Leo: Or...

Steve: Or, yes.

Leo: Mm-hmm.

Steve: He's a little less solid than we...

Leo: Doesn't surprise me.

Steve: And, you know, Mr. Robot is sort of his moniker, too, instead of like a normal name. So, interesting. So I just think it's worth watching with that in mind. I think that enhances it rather than spoils it.

Leo: I think you're Mr. Robot, by the way.

Steve: Huh?

Leo: I believe that you are Mr. Robot. But we'll find out. Is that not where you were going with that?

Steve: I did, no, I was going to a tweet that I appreciated from Chris Rhodus, who said, "I wish I had not forgotten to pack my @harrys razor."

Leo: Oh, how funny.

Steve: "I've lost a quart of blood so far." So Chris, thank you, and thank you for the support.

Leo: I did pack my Harry's razor, I have to say.

Steve: Oh, I'm never going to forget to pack mine, although I don't go anywhere, so...

Leo: You don't go anywhere, do you.

Steve: I don't. Now that you're not going to be doing the New Year's, that's the only time I ever get on a plane is when I'm coming to see you. But...

Leo: I thought you - if I had your life, I'd travel a lot. Why don't you travel? Do you not like...

Steve: Not if you had everybody asking where SpinRite 6.1 was.

Leo: Well, yeah.

Steve: While I'm working to get SQRL done. So, yeah.

Leo: No traveling for Steve.

Steve: So everybody knows I'm working.

Leo: Do you not like to travel? Are you not a traveler?

Steve: I'm really not a traveler. See, for me, if I travel, I enjoy it. But then I come home, and I'm right where I left off. So it's like, oh, okay. Well, I didn't get any work during that.

Leo: No forward progress.

Steve: Yeah. So I'd just rather - I'm happier when I'm moving things forward. And we've had some great, great, great results with SQRL in the last couple of weeks. I had intended, in my last week's recap, because I called it "SQRL Revisited," I wanted to talk about the innovations that we've had. But all I ended up doing was, like, sort of going back over what we'd already discussed. But I did describe it in a way that many people really grokked it.

Leo: Ah. Sorry I missed it. I'll go back and listen to that episode.

Steve: It was really worthwhile. And in fact I did, there was a huge amount of feedback about it. So I did let three of our 10 questions be about that today because there's some people had some great follow-up from what they now understood from that episode.

I did want to mention that the PDP-8 kits are arriving. And I got a tweet, or I saw a tweet, who did an @SGgrc, from Baigent or Baigent who said, "Just received my PDP-8 kit from Oscar. Well worth the wait. Now need to find a quiet space to geek out." So he'll be putting that together.

Oh, and our friend Taylor Hornby tweeted something. And Leo, I think this is for you. It's a Kickstarter project. I tweeted it yesterday. The guy who's doing this has a computer-programmed loom and is weaving custom, no-two-are-alike scarves with a really - it's based on a cellular automata pattern.

Leo: Oh.

Steve: So no two are alike. It's called...

Leo: So these are Martin Gardner scarves.

Steve: They are. Well, we all know Martin Gardner from the classic cellular automata was the game of Life, where you had a grid of cells, and the rules for whether you would have a new birth, you would stay alive, or you would die in any given cell. So he's come up with rules for his cellular automata. And this is pure geek land. But he's very close. I mention it because there's only 44 hours left, so less than two days remaining.

Leo: And he has fully funded, I see. He's over a hundred thousand.

Steve: Oh, fantastic. Last time I looked he wasn't. He was way shy of that. So I'm glad that he got some attention. Anyway, I funded because...

Leo: Oh, it's not a guy. It's her.

Steve: Oh, it's her. Why did I think it was a guy?

Leo: Fabienne Serriere.

Steve: Nice.

Leo: I think this is cool.

Steve: I thought you would. And it is not cashmere, but it is a very soft wool.

Leo: It's merino wool, which is nice, yeah.

Steve: Yes, that she likes better than cashmere. And I just love the idea of a geek scarf. In Southern California, odd as it may seem, it does get cold - for like a week - and I'm glad to have one. I do wear a scarf during the winter down here, and I'm going to be wearing a digital scarf.

Leo: Oh, I can't wait. It says she's a hand knitter and a mathematician. So the perfect person to do this.

Steve: And look at, if you scroll back up, you'll see the algorithm generating - I think she shows it a couple places, you could see...

Leo: Oh, on the video, yeah.

Steve: No, it's not, I think it's on the web page. You can see the algorithm generating, actually doing the cellular automaton - there. Oh, there, there. It's actually generating it right there, following the rules of the cellular automata to create the pattern for a single scarf. No two are alike.

Leo: So Conway created the Game of Life, but Martin Gardner popularized it in his Scientific American column.

Steve: Right.

Leo: That's how I first learned about it as a kid, I think.

Steve: John Horton Conway, I think it was.

Leo: Yeah, yeah. But this isn't the Game of Life. It's something similar. There are people who are still actively, this is like their hobby, is cellular automata and so forth.

Steve: Yeah. It's an engaging idea, I think, the idea that you can have, I mean, it's intellectually intriguing. You have a very simple set of rules which you apply to a grid of cells. And there are some that are sort of two-dimensional, sort of like hers was, where you have a single line, and you're evolving a line over time, or, I'm sorry, like one-dimensional; or two dimensional, where you have a grid. And it's like, you know, there's all kinds of strange things that sort of arise from a very simple set of rules. I think that's what's cool is the emergent property of what you can almost think is life based on a very simple set of rules. And there she shows what the rules are for her automata.

Leo: It's quite beautiful.

Steve: Yeah.

Leo: They're black and white.

Steve: Yeah, I actually like that rectangular one better than the triangular one, I think. But...

Leo: This is really neat.

Steve: I thought you'd get a kick out of it.

Leo: Very geeky. You are a geek.

Steve: Yeah, I am. As I've heard you often say, this is the geekiest of the netcasts...

