Listener Feedback #96

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They 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-257.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-257-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 257, recorded July 14, 2010: Your questions, Steve's answers, #96.

It's time for Security Now!, the show that covers all your security needs, your privacy issues, all the things that are keeping you safe online. And who's better to do that than Mr. Safety First from GRC.com, the creator of SpinRite, the world's finest hard drive maintenance utility, and of course all those great free security utilities like ShieldsUP!, Shoot The Messenger, DCOMbobulator: Steve Gibson. Hi, Steve.

Steve Gibson: Hey, Leo. It's great to be with you again, as always.

Leo: Welcome.

Steve: We're creeping up on the end of year five, Episode 257, so we've got three to go.

Leo: Holy moley. Hex 101. Now, thanks to last week, see that? See that little doohickey right here? That is my LastPass USB key. It's on my keychain. And that is my second factor authentication.

Steve: Yay. Very cool.

Leo: Thanks to you, I did it. And I'm really happy with it. It means that I have to

stick this into any computer - and by the way, I have three partitions: one for Linux, one for Windows, and one for Mac. And I run that Sesame program. So I've been - I have to say, as long as I've used LastPass, and I've been using it for a long time, you taught me a lot last week.

Steve: Actually, that has been pretty uniformly the feedback that I received back from Twitter followers. What I kept seeing was, wow, I've been using LastPass for, like, a long time, and I didn't know half of the things that it could do, so...

Leo: Yeah. I've started kind of implementing more, and also using the password generator, trusting it more.

Steve: Yes. Well, we've got - I'm going to do, this week, we pretty much - I would characterize this Q&A as an unapologetic LastPass Q&A.

Leo: Okay.

Steve: The very first question is one that I've been trying to do for the last two Q&As, but I always put it at the end because it was kind of a fluffy one. But we kept running out of time and so never got to it. So I thought, okay, finally this time I'm putting it number one so we get to it first.

Leo: Good. Well, we're starting a little more on time this time, too. Maybe we'll have time.

Steve: Well, and we haven't had technical difficulties so far, either, so that's been good.

Leo: So far, so good.

Steve: So everything's working. Let's knock on something. So anyway, but we've got such well-informed and smart listeners, and the reaction from last week's LastPass episode has been so overwhelming, that there were just a ton of really good follow-up questions - things that I actually had notes about but didn't cover, some additional things, some very good points that were raised, some people questioning stuff. So we have, I think, even for people who heard last week's LastPass episode but weren't moved, what we've got is still fundamental good security practice questions.

Leo: Good, good.

Steve: So even though they're relative to LastPass, I think everyone will find them really interesting. And we've got, of course, news and updates and so forth.

Leo: As always, there's a ton of stuff to talk about. Well, I'll tell you what, I have one commercial. We'll do it before we get to the questions. Let's start with the updates. And I know you like to start with patches.

Steve: Yes. Well, we have, as it happens, just passed the second Tuesday of July. And everybody knows what that means. That was Microsoft's opportunity to fix things. The good news is they fixed four serious critical remote code execution vulnerabilities. The most significant one is the one that we've talked about now several times, the Help Center vulnerability, which was being actively exploited in the wild. That was the one where a couple weeks ago, I blogged about it actually, it was the HCP protocol. HCP:// was the way that Windows could access this Help Center, sort of with its own sort of pseudo URL. And Microsoft's little Fix it button, or changing the registry, could disable that functionality to protect people in the meantime. Well, they finally, with the second Tuesday of July, have that fixed. So that's behind us now.

Also we talked quite a while ago about a problem that had been lurking in the video drivers for Windows Vista and Windows 7 with the Aero interface. And Microsoft's only workaround was, well, disable Aero until we get it patched. That will definitely require a restart for people because this is the video driver that you can't change on the fly. So that's been fixed also. And then there was an Office ActiveX vulnerability that was remote code execution that had been privately reported to Microsoft, not being exploited in the wild yet; and an Outlook vulnerability, both that allowed code to be executed, remote code to be executed locally on your system. All of that's fixed.

So your standard, let's update Windows, and definitely reboot. Microsoft says definitely, if you're running Vista or Windows 7. Maybe, if you're not. And I've got these updates pending myself because for me, rebooting my system is a workout. So I will be doing that probably when I'm through the podcast. I didn't want anything - I didn't want to risk anything not coming back up in time.

Chrome continues to move forward. Last week we talked about it moving to 375.86. We're now at 375.99. So just there were four other memory corruption-related bugs. Again, Google's not telling us very much about it. We know that it involves scalable vector graphics, that is, the SVG format, and the portable network graphics, PNG format, and also CSS style sheets. So they've fixed that and, as you commented last week, probably silently updated people. I did fire up Chrome and verify that, yup, it was now at 375.99. So that's been fixed.

Leo: I like that, that I never have to think about it. It just does it.

Steve: Yeah, that it just does it for you. In security news, I wanted to note that there's a new DNS service that has popped up from some friends of ours. Alex Eckelberry and Sunbelt Software have something called ClearCloud DNS which is specifically designed to protect people. We've talked, for example, about OpenDNS in the past where they can protect your computer if you use their DNS service because the first thing the computer has to do is look up domain names. That is, unless the bad guys use IP addresses, which they could certainly use. But typically they're spoofed domain names like, you know, PayPol.com instead of PayPal. You won't notice that it's an "o" instead of an "a." And then they'll take you somewhere.

Well, what Sunbelt Software is doing is being proactive about not listing the DNS

addresses of known bad sites. So malware that assumes you're just using regular DNS may use a trick like PayPol.com to try to get you to go to a bad site. It won't be listed, for example, it's just not available if you use ClearCloud DNS. For those interested, the IP address of their DNS server, and they only give us one at this point, is 74.118.212.1.

Leo: Of course it is.

Steve: Or just go ClearCloudDNS.com, all one word, ClearCloudDNS.com, which will take you to the site that Sunbelt has set up. And I also noted in the news...

Leo: So what do you think? I mean, is this a worthwhile thing, if I'm using OpenDNS, to replace OpenDNS? I mean...

Steve: I don't think - I added it to my benchmark the other day...

Leo: Oh, good.

Steve: ...just to see how speedy it was. And it wasn't really very fast at this point, that is, compared...

Leo: Well, now it's going to really be slow because you just told a million people about it.

Steve: ...compared to the things that I've been using.

Leo: Right.

Steve: The benchmark now knows about it, so it'll list it there. I think they're just starting up. They talked about, in fact, some of the pages on their site still just has, like, gibberish text paragraphs where someone dropped...

Leo: Laura missed some stuff, wow.

Steve: ...literally dropped in some boilerplate just to sort of, you know, they're still working on their site. So this may be a bit of a preannounce of where they are. So I wouldn't give - and I would imagine they'll have maybe a second IP address because, you know, DNS servers like to have two so that you've got some redundancy and backup. So, but that's on its way, and we'll keep an eye on them. And Sunbelt just got acquired by, I guess, a large company - I think it's GRI, someone I have never...

Leo: Oh, interesting.

Steve: ...hasn't been on my radar before - because of their Vipre, V-i-p-r-e, technology apparently was what the acquiring company wanted from them.

Leo: Vipre's pretty cool.

Steve: I don't, yeah, I don't know what that means exactly. But hopefully Sunbelt will stay pretty much as it is because they're doing a great job.

