SECURITY NOW!

Transcript of Episode #360

Listener Feedback #147

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-360.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-360-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is back! He's refreshed, he's ready, he's going to talk about the Microsoft updates, security flaws, password leaks and, yes, your questions, too. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 360, recorded July 11th, 2012: Your questions, Steve's answers, #147.

It's time for Security Now!, and what a great opportunity. This is one of our most popular shows. Steve Gibson is here, of GRC.com, our Explainer in Chief. This is one of our most popular shows, and in fact one of the few shows that numbers are going up and up consistently. And I have to think it's just people are more and more aware of the issues of security. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be back with you after our two-week hiatus.

Leo: Yes. Thank you for letting me do that, by the way.

Steve: I'm not letting it happen again.

Leo: Oh, no. Why not?

Steve: Well, I missed it, actually. It was like, wow. It was odd not doing it. And all I need is a little hour of your time, just to do a little time skew.

Leo: So never again. You're saying we will never miss an other episode again.

Steve: No. And maybe it was good that we did one, just so that we broke our perfection.

Leo: Well, I'm just going to say this. You're going to be fighting, not me, but a person named Lisa. And whatever you guys work out is okay with me.

Steve: All right. And someone tweeted that we were okay until 2018. They've already figured out when the next time is...

Leo: Oh, once every five years. That's good.

Steve: ...that July 4th falls on a Wednesday. So it's like...

Leo: Oh, well, that's fine. In 2018 we'll take the day off.

Steve: What? No.

Leo: We'll discuss it then.

Steve: All right.

Leo: Actually this was an important week because of the hoorah, and I don't know if you plan to talk about it - in fact, I should run through your outline, I don't think you are going to talk about it - of DNSChanger.

Steve: It's the topic of the entire next week's podcast.

Leo: Ah.

Steve: Because Paul Vixie...

Leo: Love him.

Steve: ...who is extremely well known, he's one of the Internet pioneers, he's a cofounder of ISC [Internet Systems Consortium] that are the creators of BIND, the leading DNS server. He was very involved, it turns out, with the FBI's effort in doing it.

Leo: Really. Well, then I can blame him. I'd like to hear his explanation of why this was such a good idea.

Steve: Well, as a matter of fact, that's what we're going to do next week.

Leo: Good.

Steve: We're going to completely cover it. And what was interesting was, as you said, it was like this biggest non-event. I was...

Leo: CNN said, "There is a major virus out there, and it strikes on Monday." Morons.

Steve: Yeah, and people were coming up to me as they were hearing about it, saying, "Oh, Steve, do I have to worry about this? What's going to happen? I'm told that there's some horrible thing's going to...." I said no, nothing is going to happen.

Leo: Idiots. Not the people. I don't blame people because they're getting informed by news media that is stupid.

Steve: Yeah. And people were being told that it was some malware that was going to strike them, rather than a six-month delayed reaction to something that was pretty much by now a non-issue. It was weird that it captured the amount of press that it did. But Paul Vixie...

Leo: I was just disappointed that more people weren't angry at the FBI. But maybe you're going to convince me that this was a good idea.

Steve: I think I'll be neutral on that topic because to me that's...

Leo: Okay. I'll be the negative.

Steve: What captivated me was the things that Paul said and wrote that I'm going to share with our listeners next week. He had a lot of really interesting points to make. So I'm going to share that, and then we're going to get into a discussion next week.

Leo: I have huge respect for him, and of course he's the father of DNS. So if he says it's a good idea, then I still don't believe it, but...

Steve: And actually he has a lot of good stuff about all of the recent - as I was digging into this, doing some pre-research for next week, I realized naturally he would have been very, very much out in front of the whole DNS filtering, SOPA, and all of that nonsense that we have been dancing around with. So that's for next week.

This week is Q&A #147. We've got 10 great questions. Actually, some surprises that I encountered as I was going through the mailbag. So we've got a great Tip of the Week to wrap it up, and something that surprised me is second to last, and a bunch of things to talk about. But I just wanted - there was so much reaction, literally withdrawal, from us not having a podcast for our listeners last week, that I was going to assure everyone that, by hook or by crook, we'll make that not happen again. But it was kind of fun to have it happen once because, you know.

Leo: Whatever you say, Steve. Another Patch Tuesday. Seems like it was just Patch Tuesday. I guess last month.

Steve: That's because we skipped an episode, Leo.