Leo: Oh, easy.

Steve: ...the TWiT network produces.

Leo: Not even close. By the way - although I think we should try to get this woman on The New Screen Savers. If you want to do it, as Steve said, as we record on, what is this, July 21st, there's only 44 hours left. Search Kickstarter for KnitYak, K-N-I-T-Y-A-K.

Steve: Yes.

Leo: KnitYak.

Steve: Yes.

Leo: You're not going to get a knit yak.

Steve: And so just to clarify, she has a computer-controlled loom, and so she's programmed her computer to generate this. And if you're interested, there's a lot of really interesting background on, like, she really understands this stuff. Like the type of weaving she's doing is maximally efficient for both colors of yarn and blah blah blah. I didn't, you know, I didn't spend too much time on it. I just said, "I want one." So I got one.

Leo: They're kind of like fractals, almost.

Steve: Yes, they are, very fractal-like, yeah.

Leo: Very pretty, yeah.

Steve: Okay. So last piece is - I read this, and I thought, you know, hopefully Dan's wife is not listening to this. We have a listener, Dan Long in Elgin, Illinois, who experienced what he called "The Miracle of SpinRite." But it's not what you think. So he says: "The Miracle of SpinRite: My wife's laptop stopped booting. I had purchased a copy of SpinRite for my computer a year or so ago, so I started running SpinRite on her laptop. This drive had serious problems, so SpinRite took some time, during which my wife was getting impatient. I asked her to have faith in the process and let it finish." She wanted just to throw it away.

"I titled this 'The Miracle of SpinRite,'" writes Dan, "understanding that the function of SpinRite is not itself a miracle. It is a product of a deep understanding of the technology, and writing code to elegantly address that technology. The miracle occurred once SpinRite was finished. My wife was telling me that this would never work, and that I should just throw it out. I saw that SpinRite was working on the last region, the less critical slack space at the end of the drive. So I stopped SpinRite and rebooted.

"While my wife was mid-sentence, telling me how this was doomed to fail, the Windows logo appeared on her screen. And that is when the miracle occurred. My wife stopped in mid-sentence and was speechless. This was the first time in more than 20 years I have ever seen her speechless."

Leo: Oh, how funny. Oh, dear.

Steve: "That is the Miracle of SpinRite. Not only that, after this we were able to recover all of the data and move it to a new laptop. Steve, I want to thank you for your work in bringing that moment to me. I will treasure it always."

Leo: Oh, that's so funny. I hope she doesn't hear it.

Steve: So, Dan, I hope she's not listening to this.

Leo: Yup.

Steve: Hopefully you know better. And thank you for sharing your miracle.

Leo: All right. We're going to take a break. I've got questions; you've got answers. Our audience has provided us with the grist. You are the mill, the wind beneath my wings, Mr. Steve. All right, Steve, time for questions.

Steve: Yes. I should mention that our listeners have notified Fabienne that we were just talking about her.

Leo: Oh, good.

Steve: Her twitter handle is @fbz. And I just, while you were telling our listeners about PagerDuty, I checked the feed, and there was some dialogue back and forth.

Leo: Oh, good.

Steve: So she knows that we're fans now.

Leo: That's the most valuable thing, frankly. If you're doing a Kickstarter, the key is to get publicity because you've got to get your head up above the surf.

Steve: Yeah.

Leo: All right. Time for Q&A #216.

Steve: Yay.

Leo: Starting with Jonathan Adams in Chicago, Illinois. He's wondering about SSL cert requirements: Steve, with the increase in malicious payloads being delivered by SSL, do you see more stringent policies being enforced by public CAs? For instance, I don't know, making EV validation checks required, something like that.

Steve: Yeah, this was sort of an interesting question. It sort of threw me off for a second, as I was thinking about it. It's like, wait a minute. You know? Okay. So malicious...

Leo: I'm not sure I accept the premise, really.

Steve: Correct. That's the problem. But I thought that was an interesting premise to address. And that is, Jonathan, that that's sort of not their problem. So SSL is about two things. It's about privacy and authentication. Privacy is the encryption portion, which means that what is going over the wire is not in plaintext and cannot be sucked up without a tremendous amount of effort and then decrypted. And then the authentication portion is, because SSL is typically, or now TLS is typically authenticated at the server end, your client is able to absolutely verify that the thing you're connected to over the multi-hop, crazy, somehow-the-packets-get-there Internet is the server that you believe you're connected to. That is, it prevents what could otherwise be all kinds of spoofing problems.

So the role of SSL is to give you privacy and the assurance that you are hooked to who you think you are. The EV portion is only a stronger assertion of the second of those two. So that's what the extended validation, as its name sounds like, it's extended validation

of the identity of the corporation that you're connected to. Above and beyond just the domain name, it's like, no, this is a company. We've checked them out, and they're the company that has that domain.

But neither of those, neither the privacy aspect nor the identity, have anything to do with the maliciousness of the payloads. For example, as sites are going secure, their advertisers are needing to also be secure, to offer secure delivery of ads so that you don't have mixed content warnings saying, hey, some of the assets that you are loading are not secure on a page that is. So the ads are secure. So the ad servers and those connections are secure. But as we know, every so often some malicious ad content is served by the secure channel. Which is to say, these things are really sort of separate. We have privacy to an increasing degree. We have more assurance who we're connecting to at the other end. But what the data is that moves through is sort of disconnected from those two things.

Leo: Fair enough. So, good, because I don't want to do an EV cert. It's too expensive, for one thing. Dan Long, Elgin, Illinois, we're still in Illinois, brings up a great SQRL question, the first of three: In your talk at DigiCert about SQRL, you talked about needing to - so you did a DigiCert talk about SQRL?

Steve: Yeah, last November. I went to Vegas with the presentation, yeah.