Leo: Well, when you buy a company for something that they do, you probably aren't going to change it a lot unless they wanted to make their own antivirus. I don't know, that's interesting.

Steve: I don't know.

Leo: Yeah.

Steve: And Facebook is now in trouble with Germany. The German government has very strict privacy, or Germany has very strict privacy laws. And the German government likes to enforce it. What I saw, I saw the clearest sort of summary in the SANS security newsletter. They said that Facebook routinely asks people who are already members of Facebook to upload their contact lists from their mobile phones and email accounts so that Facebook can invite those people to join. Facebook retains the contact information, whether or not the people choose to join.

Leo: [Buzzer sound]

Steve: Uh-huh. Even though the people have not given Facebook permission to store that information. Hamburg Data Protection Authority head Johannes Caspar has received several complaints from individuals whose information has since been shared with third parties.

Leo: Oh, dear. Oh, dear.

Steve: So, not good. So apparently the German government is suing Facebook.

Leo: Hah.

Steve: I mean, is putting together a lawsuit and going to say this is not okay for you to do over here.

Leo: I've got to talk about this with Jeff Jarvis, who speaks German, is also very

interested in German privacy issues. And of course Germany is the country that's been going after Google, as well. And they are very privacy sensitive. But this sounds like a clear case of kind of violating good practice.

Steve: Yeah, not good. And then - and this one I just, I think to myself, what are they thinking? I gave myself the little tagline, "We're all comrades here, no?" Because the news is that Microsoft has decided to share their source code with the Russian intelligence agency.

Leo: Oh, that's positive.

Steve: Extending their 2002 agreement...

Leo: What could possibly go wrong?

Steve: I know. This really makes FreeBSD look a lot better to me.

Leo: Geez.

Steve: Or Linux. Extending their existing 2002 agreement which covered Windows 2K, 2K Server, and XP, Microsoft has just given the Russian Federal Security Service, the initials are FSB, the source code for Windows 7, Server 2008, Office 2010, and Microsoft SQL Server.

Leo: They must have had to do that. That must have been part of the deal to be able to sell in Russia; right?

Steve: Well, they say, quote, "with hopes of improving sales to the Russian state."

Leo: Yeah, yeah. That makes sense.

Steve: And then according to the Russian publication Vedomosti, quote, "The agreement will" - now, this does, okay, here, listen to this. "The agreement will allow state bodies to study the source code and develop cryptography for the Microsoft products through the Science-Technical Centre 'Atlas,' a government body controlled by the Ministry of Communications and Press." I don't know. I did note that Vista was not on the list. I guess even Russia doesn't want Vista source code.

Leo: You do not need to tell us how Vista works. We already know, and we don't want it. But thanks anyway, comrade. Give me Windows 7, I'll take that.

Steve: Oh, goodness.

Leo: Wow, wow. That's pretty funny. No, we don't need Vista.

Steve: We'll just skip over that one.

Leo: Just put it on the list, please, because it's embarrassing not to have it on the list, at least. We won't look at it. Oh, my god. That's very funny. So what does this mean? It doesn't mean that they're going to release a patched version of Windows with a backdoor for the Russian security.

Steve: Well, the security community has responded in all kinds of ways. Generally negatively, feeling that, I mean, one UK security researcher was quoted as commenting that Windows has tens of thousands of bugs. And he feels uncomfortable with the idea that a government would have the source code for operating proprietary software because they could use it to find problems which would allow them to leverage what they know against other governments.

Leo: Oh, interesting. Right, okay.

Steve: I mean, like, find errors. And then, you know, other people say yes, but you don't need the source code to find errors. You can use fuzzing software, throwing arguments at functions, and find problems that way, too. I would argue that the source code does make it easier because, if you were to throw fuzzing arguments at the API, and something bad happened, you could then much more easily track it down having the software source code, rather than having to, like, reverse engineer exactly, out of the binary, exactly what it was that happened. So I - and this, the idea that it's going to allow, from this quote, "The agreement will allow state bodies to study the source code and develop cryptography for the Microsoft products." What does that mean? Windows already has - it already has cryptography.

Leo: Yes, but we want Russian government cryptography, special kind, just for you. You will like our cryptography.

Steve: Oh, goodness, I just - I don't know how this is going to end well.

Leo: Vista, it wasn't my idea. That's really, yeah, I mean, look, what the Chinese government did is just mandate we're going to have our own Linux distribution. We call it Red Linux. And Linux is already open source. So I think Microsoft's attitude, quite reasonably, is, well, it's us or Linux. They're going to get the source code and do whatever they want, so - but you'd think that also the Microsoft folks would protect this stuff with, like, the crown jewels. The source code to Windows is hugely valuable. They must...

Steve: I don't know.

Leo: That's what I would be more concerned about from Microsoft's point of view.

Steve: I would, too. I mean, how can they imagine it's not going to get out, that some - how could they imagine that some purpose that they didn't intend will not be met, having released the source code? I mean, sure, lots of good people will probably be looking at it, and maybe some good can come from it. The idea that, well, and the other thing, too, is that they're very open with the fact that they're doing it to improve sales. So this is - they see it as a commercial incentive to give the Russian intelligence services Windows source code. I mean, I'm going to keep using Windows. But it does seem worrisome.

Leo: Yeah. Yeah.

Steve: From our podcast last week, LastPass is acquiring a new feature. Because all the LastPass guys were listening to the podcast. And my comment about how the additional authentication employed by the grid, which is an optional additional factor in multifactor authentication, how it was useful, but it was a little troubling to me that no one was - that the grid could be learned over time. I mean, farfetched, but possible. And they said, that's a good point. We're going to add a feature to send a person a reminder email when their grid has been used to a certain level, telling them that they ought to exchange it for a new one. So LastPass got a new feature as a consequence of the podcast.

Leo: Wow. You're a powerful man.

Steve: And speaking of which, Stina Ehrensvrd, our favorite founder of Yubico, has announced, also as a consequence of the podcast and the fact that we were mentioning the YubiKey, which does now interface very nicely with LastPass, a 30 percent discount for between one and five YubiKeys for any Security Now! listeners from now until the end of August.

Leo: What? Say that again?

Steve: So 30 percent off the purchase of from one to five standard black or white YubiKeys.

Leo: That's great. How much are they?

Steve: Good question. I didn't look. So we go to store.yubico.com...

Leo: Okay, I'm doing it right now.

Steve: ... store.yubico.com and simply enter "securitynow" - all as one word - in the coupon code field during checkout. And our listeners who do that, until August 31 or probably through August 31, will receive a 30 percent discount on between one and five

YubiKeys.

Leo: So that's like eight bucks. They're $25 each. That's a good deal.

Steve: Yeah.

Leo: That's a great deal.

Steve: So thank you, Stina. And anybody who would like the idea of the multifactor authentication with the YubiKey, it's more affordable for the next month and a half.

Leo: And if you're buying a hundred of them, that's $500 off.

Steve: No. Between one and five.

Leo: Oh, one and five, okay.

Steve: Up to five.

Leo: Up to five.

Steve: White or black YubiKeys. And since we last spoke, Leo, Windows XP SP2, the famous major security update to XP, which turned the firewall on by default, which removed raw socket support from XP and was a major improvement in security, support has been officially discontinued.