Leo: Oh, come on, stop it. Geez, you'd think I let something die or something. Come on.

Steve: Oh, you didn't hear from the listeners.

Leo: Oh, I hear from the listeners. Are you kidding? You think I don't hear from the listeners? You think they don't contact me at the drop of a hat?

Steve: Okay.

Leo: I love hearing from them, but that doesn't mean they get their way every time. That's your mistake.

Steve: We did have the second Tuesday of the month pass by just before the day that we skipped the podcast. And we had finally the XML Core Services flaw patched.

Leo: Well, well.

Steve: This was something - yes. This was the zero-day exploit that we've been talking about every week since it was revealed because it was revealed shortly before June's Patch Tuesday, certainly not enough time for Microsoft to do anything, although they did put up one of their Fixit buttons, their single-click Fixit. And I really strongly advised all of our listeners to go push that button because we just don't need XML Core Services in Internet Explorer for sites that we're visiting. We can live without that. Again, this is Microsoft's "default enabled" approach, unfortunately. So they got that patched, plus 15 other problems of varying security. There was, like, two problems with IE and something else with WebDAV or a database something or other. So it's one of those, just do it. I've done it on my various machines. And it's good that we've finally got a correct fix for this XML Core Services problem.

Now, the thing that was related to this that I just sort of shook my head over was Microsoft's Security Advisory No. 2719662. Now, that to me looks like, not a date encoded in that, but probably Advisory No. 2,719,662 because that feels like it's about the right number of advisories that we've had with Windows so far. And this one is "Vulnerabilities in Gadgets could allow remote code execution." And there's another Fixit. This Fixit turns off the Windows Vista and 7 Sidebar and Gadgets. Just turns it off. It's like, whoops. We're sorry we ever thought that was a good idea. We're turning those off now. And I was like, what? What? And so, quoting from Microsoft's advisory, it says:

"Microsoft is announcing the availability of an automated Microsoft Fixit solution that disables the Windows Sidebar and Gadgets on supported editions of Windows Vista and Windows 7. Disabling the Windows Sidebar and Gadgets can help protect customers from vulnerabilities that involve the execution of arbitrary code by the Windows Sidebar when running insecure Gadgets. In addition, Gadgets installed from untrusted sources can harm your computer and can access your computer's files, show you objectionable content, or change their behavior at any time." What a nice technology.

"An attacker who successfully exploited a Gadget vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Applying the automated Microsoft Fixit solution," we are announcing today, "described in Microsoft Knowledge Base Article [blah blah blah] disables the Windows Sidebar experience and all Gadget functionality."

So they're saying, whoops, we're sorry about all those desktop gadgets that we were promoting so heavily for the last many years. We've decided they're no good anymore. So just click this button which we're proudly announcing, and they'll all go away. Now, I only miss one. And that's the gadget that tells me how many hundreds of days left I have of Windows XP support. I rest my case.

Leo: Ooh. Very good point.

Steve: And then of course the big news that occurred, dare I say during our hiatus, was the Cisco/Linksys router firmware fiasco. You have to call it that. This affected two brand new high-end routers, the EA3500 and the EA4500, which were first released in April. These are big, as I said, high-end routers. The lesser of the two, the EA3500, is $140. And that's an N750 dual-band gigabit USB, powered by - and here's the problem - powered by Cisco Connect Cloud App Enabled. And then its bigger brother at the top of the line is the EA4500, $200 for this sucker, an N900 dual-band gigabit USB DLNA media server, powered also by the Cisco Connect Cloud. Well, this is the new thing, this Cisco Connect Cloud, that is causing the problem, is behind all of this.

What happened was everybody bought these in April. And you're not going to have low-end users, probably, spending between $140 and $200 on a router. This is going to be your serious home networking guy that wants DLNA-enabled media server stuff. So these are people, my point is, that knew what they were buying and why. And so they doubtless - this is now, what, April, May, June, July - plugged it in, logged into its admin interface, and pushed a bunch of buttons, and tuned it up. And if they're podcast listeners, if they listen to this podcast, they probably disabled Universal Plug & Play support, if they know they don't need it, or maybe statically mapped ports through in order to use the Xbox gaming through their router, I mean, deliberately spent some time tuning it up. Probably disabled WPA PIN use of the router. So spent some time with it to get going. Then, a couple weeks ago, without notifying anyone, Cisco autonomously, in the background, updated the firmware across...

Leo: Really? Without asking? Without notice?