Leo: Yeah, yeah, yeah, okay, yeah. You talked about needing to print your boarding pass from a strange and scary computer. My question is, what happens if your phone doesn't have a signal at that moment, and it can't communicate with the Internet? Is there a failsafe mode we can use? Perhaps there's a code we can enter to authenticate? Does SQRL work offline, I guess is the question.

Steve: Correct. And the answer is no. I mean, that is a requirement of this. We have, you know, SQRL works in two ways. It works in what we call same-device authentication, and cross-device authentication, meaning that you could have a SQRL client in your computer and just click on the QR code. And that client running in your computer will log you in on that computer. So that's same-device authentication. What I demonstrated with you, Leo, when I took a picture of the QR code that your laptop was showing over Skype with Jeff Arthur's iOS client, SQRL iOS client, that was very cross-device authentication because I was using a phone that had the SQRL client in it to authenticate a session that you were looking at. So it absolutely is the case that, in that mode, that your phone would need to have a signal.

Now, it wouldn't have to be a cellular signal. It could be a WiFi signal. But it would have to have access to the Internet because what's happening is that the phone is making a connection to the domain name in that QR code and then providing and proving your identity to the server at the other end. So you do have to have a connection for SQRL to work. That is something that there's just no way to get around.

I will say, though, that I don't expect that SQRL will probably ever be the only way of logging onto a website. I don't think that'll ever happen. I have no illusions about that. And I'm not even saying it would be good, for exactly this sort of reason. You could still have a username and password. They would just be a lot dustier than they would be if you have SQRL because that would be your fallback.

Leo: You'd rarely lose it.

Steve: Yup.

Leo: That's a good point. You still have the password available.

Steve: Yeah. And in fact we have a question that we'll get to here in a while about, like, how do you see SQRL and, for example, LastPass coexisting. But we'll wait for that.

Leo: Well, and also, I mean, it confirms my thought that SQRL is primarily an online authentication tool. I mean, it's for logging into websites. If you're not online, it's not exactly, I mean, I guess there are some uses for it. But it's not the primary use of it.

Steve: Well, exactly. And, for example, I think he was suggesting that the computer he's standing in front of might have, like, a wired connection.

Leo: Oh, it's online, but you're not.

Steve: Right.

Leo: Yeah, well, then you use your password.

Steve: Yeah.

Leo: Andrew McDonald in Odessa, MO wonders whether he's safe running in standard user mode: I seem to recall you saying in a previous episode that we are only vulnerable to the vast majority of security issues because we run Windows in Admin mode. I've become increasingly frustrated with the issues I run into while browsing with NoScript turned on, and I'm bothered that this is my only shield against the scum and villainy present on the Internet.

So here's my question: If I'm running as a standard, non-admin user, how safe am I? Would I still need to run NoScript to be safe on the web? Thanks for all the time and effort you put into the show. I've been listening for years, first started using SpinRite in '89 to keep a 20MB hard drive working.

Steve: Actually, I think I wrote SpinRite on a 20MB hard drive.

Leo: One of those fine Seagate MFM drives, no doubt.

Steve: Ah, yup, yup. So, okay. So I just sort of thought it was worth revisiting this

because it's something we really can't say often enough. And that is, there's this concept, another fundamental principle in security, known as the principle of least privilege. Meaning that, in general, it is best to operate with the least amount of privilege.

Now, running NoScript is that. It's sort of, you might argue, an extreme example of that, where we've removed scripting privilege from our browser completely, so that unfortunately, sites that depend upon it are broken until we go, okay, fine, for this site I'll turn it on. And then you raise the privilege to allow scripting to function. But that's just one, the scripting privilege is one of a multidimensional set of privileges that exist in security. A key one is the one that Andrew mentions, and that is the so-called admin mode, or root, as sort of the equivalent infinite power that you have in Linux or UNIX, where a user who is logged in as the root user, much as Windows as an administrator, has no OS-imposed barriers. They can delete directories. And, you know, they're the administrator of the system.

The danger is that - and here's the key to your question, Andrew, is that almost all of the exploits which we see occurring involve something happening, not by design, sort of an exceptional case, where you as the user are running a program. Maybe it's your browser that you're running. And something, there's a mistake in the code that allows the code that's running in your browser to escape from the browser's sandbox, as it's called. It's able to get loose. You don't want it to get loose from the webpage; but there's a mistake, so it can. When it gets loose, it essentially impersonates you. It becomes you from the standpoint of the operating system, meaning that it has the privileges you have.

So if you are running as an administrator, then the code has administrative privileges, too, just like you do. It's running in your user space. So that's not good because it can install things and have much greater access to a full run of the system, essentially. And the fact is our OSes have been designed so that you can completely use them in a much-constrained environment, as it's often called, as a non-admin or as a regular, or sometimes it's called a limited user. And no one should think, you shouldn't feel like it's like privileges that you need are unavailable or that there's anything wrong with you running as a limited user. It's actually one of the best things you can do.

Again, it's this issue of least privilege. A limited user typically cannot install or remove new programs. Well, that's a good thing, if malware has gotten into your user space, and it's trying to install itself on your computer. You don't want it to install, so you want that barrier. And the fact is, most people are not installing and removing programs all the time. So what that means is you could change your privilege to an admin user when you needed to install or remove software, but otherwise run as a limited user, not with administrative privileges. And so then you're following the principle of least privilege because you're not able to install and remove and do other things to your system, but neither can malicious code that somehow you inadvertently run. And another classic example is CryptoLocker. If you are a limited user, CryptoLocker is unable to get to your Windows session backups. Can't remember the term in Windows.

Leo: System restore points or...

Steve: Restore points, yes. Restore points are outside of a limited user's reach, so they are also outside of CryptoLocker's reach. So if you get infected with CryptoLocker, but you're running as a limited user, you can recover the files in the state they were when the last restore point was made - which, I mean, that can completely save you.