Leo: Awww.

Steve: Now, that's not a problem because we have SP3 now. And so everyone should have long since moved to that. Come to think of it, I wonder if I did.

Leo: Whoops.

Steve: Because remember my - SP3 was a problem for people.

Leo: Right, right, right, right. It was hard to install. In fact, SP2 was a major problem. And that I got - I did more radio shows on SP2 issues than I've ever done.

Steve: Oh, yeah. Well, because it was an aggressive change. Microsoft doesn't want to

do aggressive change. Microsoft doesn't do aggressive change well. Which is why Vista was a big thud, and then they worked on fixing it. And Windows 7 made basically just a few little UI tweaks, basically the same code. It's not another big change.

Leo: Right.

Steve: But what I did find interesting, also in the news, while we're talking about Windows XP SP2, is that Microsoft has sort of stated - confessed, acknowledged - that 74 percent, that is, three quarters of workplace PCs are happily still running Windows XP. And they're doing so...

Leo: Oh, that's not good.

Steve: ...on 4.4-year-old hardware, with no plans to upgrade.

Leo: Yeah. So I hope they continue to offer security updates for this.

Steve: Well, SP2, no. But SP3, yes. So that's - I'm sure that the bulk, if not all, of those three quarters of workplace PCs will be using SP3, and Microsoft will be extending support. I think what's going to happen is Microsoft is going to be forced, just by virtue of the population of Windows XP, not to discontinue it as soon as they would like. I mean, sure, they would like to get - and you can understand that it's a pain to have to support down versions of operating systems, especially when they're so different, XP versus Windows 7 and to a lesser degree Vista.

So I don't think Microsoft's going to have a choice. I think they're going to have to continue XP support longer than they intend to because people are just not going to let go of it. I mean, sorry, Windows XP support. Because I think that, I mean, XP is a great operating system. It's where I am, finally. I moved from 2000 to XP. I have no plans to go forward. I'm happy right here. It works.

Leo: Well, I mean, I guess if we could pick and choose, I'd say, and you'd probably agree, stay with Windows 2000. But Microsoft doesn't work that way. Right? Eventually they're going to move us on.

Steve: Right, right. Well, they're going to do everything they can. But if, see, the problem is, companies right now have installed hardware that will not run Windows 7 well. So they're staying on Vista because Vista - I'm sorry, I keep saying that. They're staying on XP because XP has substantially lesser demands on the hardware than does Windows 7. So the problem is, it's very expensive, not only for Windows 7 licenses, but to upgrade almost five-year-old hardware so that it can run Windows 7 well. Companies have certainly - they, like, got a copy of Windows 7, ran it on their standard installed hardware, and it's just kind of like, ugh. It's like, well, why, what do we need from Windows 7?

Leo: Ugh.

Steve: Ugh.

Leo: Well, I think we need security patches. It's really concerning, I mean, I'd like to know what the number of Windows, unpatched Windows 98 machines are running out there, sitting in closets, in the back of offices, doing mission-critical networking stuff.

Steve: Yeah. I did have a neat and sort of fun SpinRite story to share. The subject line caught my eye because it was, "Damn you, SpinRite." I thought, okay.

Leo: Ooh, that's harsh.

Steve: From Eric Gerlach, who says, "Hi, Steve. I picked up a copy of SpinRite a while ago, when I first started listening to Security Now!. It's come in handy a few times since then. But never has it frustrated me as much as it did a few months ago. One of the computers at work, a point-of-sale terminal, got the dreaded unmountable boot volume error. Given that it was needlessly" - I'm sorry. "Given that it was needed desperately that night, I got out SpinRite and did a run. A few hours later the drive was running like new again, and the night went without a hitch. I still had my suspicions about the drive, though. And as the computer was still under warranty, I decided to call Dell to get a replacement. When I called them the next day, SpinRite had worked too well. I could not convince the Dell representative that the drive had failed in the first place."

Leo: Damn you, SpinRite.

Steve: He said, "After many months more of waiting, two days ago the drive failed again, once more right before a busy night. But this time we called Dell first and got the new drive sent. Then we ran SpinRite on the drive to fix it. Curse you, Steve, for making a product that works too well. Cheers, Eric."

Leo: Speaking for Russian government, we would love to get source code of SpinRite, as well.

Steve: Yeah.

Leo: Would you mind sending it to us? We would like to add encryption, special Soviet style.

Steve: Special Russian encryption.

Leo: Russian encryption.

Steve: But he said, "P.S.: I know that using my personal copy of SpinRite for work was bad form. But I've got a site license in my budget for next fiscal." So thank you very much, Eric.

Leo: Good, good, good. That's a nice story. And the moral of it is, run SpinRite before you call tech support.

Steve: After.

Leo: I mean, after you call tech support. Call them first.

Steve: After you've shown them and you've convinced them it's not working, they'll say, okay, we'll send you out a new drive.

Leo: And if you work in tech support, the moral would be, get SpinRite.

Steve: Yeah.

Leo: Steve Gibson, I have questions. Do you have answers?

Steve: I bet I do.

Leo: Since you picked the questions.

Steve: Since I chose the questions, yes.

Leo: I would guess you're not going to put anything in here - well, yeah, you know, sometimes I take questions on the tech - of course I don't go through the questions ahead of time. But I'll take questions on The Tech Guy, and I'm proud to say I don't know. I mean, because if you don't know, you should never say; right? But I don't have the luxury you do of having a brain the size of a city.

Steve: Well, you also have the chatroom, and that helps a lot.

Leo: The chatroom is my brain, and they are the size of a city. A small city, but...

Steve: But the fact is there are so many obscure little corners, that someone could say,

well, what about - someone was - I saw something about how do I get a copy of some random audio player that runs under Mac 10.6.2 or some - it's like, what? Okay, that's - okay, I'm not answering that question.

Leo: No.

Steve: No.

Leo: And if I had that luxury, I, too, would say no way. Dan Ducasse in Atascadero, California, a former San Mateoian - as are you, I think.

Steve: Yes.

Leo: He is "Aragon Don" and a Troop 12 Member. Is that meaningful to you?

Steve: You'll see why in a minute.

Leo: All right. Dear Steve, I have been listening to you and Leo on the Security Now! podcast for several years. I really enjoy the shows. The "How Computers Work" series has been informative, and in hindsight I wish I had taken electronics in high school. As a former Aragon Don - oh, is that the high school...

Steve: Yup, that's where the portable dog killer episode occurred.

Leo: ...and a few years younger than you, I would have probably been one of the first students to take your classes in digital electronics. Isn't that cool. After listening to "The Portable Dog Killer" episode - that's 248. If you haven't heard it, go back, listen, please. We'll wait. Go ahead. I wanted to write because you also mentioned the "Shock Machine." You were in Troop 12, Boy Scout Troop 12 with my brothers, Paul and Marc, and had come over to our house - oh, this guy has memories of you as a kid.

Steve: Exactly.

Leo: ...come over to our house for some reason and brought with you a cigar box - oh, dear - with two brass door knobs mounted on the lid. This can't end well. Back then you were known for your inventions, and you and my brothers approached me to test out your latest gadget, "The Smile Machine." Steve, this is good. We're getting some insight.