Steve: Without any notice. Without any notice.

Leo: Oh, that's not nice.

Steve: So what that means is all these routers were phoning home periodically. That's the only way Cisco would know where they were. They were phoning home, saying hi there, I'm this fancy new router, got any news? And Cisco said, ah, thanks for checking in. Here's new firmware, brmmp, and sends the firmware down. Now...

Leo: Wow. I didn't even know they had that capability.

Steve: Get this, Leo. It removed the admin interface...

Leo: Oh, come on.

Steve: ...so that then these high-end router customers attempted to log onto their router and were told, oops, sorry, you need to go set up an account with Cisco Connect Cloud in order...

Leo: Come on. I bought this hardware. You're making me do something? Holy cow.

Steve: In order to manage their own router.

Leo: Oh, that's just evil.

Steve: Well, and it gets worse because then people looked at some of the fine print in the agreement that went with this, that says, for example - and I'm quoting. I copied and pasted this out of their license this morning. "For example, if you download a media app, the Service" - that's capital "S" because attorneys were involved - "Service will need to share information with the third party about what media content..."

Leo: What?

Steve: "...you have in your home network, or if you download a parental control app, the

Service" - again giving you a big Service here, a capital "S" - "will need to share information with the third party about what devices are inside your home network."

Leo: Well, that's weird. Can you think of a reason why that would be needed? Anti-piracy is the only thing I can think of.

Steve: Well, and it also says, "When you use the Service, we may keep track" - okay. And remember, using it is not optional. You attempt to log onto your router, and your only choice...

Leo: You have to.

Steve: ...is to go create an account with Cisco Connect Cloud in order to then use web-based admin. And what they're selling is that you can remotely administer your router. So it's cross-device, it's web-based, meaning that you can use a smartphone from somewhere outside your home network to do stuff on your router. And it's like, okay. That can't possibly go wrong. Uh-huh. Yeah.

Leo: Wow. I have one of those. I'm throwing it out right now. That's it. Goodbye.

Steve: So they're saying, get this: "When you use the Service, we may keep track of certain information related to your use of the service. Among other things, that data may include how much traffic is going through the router every hour and includes the Internet history from the home network."

Leo: No, no.

Steve: So basically people have installed spyware boxes without knowing it.

Leo: What? Now, I'm trying to think, because sometimes they do these Terms of Service because for a technical reason they need to be able to act. But I can't think of any technical reason why they'd need to know any of this. Your history?

Steve: You can imagine the backlash...

Leo: Holy cow.

Steve: ...against this as people dug into it and read these Terms of Service.

Leo: This is clearly the Motion Picture Association of America, people like that. Right?

Steve: Well, the most benign thing we could say is that it is some plan that Cisco has for monetizing their customers in a new way. So they're talking about selling aggregate information. This looks like it's - they're saying they need to peer into your network and see what media you have and what devices you have.

Leo: And why would they need my Internet history? That is just a flagrant invasion of privacy.

Steve: Yeah. And the problem is they have access to it. They are the router that connects the internal home network to the Internet. Everything, as we know, passes through it. The good news is SSL doesn't. But, for example, DNS queries do, unless you're using encrypted DNS. So they're in a position with a powerful router to aggregate information. And we already know these things are phoning home because they all - every installed one spontaneously updated itself...

Leo: Horrible.

Steve: ...to do this. So as a consequence of the backlash, Cisco quickly responded and put up instructions for downgrading these routers back to the previous firmware because users were so upset. Many people simply returned them. They said, "I'm not keeping this."

Leo: That's right. Don't keep it. Because you know what, that means they still could do this. They have unmonitored access.

Steve: We don't know what the router is doing on the outside, on the WAN link. There's no way to know.

Leo: Shocking.

Steve: Not good.

Leo: Shocking. I will never use another Cisco/Linksys router again. And we won't use them in our enterprise. That is appalling. And I don't think that's a mistake. There's a new trend going on, and I call it - this is not a mistake. I call this the "Facebook M.O." Facebook's pioneered this, and I'm seeing more and more companies do this, which is you do it even though you know it's wrong and bad. You apologize afterwards. You fix it for those who complain. Meanwhile, 90 percent of your customers never notice and just go along with it. And you get away with it, basically.

Steve: Yes. Imagine all the people who have not logged into their router to discover what has happened behind their backs.