So I can't say that, well, in Andrew's case he's saying NoScript is a pain. I get that. I

completely understand it. I would argue that running as a non-admin user is a great thing to do instead of, or in addition to, the idea being that the other concept that we have in security is multiple layers of security. You don't want to rely just on one thing. You'd like to have multiple things. And so running as a limited user and using NoScript is better than using either one by themselves. But I would say definitely experiment with running as a non-admin if you are in the process of saying that NoScript is too big a pain.

Leo: Question 4 from Advait - or something like that - in India. He reminds us of Sandboxie.

Steve: Ah.

Leo: Steve, in Episode 514 you talked about the pros and cons of NoScript. I used NoScript for a long time, and it was always kind of annoying. You had to allow some scripts for some sites for the site to function. Our site, for instance, does not run without JavaScript. And of course running any script is potentially risky. One day a light bulb went off, and I got Sandboxie. Now, I always run Firefox in Sandboxie, along with an ad blocker, but without NoScript.

Now I can browse all over without worrying about bad scripts. I know Sandboxie's not perfect, but it's been around a long time, and it's always being improved. Now my browsing experience is much better and, more importantly, safer. It seems that Sandboxie is one of the best tools out there to greatly reduce the risks of browsing around. Thank you for all you do. Advait, SpinRite evangelist for South India and happy member of both GPM, that's Gibson's Paranoid Minions, and SAFER, Steve's Association for the Elimination of Risk.

Steve: Well, our longtime listeners will know that we did a podcast on Sandboxie, and that I am bullish about Sandboxie. It is a very nice solution. And I agree, just as Andrew was talking about an alternative to NoScript, here's another alternative to NoScript, and that is to use Sandboxie. The name is from Sandbox IE, as in Internet Explorer, but it has been expanded over time, and it is a good sandbox for Firefox, as well, and Chrome.

The idea is that it's a program which hooks all of the operating system access for any programs you run inside it. We've talked about virtual machines, where you have a VM. A VM, a full virtual machine is sort of a heavy-duty sandbox. This is a lightweight sandbox which runs as an application. And then, when the program you run inside it, like a browser, starts itself up, Sandboxie is able to intercept the browser's access to the operating system so that, for example, things you read and write, like modifications to the registry, modifications to the file system, any sort of permanent things you do, even modifications to cookies that the browser is trying to save, they are intercepted and sort of redirected into a holding area so that the browser can read them back while it's running. But when you shut it down, when you close the sandbox, all of those changes are wiped away. They're eliminated. So the idea is that nothing bad can escape from the sandbox.

Now, browsers have their own sandbox, as I mentioned before. But we keep finding mistakes, which allows code, malicious code, to escape from the browser sandbox. So as Advait mentions, putting the browser in your own sandbox, that is, in Sandboxie, gives you another layer of protection. And I would argue that it's very good protection. And, yes, you could use it as an alternative to NoScript. So I wanted to remind our listeners

that Sandboxie exists. And for anybody who finds that managing scripting constantly is more than they want to put up with, you might consider Sandboxie because it does not get in the way.

Leo: Question 5, John in Lethbridge, Alberta, Canada wonders about relief from CryptoLocker: Just curious if there's a solution on this CryptoLocker virus I've been hearing about. A close friend of mine just got hit with it. That's how I found out about it. I'm wondering, how do we get around it? Don't get it, John, don't get it.

Steve: Exactly. We've talked about CryptoLocker a lot. We also immediately identified this as something that was not going to go away soon because, unlike other viruses, which have just sort of been mischievous, this thing, CryptoLocker, is making the miscreants behind it some serious coin. And in fact, it's funny, I saw some other communication from a listener who has a friend who got hit by it and had to pay with bitcoin. And he came away saying, boy, you know, I helped him figure out bitcoin. That thing's not ready for the mass market yet. So it's like, no, it does take a little bit of work to make bitcoin payments happen.

So anyway, John, to answer your question, the CryptoLocker virus, as Leo said, you don't want to get it. I would say a perfect example of protection, as we just mentioned, is running as a non-admin user. If you're running as a regular user, or a limited user, then there is recourse from CryptoLocker in that you're able to do a system restore and recover to the restore point that was made prior to that infection, which may be all that you need. Another, of course, is backups. Keeping your system regularly backed up will prevent CryptoLocker from being able to get to your backups. And then Sandboxie, as we were just talking about, is another thing. You could run your browser inside Sandboxie, probably see no sort of problem, and CryptoLocker would be prevented from being able to escape from the Sandbox. So basically the sort of things we talk about on this podcast all the time.

Leo: Do we know what the most common vector for CryptoLocker is? I bet it's not browser. It's probably email.

Steve: No, it's phishing emails.

Leo: Yeah.

Steve: Yes. It's phishing emails.

Leo: And Sandboxie won't help you there; right? Or do they have an email thing now? They might. They keep extending it beyond browser, I think.

Steve: It might be that the link in email is to a malicious website.

Leo: Right.

Steve: So it fires up your browser. And then, typically, the most recent one was a Flash exploit, where it used a zero-day Flash in order to get code. So it's like this stuff, these guys are clever, and they're linking three or four different apps all together in order to pull this off.

Leo: Of course they are.

Steve: Of course.

Leo: Aaron is writing to us, Aaron Cavender from Salt Lake City, Utah. He wonders about SQRL and LastPass: While SQRL, Steve's login process, SQRL, eliminates username and password authentication for websites, I don't see password managers like LastPass going away anytime soon. In fact, I could see LastPass incorporating SQRL. Wouldn't that be a good solution.

Steve: Yup.

Leo: Is there a meaningful way to use your SQRL identity with LastPass so there aren't multiple master passwords to remember? Is there a way I can prevent my dear, but not-tech-savvy, grandma from having to use both a SQRL client and a password manager? Seems to me both apps are trying to do the same thing, TNO decryption. So it seems to me that LastPass could never truly trust or defer to SQRL to store a master password or some decryption key, as that would break TNO. Am I right?