Steve: [Sighing]

Leo: Deep insight. It looked harmless enough - a couple of door knobs, a switch on the outside; a little battery, some wires, some other junk on the inside. What could possibly go wrong? You or my brothers instructed me to, "Just hold the door knobs; and, when the switch is pushed, it will make you smile." Sure enough, when the button was pushed I was grinning from ear to ear. I was also locked onto the door knobs until the power was turned off. It was a great gag. What the heck? Oh, I've got to find out about this.

Listening to the story of the sonic gun, the memories started coming back. I remember my brothers coming home from school telling stories of seagulls falling out of the sky and the incident with Vice Principal Archibald. You were educating and entertaining us back then, and you still are educating and entertaining us today. That's so great. Thanks for the memories; thanks for all of your current work. Dan Ducasse. Wow. Do you remember the Ducasse brothers?

Steve: Oh, absolutely do. I think it was Marc who was one of the funniest kids I have ever known in my life. I mean, just, you know how like sometimes you run across an incredibly funny kid in high school who's just - I don't know. He just had an amazing - his timing was perfect. I mean, he was like a born comedian. And I very much remember them. And it's funny, I'd forgotten Troop 12, but that's the troop that I was a member of. And those guys were both in my high school and the same Boy Scout troop.

Leo: That's neat.

Steve: So anyway, I just got a kick out of that. I wanted to toss that in, and it was the last...

Leo: Do you want to say how that worked, the smile machine?

Steve: I was fascinated with shock machines. And my sister was my guinea pig for most of them. I'd say...

Leo: Oh, your poor sister.

Steve: ... "Here, Nancy, hold these...."

Leo: She still likes you; right?

Steve: Oh, yeah. "Hold these two nails in each hand, and tell me if this one is better than the last one." So...

Leo: Oh, boy.

Steve: She's - very minor damage was done.

Leo: So was it like a taser kind of? I mean...

Steve: It was - I was conscious of - I mean, now, with the benefit of, you know, 55 years of wisdom, I wouldn't be running current from one arm to the other across everyone's heart muscle. That seems unwise. Although it was very high frequency, and that would tend not to interfere with anyone's cardiac rhythm. So it's like Tesla coils don't hurt you because they're such very high frequency. And so I was just experimenting with stepping up the voltage of small batteries using various oscillators and things. And it was fun.

Leo: Wow. Impressive.

Steve: So apparently I took one of those to school, also, and we were all holding - I had several - I don't think maybe - I don't think a hundred, but more than several sets of ten. So maybe 20 or 30 people all in a huge circuit holding hands, feeling this...

Leo: All frozen. All frozen solid.

Steve: Yeah, the thing had been one of my early escapades, so...

Leo: That's the spirit of inquiry, I think.

Steve: It was fun. No one ever died, so that's good.

Leo: Yeah, that's good. I'll agree with you on that one.

Steve: Okay.

Leo: Question 2, Mary, the "skeptical packet goddess" in Sparks, Nevada still wonders about trusting LastPass. She writes: I listened with great interest to episode 100000000...

Steve: Eight zeroes.

Leo: ...about LastPass. I've been thinking of switching from Roboform to LastPass, but never had 100 percent trust in their model. It's very similar to LastPass. One thing I was hoping to hear from your review was how it's possible to know whether or not their JavaScript-based encryption algorithm has been properly validated. Could it be possible they could end up in a WEP situation? In other words, something

that looks right, but isn't.

Also, is it possible to know whether they might be performing two separate encryptions of user data? They might encrypt once with a key based on the user's master password, and separately a second time with their own closely guarded master password which only the developers at LastPass know. Then after a short time of collecting millions of users' sensitive data, they could be doing all sorts of havoc unbeknownst to the trusting users. I'm sure it would be nice if they had some kind of independent code review.

I'm also concerned that they send the users' encrypted data over HTTPS to their servers. If their local encryption is done well, then, well, that should be okay for them to send the already encrypted data in the clear so a user could examine the outgoing data packets to make sure the data local encryption was actually performed. How is it possible to confirm the TNO model - the Trust No One model - if we are left to trust that they are performing the local encryption properly? These questions seem to have been left unanswered by your review of LastPass. Good on you, Mary. That's great.

Steve: Yes, very good. And the answer is all good news.

Leo: Okay.

Steve: There is a page which Mary and anyone who is similarly curious can check out, which my contact at LastPass assembled more than a year ago, or quite some while ago. I read in detail a forum dialogue where somebody was similarly both technically proficient and skeptical and wanted to trust LastPass, but needed LastPass to prove to him beyond any doubt exactly what it was they were doing.

So the page is https://lastpass.com/js/enc.php. So it's, again, you need to be over SSL. So https://lastpass.com. Then it's slash, and then "js" as in JavaScript, slash "enc" as in encode, dot php. That will take you to a beautiful little standalone page which does no communicating with the Internet, which has code that anyone who is curious can examine. It loads a couple JavaScript libraries. I checked it out myself extensively. You can put in your username, which for LastPass is the email address, and your password. Punch the button, and it will then generate and show you, using exactly the algorithms I talked about last week, the 256-bit key used for logging in, and the separate 256-bit key used for driving the AES encryption. Then you can put data into either of the encrypted or decryption fields and cause that key to be used against AES-256 to perform the conversion.

Leo: So you can validate it by running it backwards.

Steve: Yes. Basically you can completely validate it. Now, the other thing that's possible is the reason they use HTTPS is not because they're worried about encrypting the already encrypted data. As Mary points out, it's been encrypted, so why do we care? It's because HTTPS is the only solution for providing authentication. We remember that HTTP can be intercepted, and you could be subjected to a man-in-the-middle attack. So their client is using SSL's authentication to make sure that you've got a non-spoofed, non-intercepted

connection to LastPass backend servers.

Now, we don't have to worry about that being used to obscure what they're doing because there are several libraries and tools which do allow users, end-users, to look at encrypted data. I've got one that I use and like a lot. And I can bring up the menu here on the fly to remember what it's called: HTTP Analyzer. And it is - it's a tool which is able to intercept SSL communications on my own system. It's able to do that because Microsoft implemented the cryptographic libraries as separate modules. So it's possible for something to hook those and show the data that's being encrypted as it's going into Microsoft's encryption library. And so you're able to see the contents of your own local SSL communications because it happens before it gets encrypted.

Microsoft also has something called Fiddler. Fiddler2, I think, is the current release. And it similarly allows you to intercept and monitor these kinds of - this kind of traffic. And there was some discussion of some other similar libraries in this forum thread.

So this very skeptical person who was in the dialogue with the LastPass guys, he went to the trouble of capturing packets, grabbing the data, dropping, basically recreating from this js/enc.php page, dropped that stuff in, decrypted it, saw what the contents was, verified what was going on. And I, about a week and a half ago, followed in his footsteps to do the same sort of thing. So I've seen all this, too. So again, LastPass has no commercial incentive, in my opinion, for violating our trust and privacy. All of their communications can be monitored, can be verified. They've provided all of the protocol for doing that. Now, the one thing I haven't addressed yet from Mary's question is what about the possibility of some sort of WEP...

Leo: Error, kind of.

Steve: ...error.

Leo: Yeah.