Steve: Yeah. So I have no illusions about this idea that SQRL's going to take over the world. My whole position has been that this is a workable, like a really workable, lightweight solution to the whole problem of usernames and passwords. And it has a number of features that distinguish it from FIDO, which is the competition to SQRL, such as it is. I mean, we're both emerging at around the same time.

And my feeling is that, if sites choose to adopt SQRL, it'll sort of happen organically, that sites where there's a low tolerance for creating a new account, like blogging sites, will say, hey, if we offer SQRL authentication, then users will not have to go through the regular account creation process, and that would allow people to more easily put up blog posts and prevent being impersonated and being able to come back and respond to answers. So it would reduce the friction on sites which are friction sensitive. And the cool thing is that users only need one SQRL authentication, you know, authenticator. They might install it in their mobile device and on whatever desktop machine they use. And then to the degree that sites use it, they could log in with SQRL.

And so clearly we don't know what the future holds. We don't know what the adoption rate will be. The whole thing just might not happen. But my feeling is I just needed to make it, like work out the details and give it the possibility of happening, and then let the industry decide if it makes sense. We see constant pressure from events on the Internet for a replacement for usernames and passwords. And I do know within our own community, I acknowledge that this is a special group that we have listening to this podcast, but there's a huge amount of interest in an alternative like this. So we'll just have to see. They will coexist because usernames and passwords will probably never go

away.

But what I hope to see is that, at some rate of acquisition, sites will recognize that it is easy for them to add SQRL authentication. And it will be easy. We've got existing packages for all the major web platforms that are on the way. Some are working now. And we're just working on nailing down the final details of the protocol, which would make it easy for sites to adopt SQRL over time. And so I'm sure lots of sites won't. Hopefully we'll see adoption happen over time and the SQRL option grow.

Leo: And we haven't shown the new SQRL logo yet, so you can go to GRC.com/SQRL, which stands for Secure Quick Reliable Login. Who did the logo? That's awesome.

Steve: Yeah, I ran a competition. There's a site called Logosauce.com. And so I offered a prize of $750 to a global group of designers, and someone named Marcos in Spain, who is a very talented designer, came up with that. We ran it for a month and got a whole bunch of submissions. And that one was just, like, that one just hit the sweet spot, memorable and symbolic of a lock with a hasp and a squirrel. So that's the project's logo.

Leo: Nice job. Like it.

Steve: Yeah. Really happy with it.

Leo: And I do, you know, you have a great relationship with Mr. LastPass, and I think that that's the kind of - he's already incorporated all sorts of other second-factor stuff, and he's very open to that.

Steve: Yep. I think Joe is probably just waiting for it to, like, settle down. One of the nice things about it, though, is that it is cross-browser, meaning that I've got Firefox and IE and Chrome and Opera, and I only need to install my Windows client once, and it automatically runs on all the browsers. So with LastPass you do install it in each browser. But most people are probably mono browser people. So, but you're right, it would make sense. It would coexist very well with LastPass. I wouldn't be at all surprised. And it would work well as a browser plugin, too. So I wouldn't be surprised if Joe is keeping an eye on it.

Leo: Oh, yeah. Yeah. That's a good point. But that would get you on mobile platforms, too, because LastPass has apps and et cetera, et cetera.

Steve: Yup.

Leo: Don's in Evergreen, Colorado. He can't scrape the Windows 10 off his system. We actually answered this question on the radio show, too. There's a little program that'll do it.

Steve: Yup.

Leo: Dear Steve, as you suggested a few weeks ago, I went in and uninstalled a couple of hotfixes, KB3035583 and KB2952664 and got rid of the annoying Windows 10 upgrade icon and the in-your-face upgrade offers. Windows immediately tried to re-install them as "Critical Updates," which makes me wonder, what the hell's "critical," anyway? I right-clicked on their attempts to reinstall and told Windows Update to ignore these two updates. All was well for a few weeks, until last Tuesday's Patch Tuesday, when they somehow snuck the upgrade offer icon and in-your-face messages back into my machine. Ay, ay, ay. I checked and, yup, KB3035583 and KB2952664 are not installed, so they did it some other way. Has anyone figured out how to remove them this time? My machine's been taken over by Microsoft Zombies.

Also, due to the articles from Germany, where their security agencies will not allow Windows 8, and I presume Windows 10, in any German government office due to Microsoft rolling out the welcome mat to the NSA via TPM, I'm sticking with Windows 7, running RAID for hard drive firmware protection, as long as Windows 7 is supported. And then, well, it's probably Ubuntu Linux after that.

Steve: So this is interesting. I'm glad you know about the little program. There's a program over on GitHub which it's got a funny name. It's like "Please stop trying to upgrade me to Windows" or something like that. And what I wanted to tell Don, I mean, I'm sure he knows this, and I know he would rather remove it. But if you can't get rid of it, you can at least hide it. And so the easiest thing to do is just to right-click on it and say "Hide this. I don't want to see this anymore." And so it slips it down over there to the left in your hidden icons region so that it's technically still there, but at least it's not in your face and presumably not popping up any longer.

Leo: Yeah, it's really annoying, isn't it.

Steve: Yeah. It's amazing that they're pushing it as much as they are. You'd think if you just said, okay, thank you, I got the message, go away and don't come back, that they would do that. But no.

Leo: I think the one, well, there's a couple. There's one that's called "I don't want Windows 10." It has a graphical installer. I don't want Windows 10. Then there's another one called, let's see, wait a minute, J2TeaM/Windows-10-Notice-Remover.

Steve: Yeah, the "I don't want Windows 10" is now at version 3.

Leo: Yeah.

Steve: So they've been moving...

Leo: Yeah, Microsoft apparently considers it a virus. Geez, Louise. Yeah, well, our long national nightmare will be over in eight days. That's all I can say.

Steve: You know, I have it, and I've been poking at it. I just - I guess maybe it's a matter of getting used to it. To me, it just feels like it's wasting screen space. Like everything sort of seems bigger and flatter, with big margins. And I'm just, you know, I want to use my screen. I don't want, like, big designer regions of empty space that look nice. It's like, if you'll get out of my way.

Leo: Eliz says the long national nightmare begins in eight days.

Steve: Yeah.

Leo: I guess it depends on which you hate worse, 8 or 10. You're going to go to 10, I thought you said. Am I wrong?

Steve: Yeah. Yeah, I think, well, I'm going to let it - I don't know. I have to decide if I - I have to see if I can get used to the UI. For me that's, you know, can I get it out of my way? And maybe the WindowBlinds guys will, like, give me an XP experience.

Leo: Oh, yes. Yeah, Stardock will for sure.

Steve: Good. In that case...

Leo: You want the XP - wait a second. I don't know if they'll have the XP experience. But they'll have something for you. Maybe the Windows 7 experience.

Steve: Okay.

Leo: The XP experience may be going a little too far.

Steve: It does seem a little - it seems a little retro for me to go to 7 because, I mean, I'm on XP mostly because it's just such a horrendous pain to go to a different operating system.

Leo: Right.

Steve: I have to start everything over again.

Leo: Right.

Steve: So I'm like, okay, well, if I'm going to make the jump, hold my breath and pinch my nose and...

Leo: Go all the way.

Steve: Go all the way.

Leo: Yeah. Well, we kind of all want you to use Windows 10 so you can suffer with us.

Steve: Yeah. And also I had to move to Windows Server 2008R2 to get the updated cryptographic suites because I was quite happy on Windows - I was running 2000, NT, you know, or, yeah, Windows 2000. It was fine because it worked, and all my security that I had kept me from being infected from anything. But it didn't have the latest technology. And if I'm going to make the jump to the next server, I ought to have a synchronized desktop because I need to cross-develop between this and server stuff, too.

Leo: Right. Gregg Kowbasa has our eighth question. He's in London with a SQRL conundrum: Hi, Steve. I was pondering something the other day which I assume you have an answer to. After listening to last week's Security Now! and finally really getting the concept behind SQRL, I was left wondering one thing: If it relies on the user's identity and the website's domain to generate authentications for websites, what happens if the site's domain changes?

Steve: Ah.

Leo: Microsoft has changed its email domain at least half a dozen times, and I'm sure many companies go through changes which require a domain change. Do users then get locked out of their accounts? Or is there some sort of built-in protection against things like this?

Steve: So first of all I should say that Gregg's question is a proxy for many tweets and a lot of other email that I saw about this. And he is exactly right. This is a problem. Because what I explained is that essentially, in the same way that ciphers have keys, where the key that you use determines the specific pattern of cryptography, what SQRL uses is a keyed hash, where the user's identity is the key to the hash function, so that essentially all SQRL users have their own personalized hash function. And so we put the web domain into the hash function, and out comes the private key. That's the essence of SQRL. So every SQRL user with a custom hash function hashes the same web domain and gets a different private key. And that allows them to come back later and rehash the same web domain and reproduce the same private key. So it's an elegant system. But it does lock their identity to the web domain.

And so this is something that one of the very first things we looked at carefully was is there any way to solve the problem. And the answer is no. Anything that we might do to give the domain owner some sort of variation, some variable, some means to break that association, completely breaks the system. That is, one of the main security guarantees is that the SQRL identity and the domain name produce the private key. That's what makes that private key, and in fact the public key that you give to the website as your identity, it makes it useless to anybody else because no other person has control of that domain.

But so what we have is a process which a website could use to sort of mitigate this problem, and that is, typically a site isn't losing control of their domain, but for whatever reason they're, like, saying, oh, we have a better place we want to go. Like in the case of Microsoft, they still have all those wacky other email domains, but they've said now we want to be over at Outlook.com rather than live.microsoft.com or whatever. And in fact, when you're logging in, Microsoft is still taking you back over to their older authentication domain at live.microsoft or whatever it is that they were using.

So that is one thing that anyone can do. There's nothing to prevent a website which changes its presentation domain, its main domain, from still issuing the SQRL QR codes from its old domain, which is where your identity is anchored. So that still works. That is to say, that can be done. So if they wanted to, they could leave SQRL where it is and just leave you authenticating against the domain that they still control, even though it's not where the website is now.

But if they knew over time they wanted to migrate people, that's possible, too. When you go to their site to log in, they would give you a SQRL code from their new domain. And if it did not know you, it could then take you to a page saying, oh, you may have noticed we moved. Please use this SQRL code to log in. So what would happen is you would be known under your old code, but it would have just identified you during your first failed attempt to authenticate with your new code. And so the act of using both would allow them to transparently transfer you. You would then be known as who you are under the new code. So migration, while it's not completely seamless, it can be done.

And so they might maintain the old domain for another year to move people. Anyone who logged in with SQRL during that time would automatically get moved over to authenticating under the new domain, and then they could just retire the old one. So not painless; but it is, you know, there's no way to soften that binding to the domain, I mean, that's where the security comes from. So naturally, if you have to change the domain, that does, as our astute listeners have noted, it changes your identity. So there is a way. You could either continue using the old one, or use a sort of a migration solution over to the new one.

Leo: Brian, Mechanicsburg, PA brings up the issue of Microsoft's WiFi Sense. You're going to have to explain this one to me because I think this must be from while I was gone: Being safe from WiFi Sense leakage isn't just an issue of me being sure to never turn it on, or remembering to turn it off. I had read that it was defaulted on. Say I never enable this on my machine, but I manually give some of my friends the password to my guest network. What's to stop them from having their WiFi Sense enabled and sharing my password with Microsoft, outside of my control?