Steve: And that's what I really like about this is one of the enemies of security, as we know, is complexity. And there isn't a simpler, more straightforward solution than what these guys have done, simply taking your username and your password and hashing it using a secure SHA-256 hash, which is super strong, not now like SHA-1, which is pretty much too weak to be usable. They're using SHA-256, taking that data. That produces a key which they simply use with AES. I mean, it doesn't get any simpler than that. And what's beautiful about it is the transparency. There just - there isn't any room for there to be a mistake. They're simply using your credentials to produce a key which is used with symmetric encryption. And so, again, it's just - it's clear and clean and simple and completely verifiable.

Leo: Excellent. Moving on to our next question, Question 3, a listener requesting anonymity in Boston, Mass. mentions a LastPass vulnerability, he says, due to their password account recovery request system: Steve, thanks for the great LastPass review. If I leave my email account open, or somebody knows my email password, then anyone with access to a PC where I have installed and used LastPass can break into my LastPass account. Actually this is good for me to know because I in fact have

LastPass on all my computers. And some of the computers, like the ones here in the studio, are left, you know, people can get into my system if I forget to log out. I lately have been doing that.

By default, this Preference => Advanced option, so you go to Preferences, Advanced, is selected: "Save a disabled one-time password locally for account recovery." At login, if an intruder selects "I forgot my password, help," he's taken to the account recovery page to activate your local one-time password and recover your account. The intruder enters my email address and then receives a message sent to my email account, and he gets the option to set a new LastPass master password for my account. I'll vouch for it. This does work. I've done this, actually.

This is a weakness that could be resolved by changing the account recovery default to deselected in that Preferences => Advanced area, as I have done manually. This option is presumably set to assist all those people who forget their LastPass master password. But it's a real vulnerability which should be addressed. Regards. What do you think, Steve?

Steve: Okay. He's completely correct. And this is a feature which I didn't have a chance to cover last week among everything that we did cover. And so I wanted to bring it to all of our listeners' attention. Because it is absolutely the case that the LastPass folks cannot decrypt the data that they are saving for us, storing for us, using the Internet cloud to synchronize among multiple machines, which is the cool thing about LastPass, the fact that it's so ubiquitous across platforms and devices. If a user loses their password, it's over. I mean, there is no - they do not have the password. You would not be able to log into their system because you need your password to create that hash which is used as the login credential. Nor could you ever again decrypt the data which has been stored. I mean, you're just completely out of luck.

So at some point I'm sure people had problems with this. Probably in the early days of LastPass people contacted them and said, gee, I've really been liking your service. I've created passwords that I haven't written down anywhere. But I've lost my - I forgot my master password for LastPass. I need you to tell me what it is. And so they said, uh, we don't know. I mean, that's the whole point is we don't know. TNO, baby.

And so I'm sure they had a skull session and did some brainstorming and said, look, we have to have some solution for, like, optional for account recovery. And so what they came up with was sort of clever. We talked about how you can create one-time passwords. You can, if you know you're going to be roaming around, and you don't have other means for doing multifactor authentication, so that using your username and password in a potentially hostile location might create a vulnerability, you can ask them to create some one-time passwords for you. They're annoyingly long, but that's good. You write them down in your wallet or whatever, and you sort of have them, if you ever need to log in somewhere scary.

So they said, okay, we can use that by creating, for everybody, by default, putting one of these on the machines where they're using LastPass, and but we'll have it disabled so that it can't be used until our script enables it. So what they did was, and I've tested it during my getting-to-know-you phase with LastPass, just as you had used it in the past, Leo, and it works very well. So you're able to tell them that I've forgotten my password.

Now, other systems that people are familiar with where you lose your password, they actually have your password, so they're able to - they ask you some security questions

or something, and then they reset your account with, like, a temporary password that allows you to log in, and then you change it back to something that you want. Which means they have access to your data. Well, LastPass explicitly doesn't have access to your data. LastPass doesn't have the ability to give you a temporary password, except that they've prestored one, if you've chosen this option. Or I should say, if you've not deselected the option, they've stored one on your machine.

So this listener's point is correct. For the maximum security you should go into the Preferences - log in with the web browser. Go into the Preferences and, under Advanced option, disable that one-time password stored locally, recognizing that doing so means they can never help you, nothing can help you, no force on earth can help you if you forget your master - if you forget or lose or somehow get confused with your master password. So I guess I would be a little more comfortable if this were disabled by default. On the other hand, if it were disabled by default, then it's just the same as not having it because people who forget their password would have no way of recovering themselves. So, I mean, this is a tricky one.

Leo: I just turned it off. I hope I don't forget my password.

Steve: Yeah, maybe they ought to, like, bring up a special dialogue when you're setting up your account and saying, okay, look. There's one softening of the absolute security here that we've come up with where, if somebody has access to your email system - I mean, and so you could see all the requirements that have to be lined up. They have to have access to the computer where these one-time passwords are stored. They have to have access to your email account, meaning they have to be able to access that and log into it in order to receive the email at the registered email address where the LastPass folks send a link which is used to activate the otherwise, the normally disabled password. So they did everything they could to still protect us, while giving us some way out. But the very fact that there is some way out creates a theoretical potential vulnerability. So you can disable that, but then there is no way out. If you've lost your password, it's over.

Leo: So it looks like it's on a per-machine basis because it doesn't seem to save that setting across all the machines.

Steve: Correct. Per...

Leo: So you could turn it off on all the machines except for one machine that you know no one would ever get access to, for instance.

Steve: Exactly. Exactly. And so, for example, yes. If you had machines where you did not have full, tight, administrative control, absolutely disable it there.

Leo: So this is what I've done. I've turned it off on all the machines in the studio. But my home machine, I'm going to have one machine where I could, if I really got in trouble, save it.

Steve: I think that's a very good policy.

Leo: Okay, all right.

Steve: That way you do have a way to recover if the worst happened.

Leo: Yup. I just have done that. I like having the USB key with the multifactor authentication. I think that's - instead of a YubiKey. I could have used a YubiKey, but this works quite nicely, as well.

Steve: Yeah. And it's, I mean, you're able to add it to an existing one, and the price is right because it's free.

Leo: It's free.

Steve: Yeah.

Leo: All right. Moving along to our...

Steve: Although we should mention it's free for the people who have upgraded and are paying the $1 a month, the $12 a year.

Leo: Right, right.

Steve: Because that is a feature that you need to have the paid version for. Whereas the YubiKey, you buy that once, and then that will work with the free, the 100 percent free version of LastPass.

Leo: Mm-hmm. Ren van Belzen, who lives in The Netherlands and has our deepest sympathy for the World Cup, wonders whether LastPass filters out dictionary words. You mentioned the word "gibberish" a lot - I wonder if there's a Dutch equivalent? I bet it's a great word - when referring to random data in SN-256. However, aren't dictionary words a subset of randomly produced strings of characters? Yes, I guess that's, strictly speaking, true. An infinite number of monkeys typing gibberish on an infinite number of computers would eventually type all the words in the language, in every language, ever. So my question to you is, what did you find out about if and how LastPass filters out easy-to-guess passwords? Also, is there a way for me to check the strength of the password independently of LastPass? It does give you a strength meter on it.

Steve: Yes. LastPass does have a built-in strength meter, which I didn't mention, but that's another feature. One thing I did mention that I'll highlight. First of all, I had the exact same thought, which is, if you only used characters, it would be theoretically possible for the password LastPass generates to be words which occur in the dictionary. In which case, that would not be good.

Leo: Turns out to be highly unlikely.

Steve: Well, very, very unlikely, especially a 10-character word, where each character is being chosen randomly. The chances of that are one in 7.9 x 10^17, divided by the number of words in the dictionary that are 10 characters long, which is not many. But the point is, their random password generator does have a very nice feature, where you can specify the minimum number of digits that you wish to have forced into your however long password. So that pretty much breaks the pure word dictionary deal.

So you could say, for example, out of my 10-character, assuming 10-character password, I want to have a minimum of four of those be digits. In which case you're not going to have a 100-percent dictionary match. They can't do a dictionary exclusion easily because they never get the unencrypted words. They never get the unencrypted passwords. The only way they could do it would be if they downloaded into your plug-in the entire dictionary in whatever language was local to you, and then made sure that they weren't choosing any. Which seems like much more work than it's worth, especially when you can just say salt this thing with some digits, and then the problem's gone.

Leo: Salt it. I like that phrase. Question 5, Ronald Stepp in Enterprise, Alabama. He asks several great questions: Listened to the, as always, excellent Security Now! podcast, this one about LastPass, which I am now using, thanks to you, Steve. One question that kept popping up in my head was what do you do in the case of something like the iPad - oh, this actually is my question, too - where iTunes or the App Store, something that isn't a website, keeps asking for your password to verify it's really you? LastPass doesn't have a plug-in for it, it's not browser-based, and there's no easy way to insert it inside such places on the iPad. So we have to forget everything we know about password security just not to lose your mind when you exit the application, go into LastPass, bring up your Apple password (in this case), copy it to the clipboard, go back into iTunes or the App Store and paste it in. Which is, by the way, what I do. Is there something I'm missing, or does Apple just not really put any kind of premium on secure passwords? I don't know if you'd blame Apple for this.

Steve: No.

Leo: There's a lot of applications that do this. If an application asks for a password, you've got a problem. Hard to believe, especially now as we see an example of what happens when companies force us to keep our passwords simple. Twice in the last couple of weeks iTunes has been hacked by developers. This is, by the way, a true story, although not hugely widespread. I think there was 50 or so, maybe a hundred computers that were hacked. I personally have a short, six-character password and am thinking of changing it to a 10-character password. I wonder if the YubiKey would work in the USB camera adapter plug for the iPad? It should, by the way.

Steve: It does.

Leo: It does, okay. Just a thought. Also, in passing, my Verizon MiFi has a 10-digit,

all-number password that I cannot change. Not true, by the way.

Steve: I know.

Leo: Okay. Another example of something that worries me. Thanks, keep up the great work, looking forward to CryptoLink. Can I say his name?

Steve: Yes.

Leo: Ronald Stepp, Enterprise, Alabama.

Steve: Okay, so a couple points. Exactly as you noted, one of the, I don't know if I would call it a downside or a downfall or anything against LastPass, but it isn't a system which is able to universally provide passwords to other applications.

Leo: They could conceivably do that on Windows and Mac, on an operating system.

Steve: Yes. That was exactly the point is that, certainly where you've got a multi-windowed, multitasking OS, it's much easier to look up a password, either by logging into LastPass and using their browser plug-in to bring up the words, or even to use that standalone, the really cool LastPass Pocket, which is basically a standalone viewer. You could easily use it very much just like a password vault. And there it's much easier to, of course, using a mouse, to cut, copy, and paste between the two and drop it into password fields.

With something like an iPhone or an iPad or a device with a much more constrained UI, exactly as Ronald says, it's a pain in the butt to have to switch applications, go over and open up your vault and copy it and so forth. There isn't a solution that I can see. One of the features and security benefits of, for example, the iPad is that it really enforces inter-application privacy, so that it isn't possible, for example, for LastPass to run things in other apps and know what you're doing. They're pretty much excluded, which is why they've created their own browser, that tabbed browser for LastPass, for the iPad, so that they've got their own browser where they can add that functionality. So it isn't a deficiency in LastPass. It's only that we would like to use the LastPass technology everywhere, even not for logging into websites, but for logging into other applications. And on OSes sometimes we can. In situations with limited UIs, there just isn't any good way to do it.

Leo: Right.

Steve: And I did want to mention to him...

Leo: And by the way, there's a security risk in pasting it, cutting and pasting it,

because then your password...

Steve: It's on the clipboard.

Leo: ...sits on the clipboard. And how often do you clear the clipboard? Not that often.

Steve: Right.

Leo: So in fact I know this because I accidentally pasted my password into a message to somebody.

Steve: Very good point.

Leo: And I realized, oh, this is sitting on my clipboard. Whoops.

Steve: And malware has had a history, one of the things malware loves to do is to grab your clipboard because you never know what you're going to find on that.

Leo: Right.

Steve: It's a nice place where people often put such things that they intend to keep local on the machine. So that's a really good point, Leo. And I did want to, just for Ronald's sake, mention I also have a Verizon MiFi which I like, and you can change the password through their browser-based interface. You just log into the access point in the same way you do any home router. You log into it, and one of the things you can do on some of the screens there is to change that password.

Leo: Did that immediately, changed the password and the name. Although they do, to their credit, give you obscure name and obscure password. I mean, it's not - it wouldn't be a horrible flaw if you didn't change it because I think it's different for every device.

Steve: And we're hoping that they're not somehow algorithmically related...

Leo: Yes.

Steve: ...in a simple fashion.

Leo: We are hoping that, aren't we.

Steve: Yeah.

Leo: I like the MiFi. Let me know if you come up with a problem with it.

Steve: I do, too. I use it often and like it very much.

Leo: So here's one from Ken Varga, Stevens Point, Wisconsin. He's got an idea for an alternative format for LastPass passwords: Steve, thanks for the LastPass show. Well done. I, too, switched to LastPass, thanks to it. During your show you recommended having LastPass generate 10-character passwords - I did that, by the way. The default is eight, and I stepped it up to 10. And it remembers that, which is nice - consisting of upper, lower, and numbers for website logins - and I also did that - since this provides 59.5 bits of randomness to your passwords. You also noted that by having LastPass not include symbols or other special characters makes your passwords easier to manually type in should the need arise. It also keeps it from breaking. Some sites won't let you use...

Steve: That's actually why I was recommending it, yes.

Leo: Ran into that right away, yeah.

Steve: Yup.

Leo: In that vein, I have a suggestion to further simplify the situation. This is what I did, says Ken. In the LastPass generation screen, I tell it to give me a 12-character password using only numbers and lowercase letters. I also check the "avoid ambiguous characters" box. While I couldn't find documentation on that option, I have experimentally determined that it excludes the numbers "0" and "1," as well as the letters "i," "l," and "o." Makes sense. Those are ambiguous.

Omitting these characters helps makes it harder to misread the password, since it is easy to confuse, for instance, the number "1" with a lowercase "l." This gives 31 unique characters for LastPass to work with. And if my math is correct, a 12-character password should provide 59.4 random bits, pretty much the same as your 10-character solution. I find it much easier - less error-prone - to transcribe, if needed, than one using uppercase and lowercase characters. That's true, especially if you're on something like the iPad. It's a real pain to shift.

Steve: Oh, yes.