Steve: Okay. So you and Paul have probably talked about this. This is - I can't believe Microsoft has done this. This is, we have confirmed now that it is enabled by default in Windows 10. This is something that was in 8.1, that Microsoft has moved into Windows

10, where they're using your social networking connections to share your WiFi password with your Facebook and Twitter and Outlook and other social networking connections so that, if someone you know on Facebook, a Facebook friend, comes to your home with their laptop, it recognizes and logs into your WiFi automatically. And I just - I'm stunned that Microsoft thinks this is a good idea.

So what Brian is worried about is he says, okay, if he turns it off on Windows 10 so that he is not sharing his WiFi password, essentially, with anyone in his social networking groups, but somebody comes over to his house who has it turned on, if he gives them his WiFi password, they will share it with everyone they know. And that is true. So this is, I don't know, this is crazy. Maybe tomorrow when you're talking to Paul you can bring it up and make sure that I've read this correctly. But this seems to be the way this works. And everybody who is security conscious is just, like, shaking their head, saying this is taking ease of use way too far. There ought to be, like, some process where you have to - someone comes over, and somehow your machines are able to say, oh, do you want to have a one-time access to my WiFi network?

Anyway, my take on all this, basically what we're seeing in general with the Internet of Things, with Philips Hue lights and door locks and doorbells and the whole thing happening, you really have to have separate networks. You have to have a wireless network that is just low security. It's the guest network. And you want to run with a firewall between it and your own network. Now, Leo, I heard you talking on your podcasts about making the move to wire your home for Ethernet because WiFi is just not working for you.

Leo: Yeah. It's more for performance than security, but...

Steve: Yes. And I've done the same thing. I've got TiVos; and yes, they all have WiFi. But mine are all wired. My main TiVo and my minis are wired because you just get better operation. But at the same time I also have iOS devices floating around, a phone and iPads.

Leo: You still need WiFi, no matter what. I mean, there's a lot of stuff that can't connect.

Steve: Right. So the idea is for things that are not moving, if you can, I really think it makes sense to wire them. For things that are inherently mobile, then use WiFi. But this Internet modem that I purchased, it's the Motorola 83, whatever it is, I don't know, the fast DOCSIS 3 modem, it does have a provision for multiple wireless networks and to firewall the guest network. And I have verified that that network has no visibility into my wired network and my secure wireless network. And one way or another, that's what you want to do. I really think that's the way people who listen to this podcast, that's the solution you need so that, yes, give your visiting friend the password to your "I don't care" wireless network and keep your, if you have a non-guest WiFi, keep that one to yourself. It's crazy that Microsoft is just blasting this thing all over the place, but that seems to be what they've chosen to do.

Leo: I might disagree a little with you on this one, after looking at their FAQ.

Steve: Okay.

Leo: So the number one purpose of this is to make it easier for you to join open networks like your Starbucks. You know, usually you join the network, and then there's a popup screen, you have to fill in stuff, and they're crowdsourcing those so that you don't have to go through that process, which I think a lot of people would support. It also helps because there's some devices that you can't do that with. But the second thing they're doing, as you said, and it's fairly easy to turn this off on a network by network basis, at home or whatever, is to let your friends join your network. Now, if your friend comes to your house and asks to join your network, and you say fine, and you take the phone from him, you log in, you give it back, he still has that login forever.

Steve: True.

Leo: And so I think the theory is that this gives you actually better control because, A, there's no visible exchange of passwords; and, B, you have the control. You can go to a switch and say, yeah, I don't want to do that anymore.

Steve: Okay.

Leo: I agree with you. If you have a guest network, it's better to use a guest network, if it's properly implemented. And I do. Apples have guest networks. Yours does. Most do, I think, now. At least most not $25 routers do. So I think that their heart's in the right place. I'd have to look more closely. I mean, here's one thing that is a little weird, which says, "To stop sharing access to a WiFi network that you're currently sharing, you go into your WiFi Sense settings and turn off 'Share WiFi networks I select.'" And this is the part that's a little weird: "It can take a few days for the networks to which you've shared access to stop being shared."

Steve: It's like you've unsubscribed from this email spam, but it's going to take a few days for us to actually stop sending you spam. It's like, what?

Leo: And I gather from the correspondent and others that what they don't like about this is that Microsoft presumably is storing that network password.

Steve: Right. It's in the cloud.

Leo: But I have to tell you, that happens all the time. If you're using an Android device, and you turn on "Back up my settings," it sends, in the clear, your WiFi password and every WiFi network you've ever joined's password to Google. So I think that this kind of thing is going on.

Steve: Yeah. And we've talked about how iOS is sharing WiFi passwords among devices.

Leo: Yeah. That's right.

Steve: Which is a convenience.

Leo: Yeah, that's right. So, I mean...

Steve: I guess the difference is it's identifying people in your social networks and sharing with them without explicit per-instance approval.

Leo: Right.

Steve: Yeah.

Leo: Right. But you can turn that off. You can say, no, I don't want that.

Steve: Right, yeah.

Leo: I think it's more for a convenience. And remember, to use your WiFi, people have to be in your area.

Steve: Right.

Leo: Usually, the theory being, in your house. I'm not convinced this is - I'll ask Paul, absolutely, what he thinks of this.

Steve: Yeah, see what he says.

Leo: This is news. I hadn't heard about this. Our last question, Jeff Lopez, Heber, California. He wants some help with - dogs. Hi, Steve. Recently when I take my dog for her morning walk, we are encountering two large dogs. They've learned to get out of their yard. Now, most of the neighborhood dogs are quite friendly, but these two charge us, growling and barking. So far, they run away when I say, "No!" But I don't know if they'll get bolder over time. Aren't you supposed to, like, "No," put your hand out like that? I don't have the presence of mind to do that. I usually go, "Yikes," and I turn the other way. Anyway, he says...

Steve: Well, yeah, you don't know that they're going to stop or obey your command.

Leo: Right, exactly. That seems brave, to do that. No, wait a minute, it's bears

you're supposed to do that with. Sorry, not dogs.