Leo: Any thoughts on this? It seems to me that 12 characters is still quite compact;

and most websites, even if storing passwords in plaintext [gasp] seem to allow it. As an aside, 13 lowercase letters provides 61.1 bits of randomness and may be even easier to type, but has the problem of not being allowed - 13 just lowercase, not numbers - but has a problem of being not allowed on some sites for understandable reasons. Lot of sites, I agree, Ken, say we need a number in there.

Steve: Yup.

Leo: What do you think?

Steve: I checked his math, and his math is correct. So I just wanted to suggest that to our listeners as an alternative because I think he raises some very good points. Sometimes, and I'm sure we've all seen some logons where they specifically say you need some upper and lowercase, or they're telling you that you need some special symbols or something. Mostly, though, they say you have to put some digits in. So I like that feature that enforces some digits to be chosen. And I did the same thing on my own ecommerce site. We use a transaction code for the purchase of my software, which at this point is just SpinRite. And I specifically made transaction codes where none of the letters and numbers looked like each other. That is, I exclude any that could be confused, which is a nice thing to do.

And so I think this makes a lot of sense, to say lowercase only, and then choose the option of avoiding ambiguous characters so that you end up with something which, exactly as Ken says, if you need to type it in, it's easy to do so. And I don't think 12 characters is too long. It's two more, obviously, than 10, but still probably within any site's your-password-is-too-long limitation, I would think.

Leo: Right.

Steve: So that's a good point, Ken, thank you.

Leo: And it is a very easy way to kind of ensure that you're not using a dictionary word if you say you have to have a number because, as far as I know, very few dictionary words have a number.

Steve: Right.

Leo: Some do, I guess. Can't think of any off the top of my head. Chris Morton in Gurnee, Illinois suggests that we're not quite done: Steve, I enjoyed your review of LastPass last week. One point I wish you would have made during the show is that password management tools should not be used as a license to abandon regular password updates. Password management tools like LastPass solve the problem of having to remember long and complex passwords, but they don't solve the problem of how your credentials are used and stored on the receiving end. You made good points in regards - you know, there's a great security assay that LastPass does, in

which it will tell you how many sites, for instance, you're using the same password on, things like that. Really nice. I recommend running it.

Steve: Yeah, it's built into LastPass. I also did not mention that last week. But it's like a - "perform a security test," they call it. And it does check to see how you're doing in terms of password length and them being different from site to site.

Leo: That's where I really, being lazy, for years have used the same password. And a lot of sites I don't care; right?

Steve: A lot of our listeners have written to say...

Leo: Pretty common.

Steve: ...gee, thanks, I fixed that.

Leo: Yeah, I'm about to fix that. I'm going to have to go through my whole password store and one by one visit all those sites and change the password to a LastPass-generated password. But it's worth it. You made good points in regard to how long it would take to brute-force even a 10-character password; but this may lead some to believe that, once they set a long enough password, there is no need to change it further. A defense-in-depth, "trust no one" philosophy must consider the risks of password age and server-side compromises out of your own control. I won't get into the argument about how frequently passwords should be changed; I only wanted to make the point password updates should remain a part of good security practices that password management software does not eliminate the need for. Thanks for Security Now!. I enjoy your discussions every week. Chris Morton. Is there anything in LastPass that says this password is six months old, you should be changing it, anything like that?

Steve: No.

Leo: Not that I know of.

Steve: And I guess they could put it in the database that they're storing on the user side. So...

Leo: There might be a date. There might be a date in there somewhere. I should look.

Steve: There's a date of use. So there is definitely a date where they say the last time you used it, because I noticed I was seeing, like, five seconds ago. It was like, oh, yeah, it knows. So what's the vulnerability here? It seems to me that the policy of forcing

passwords to be changed periodically was - and we've talked about it, like remember the people I overheard at Starbucks who was pissed off that his company made him change his passwords, and they also remembered the last four he had used. And so he just, like, defeated that whole thing by quickly changing his password four times and going back to the one he originally had because he likes it and, you know, screw those IT guys.

So the danger is that the password would somehow leak over time; and that you might write it down, and someone might see it; or you would tell it to someone, just like log into your account over the phone or something just one time. And then so it's sort of gotten away from you. So the idea is that changing it from time to time is a good thing. And I agree. I mean, it's not a bad thing. The only real vulnerability I can see with something like this, where we've got LastPass filling it in, would be if we still were using the same password on multiple sites, which LastPass helps us to no longer need to do because it's remembering these things for us. So...

Leo: That would be the obvious problem because, if you were compromised on one site, then other sites would be compromised.

Steve: Right. So we don't have that. The only place I could really see there being a place for, like, safety from changing would be sort of, as Chris mentions, the server-side compromises out of our control. So a given site gets its password, user account data stolen. And maybe it's not used immediately. So, like, it leaks out, or it's on someone's hard drive, and their laptop gets stolen, or whatever happens. So if some length of time later that user account database is exploited, if you had changed your password during that intervening time, from the time it had gotten stolen and it was being used, then obviously you're protected from that exploitation. So I guess that would argue for us changing our passwords frequently on all the sites we visit, which is another level of pain which is substantial. Yes, more security.

The good thing is, we've at least, with LastPass, we've achieved real compartmentalization. That is, every site is now in its own little compartment. LastPass is doing the heavy lifting for us of memorizing and typing these things in. And boy, I can tell you, I mean, I'm spoiled. And I've had so much feedback from our listeners saying, my god, this is just wonderful. I mean, it's just logging me in.

Leo: Yeah. It's really nice.

Steve: It's spectacular, it really is. So I think Chris makes a good point. It was worth discussing. It's one of these things where, yes, you could be more secure that way. Be aware of the liability. It's not something I'm worrying about a lot because we have achieved compartmentalization, which I think is really the big win here.

Leo: Yeah. That's my task is to replace all my, you know, I have three or four passwords I use on a lot of, lot of, lot of sites, and to replace all of those with generated 10-character passwords from LastPass so that I don't have to worry.

Steve: Here's to gibberish, baby.

Leo: Yeah, here's to gibberish. I love it. Trevor Harrison, Langley, British Columbia, wonders why 63 characters for WiFi, but 10-character passwords for websites? Hey, that's a good question. Steve and Leo, I've been listening since Episode 1. Do I now have the GRC University degree in security? Even the Masters Degree? Yes. We give you that degree. It's worthless. Not even a piece of paper. Just our verbal assurance.

Last week you said that 10-character passwords are sufficient for websites, computer logins, email accounts and so on, even high security ones like banks. On the flipside, I remember you saying 63-character ASCII passwords are best for WiFi, as 20 characters or fewer passwords can easily be broken on secure WiFi networks. If 20-character WiFi passwords can easily be cracked, why then are 10-character passwords secure enough for websites, email accounts, and so on? Steve, have you gone off your rocker? Trevor Harrison, oh, Mac Write. He's a regular in our chatroom. Langley, British Columbia. Please don't cancel Security Now! as part of the five shows to be cancelled. No, don't worry. Security Now! is not on the block. And I am not canceling five shows. So what do you say to Trevor?

Steve: Well, the more characters in our passwords, the better. That is a concept we understand well. And we understand that, in terms of security, given say an alphabet of 63 characters, which is what we get if we do upper and lower case and the digits - is that right? It's 62, wait. We have 26 A through Z - 26 uppercase, 26 lowercase. So that takes us to 52. Plus the 10 digits. So it's 62. So 62 characters. So every character we add multiplies the number of possibilities by 62. And as we saw, that gets to be a very big number very quickly, such that 10 characters is whatever that was, 7.9 x 10^17 or something. And oh, by the way, Leo, you were right about - or we did hear, I heard from an astronomer who said that was substantially more than the number of stars in the galaxy.

Leo: Wow.

Steve: He knew how many there were, and you're orders of magnitude more than that many.

Leo: I love having smart people listen to this show. That's great.

Steve: So, yes, 10 characters is a lot. 63 is ridiculously high. My concern is that there are some tradeoffs here. You may find yourself in a position where you need to type in the password manually. We've just been talking about situations where LastPass is not available, but you're using a LastPass-generated password. So, and we've also talked in the past about how incredibly difficult it is to enter in a 63-character password. I mean, I never was able to get my iPod Touch on my own WiFi network initially because there was no cut-and-paste in the early iPhone and iPod Touch. They added it later, and then I was able to cut and paste and get myself online. It just wasn't possible for me to enter that 63 characters of gibberish. And one of the reasons 63 characters is like what I suggest with WiFi is it is massive overkill.

But it's like, hey, you never, I mean, the nature of WiFi configuration is that you set it up in your access point once. You drop it into your various machines once. And then they remember it. And you're never in a situation where you've having to enter it in at

random times. So, and when friends come over, it's like, okay, you can stick it in Notepad on a USB stick and give it to them, and they can drop it in in order to get onto your network. So my feeling is the model with WiFi is different than the model with website login.

And I doubt that most websites would accept a 63-character password. It's unfortunate because they ought to. They ought to accept an any-length password, which they then hash into a 256-bit hash, and then that's the token that they use, in which case they don't care about password length, that is, there's no practical maximum. But they typically don't. And many passwords, if you're logging in and watching yourself type, you get to a certain point and it stops accepting more characters. So it's got a fixed limit on the web form for how many you can type in.

So I chose 10 as an example in last week's LastPass podcast because it's a large number. We saw how large it is. It's convenient if you ever had to type it in manually. And it's going to be accepted by default by the majority, if not all, website logons. Whereas 63 characters, or even 40, or even 30, could probably find yourself getting into trouble where it just, you know, websites won't accept it. It's just more than they've got allocated for their passwords, unfortunately.

Leo: Well, and you have the luxury of trying to - brute-forcing WiFi passwords in a way that you don't usually on websites.

Steve: Yes, that's the other very good point is that, I think when I was talking about 20, we were looking at the idea of an offline attack where that's the one known vulnerability is you could take some encrypted traffic home with you, and you could then have a bunch of PS3 number-crunching things running that 4,096-iteration WPA algorithm. And it might have been WEP, in fact, it might have been very early on, like we've been doing the podcast for five years, and WEP was always in trouble. But it's become substantially weaker over time during the life of this podcast. And so WEP's architecture was much weaker. And so it's much easier to brute-force attack WEP than WPA because they really made the WPA algorithm much more processing intensive in order to generate the key from the password. So I think it was an offline brute-force attack where 20 characters, you could use huge computing resources. And there, in some feasible length of time, and as I remember, even then it was a long time, but that's very different from brute-forcing across a web connection where you submit your password, and you kind of go, hm hm hm hm hm.

Leo: Yeah, da da da da da.

Steve: You know, you're waiting for...

Leo: You can't do millions a second that way.

Steve: Exactly. Precisely.

Leo: Steve, I think, unless I'm missing something, that's all of them.

Steve: We did our - we got 'em.

Leo: For the first time in a long time, got through all of them. Leo should start on time more often. Steve Gibson is the host at GRC.com, what a great website for anybody interested in this. There's some great discussions there. Of course Security Now! lives there. Not only the full, high-quality audio of the show, but also 16KB audio for people who are bandwidth impaired. Steve makes that available himself, does all the work on that. He also pays for transcriptions, which are available at GRC.com, and show notes and all that. We do video now of the show. And you can get the video and the high-quality audio at TWiT.tv/sn, or of course subscribe on iTunes and the Zune Marketplace and all those other great places where you get video and audio.

GRC.com is also the home of SpinRite, the world's finest hard drive maintenance utility. You must have it. Get it. Don't even ask me. Just get it. Just get it. Do it. And many other freebies like ShieldsUP! and all his other great programs on there. Soon I'm sure some more stuff I know you're working on.

Steve: Yeah, I had a bit of a setback with the DNS Benchmark. I actually finally took it to v1.0, and that lasted about a day.

Leo: Yeah, of course. The hubris of saying 1.0.

Steve: Oh. After waiting, like, nine months before I did that, I then took a look for the first time at Google's namebench DNS benchmark. And it's got some problems, frankly. I asked a bunch of people in our newsgroups to give it a try, and it almost universally crashed everyone's network.

Leo: Yikes.

Steve: But one thing it has is this phenomenal list of about, for some reason I'm remembering 4,300, but I think it's more than that, resolvers all over the world. And it tries to find, from that list, the ones that are fastest for you. So what I did was, I thought, okay, I've got to figure out how I feel about this because I had, like, a list of maybe, I think of maybe like 80. And they were good resolvers for the U.S. But it was U.S.-centric. And so I hacked a version of the benchmark. The benchmark normally limits you to testing 200. I figured, that's going to be enough for anybody. But I had to have it test, I think that's actually the number I have now, is 4,800. So I set it to, like, 5,000, had to completely change data structures and things around. But I did. And then I asked a bunch of the users in the newsgroups to try this, I call it the megaplex.ini, which was all of these resolvers. Every single one of us found DNS resolvers we had never known about before that were faster than any ones we had ever seen.

Leo: Really.

Steve: So in this incredible list that Google had were secret gems. I mean, it knew of, like, resolvers near me. It was like, geographically near me, like Cox has one, and

somebody else had a different one, and it's like, whoa. And so I thought, okay. I've got to do something about this. So I'm now completely reengineering, I'm like in the middle of it, the way we handle the resolver list building so that GRC will maintain a master list. And then part of the setup for the benchmark will be the user will dynamically receive this list from GRC which they will then run through a process, sort of a preliminary benchmark, to select the best 50 out of this much larger list. And then that will be their custom list, against which they will do the full benchmark. So it's a little more involved. But the cool, I mean the upside is, virtually every single person who runs this will learn something new. They will find resolvers they never knew about that are faster than anything they've ever seen before.

Leo: Wow, that's really neat.

Steve: So it's going to be very cool.

Leo: That's really neat.

Steve: Yes, back to the drawing board. But it's going to be worth it when I come out the other end.

Leo: No kidding. Some real utility, additional utility. That's kind of the idea, I guess, really, of benchmarking, is figuring out what's the best.

Steve: Yeah, exactly. And I wanted, like, I want to surprise people. So now I can.

Leo: Yeah. Well, good. Steve Gibson, GRC.com. We'll see you next week. We do the show live Wednesdays, 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1800 UTC at live.twit.tv. You're invited to watch live and participate in our chatroom. Always a lot of fun, about 800 people in there usually, at irc.twit.tv. Steve, we'll see you next week on Security Now!.

Steve: Thanks, Leo.