Steve: I think bears you're supposed to look really big. You, like, try to, like...

Leo: Go, "No!"

Steve: ...seem larger.

Leo: Yeah, act like Thor.

Steve: Either that, or just be faster than your friend.

Leo: Old joke, but still always laugh worthy. I had hoped that your sonic dog trainer would be available, either to build or purchase. So what's the state of that Portable Sound Blaster?

Steve: So I did want to give people an update because I get a constant trickle of people. Dogs are a continuing problem. So Jeff's application is what it is useful for. And it works. That is...

Leo: Who's Jeff's application?

Steve: The questioner, Jeff Lopez.

Leo: Oh. Oh, his use of it, yeah, yeah, yeah, yeah. That's what it's for. Protection, yes.

Steve: Right. Well, exactly. Unfortunately, what happened was I told the now classic story of the Portable Dog Killer and how I used it.

Leo: It's a Christmas story. Some people want "You'll shoot your eye out." But we here at TWiT, we like to hear the yearly "Portable Dog Killer." It's a holiday favorite.

Steve: It's a holiday tradition on the Security Now! podcast. And what happened was, I used it just like that, pointblank range, to startle an aggressive dog, to train it to stop at that behavior. But then I also took it to school; and, as we learn in the story, it was able to alter the flight path of seagulls that were flying at a great distance overhead. Well, those two things sort of got conflated in many listeners' minds, where they thought that it could stop dogs from barking at a great distance. And it doesn't. We verified that. But what happened was...

Leo: In fact, it may make them bark louder and more furiously.

Steve: It could. It could incent them to bark, yes. So what happened was, before I began work on SpinRite 6.1, I did update the design. I experimented with a Google group. So if you Google "Portable Sound Blaster," that's what we called it, Portable Sound Blaster, you go to that Google forum, and I left it after I was done. Many people built them.

It is a really cool design. It's about four components. It's a pushbutton switch for the power, an inductor, an ultrasonic transducer, and like one other thing. I don't remember the design now. But it's very elegant, and it is unbelievably loud. And so it is perfect for a personal, sort of where you would spray mace, instead you can spray this sound. Think of it that way. So it's close proximity, but it will absolutely bring an attacking dog to a standstill. So Portable Sound Blaster. If you're a builder, this would be a neat project for you to build with your kids, or build it yourself. There are none for purchase. But many people built them successfully and use them as a personal blaster deterrent, and it works.

Leo: So I'm not clear. Are the plans here, or are they a work in progress?

Steve: It ended up being I just dropped it in order to switch to SpinRite 6.1.

Leo: Had better things to do.

Steve: But there is a link to "latest plans," I think, up there in the first paragraph, like "latest design."

Leo: It's a ZIP file, okay.

Steve: There's a ZIP, and then there's a schematic, and a lot of people in the group built them and successfully used them.

Leo: Nice. It's inaudible to humans.

Steve: Well, it was funny because some of the older guys that were building them weren't sure that they were working until their teenage daughters were, like, calling from upstairs, saying, "Dad, whatever you're doing, stop that, it's hurting my head." So young people can hear them, and dogs can hear them. And in fact one of the designs is a button to lower the frequency, just so that, if you can't hear it, you can make sure that it's actually working.

Leo: Right, right.

Steve: But, boy, dogs can definitely hear it.

Leo: And, well, we'll go through all the disclaimers. It doesn't hurt the dog. It's temporary, and it just really scares them. It's like shouting "No."

Steve: Right, it's just, yes, it's like dogs don't like fireworks on the Fourth of July, which we just went through. Similarly, they don't like this. And so it just stops...

Leo: You don't tie them down. You want them to go away, and they do.

Steve: And they do.

Leo: They go, whatever this is, it's annoying. I'm leaving.

Steve: Yeah, it terrifies them briefly, and that's all you want is, like, for them to turn around.

Leo: You know, you need two buttons. You need one for dogs and one for teenagers. You have, like, two settings; right? Yeah. I'm just thinking, little improvements.

Steve: That's right. Tune the design.

Leo: Ah, what fun it is to be back. I love doing this show, and I know you love listening, and we're glad that Steve just gives us his time as he has for 517 episodes. That means we're closing in on our 11th year; right?

Steve: We are closing in on the end of Year 10, yup.

Leo: Wow.

Steve: And starting, I think it's August, actually, is when we're going to hit that.

Leo: Amazing. That's because he never misses an episode. So it'll be like 521. You missed one episode or something. And that was my fault.

Steve: I think we did.

Leo: You'll find Steve at GRC.com. That's a good place to go to find the best hard

drive maintenance and recovery utility in the world, really the last one, the one.

Steve: It is. The surviving.

Leo: Well, because it works.

Steve: Yup.

Leo: Need no other. It's called SpinRite.

Steve: And SSDs. Who would have thunk that it would have ended up being as useful for solid state, because they use the same tricks. They use error correction, and they push it further than they should.

Leo: Yeah. You'll also find 16Kb audio of the show for the bandwidth-impaired; really nice transcripts, thanks, Elaine Farris; and full bandwidth audio versions there, too. GRC.com. That's where to leave questions for future episodes - we do this every other episode - at GRC.com/feedback. Or you can tweet him @Sggrc. As you see, we answered a couple of tweets.

Let's see, what else? Oh, we have full-quality bandwidth audio and video of the show, if you want to see Steve's smiling face, at TWiT.tv/sn, or you can get it wherever you get your podcasts because as a show that's been around for 10 years, it's on a lot of lists. You'll find it anywhere you look. Steve will be back here next Tuesday, 1:30 p.m. Pacific, 4:30 Eastern, 20:30 UTC, for another great edition of Security Now!.

Steve: Leo, always a pleasure. Glad to have you back, and I'm glad you had a good vacation.

Leo: Thanks, Steve. We'll see you next time.

Steve: Thank you.