Leo: Right. Or they don't care because they don't understand the ramifications. And Cisco knows that, as does Facebook, as do a lot of these companies now. This is the new M.O. in Silicon Valley. Shocking. Horrible.

Steve: See what you can get away with.

Leo: Yeah. Well, just do it, apologize afterwards, and most people will never notice anyway so you really will get away with it. And those who complain, you fix it for them. Horrible. Well, I won't be using their stuff ever again.

Steve: Yeah, I have an old little Netgear that I'm quite happy with, and an older Belkin.

Leo: Holy cow. That is just shocking. That's true malfeasance.

Steve: So we had another 420,000 password hashes stolen.

Leo: I saw that. Geez.

Steve: Formspring, a social networking Q&A site, whatever that is. I kind of went there and poked around.

Leo: I have an account there. Quora is better known. On Formspring you can ask me a question, and I can answer it. It's a Q&A form.

Steve: Ask the 'Net? Like ask everybody? Or...

Leo: No, ask specific people.

Steve: Oh, really. Interesting.

Leo: So Quora is you ask an open question. Anybody can respond. This is more like Reddit's Ask Me Anything, where you say, "I'm here, what do you want to know?" and you'll answer questions.

Steve: So the good news is they were hashed, and they were salted, and they were well hashed.

Leo: Good.

Steve: They were not as well hashed as they could be. In their blog they said, "We were notified" - and it's really fun, or not fun, but it's interesting to see how these companies find out because the first any of these companies know that this has happened is when they discover, people tell them, "Oh, by the way, apparently 420,000 of your you-thought-they-were-secret password hashes are out on the 'Net, have been posted, and people are rummaging around through them." So they said, "We were notified that approximately 420K password hashes were posted to a security forum, with suspicion from a user that they could be Formspring passwords. The post did not contain usernames or any other identifying information." Of course the bad guys had those, but they were just posting the passwords to prove they had everything.

So this blog goes on: "Once we were able to verify that the hashes were obtained from Formspring, we locked down our systems" - too bad they hadn't done that previously, I guess - "and began an investigation to determine the nature of the breach. We found that someone had broken into one of our development servers and was able to use that access to extract account information from a production database. We were able to immediately fix the hole and upgraded our hashing mechanisms from SHA-256 with random salts" - so, okay, they were implying good practice - "to bcrypt to fortify security. We take this matter very seriously and continue to review our internal security policies and practices to help ensure that this never happens again."

Now, bcrypt is not something we've spoken of directly. I've spoken of what it does many times because this is the password-strengthening approach. What's sort of interesting about bcrypt is it's explicitly scalable, that is, we've talked about, for example, how I think iOS was initially hashing, iteratively hashing using so-called password-based key derivation, that horrible acronym PBKDF2. iOS was doing it, I don't remember now, like 2,000 times, and now they're doing it 4,000 times. And we talked about how a couple weeks ago LastPass added that, but to existing customers it was still set to zero by default, so we advised all of our listeners to go set it to 512, which I think is their recommended number. And then they're now doing iterative hashing.

The point is, it doesn't actually create more security, but it lengthens the time that any kind of brute-force cracking requires by that factor, by a factor of 512 or 4,000 or whatever. So the fact that Formspring has switched to a bcrypt-based approach says, okay, they were good already, random salts, SHA-256, that's all good. And now they've decided, well, there is a little more we can do, so we're going to do that, too.

So there's really no egg on their face. It's not like they had MD5 hashes, as we recently saw. They were doing good hashing. Random salts is best practice for hash management. So it's unfortunate that those got loose. They immediately shut down logins, required all users to change their hashes using an email loop in order to reauthenticate themselves and had to create new passwords. And they also posted at that time best policies for what constitutes good passwords. So they acted as we would hope anyone could.

Leo: Should you change your Formspring password now? Should I?

Steve: You have no choice. You cannot log in without doing so.

Leo: Good. Even better. Even better.

Steve: Yes. So they immediately improved their security and then required all of their users to use that improved security for the passwords which they are now storing in a password database which they believe is more secure than, well, I'm sure it's more secure, and hopefully it's secure enough to keep from the bad guys.

But speaking of that, something else happened that had a lot of people scratching their heads initially, and that is there was a massive attack across 50,000 websites that were defaced with the installation of the Blackhole Exploit Kit. Now, this is something we spoke of recently because, for example, the XML Core Services vulnerability was turned into an exploit that was recently added to this Blackhole Exploit Kit, which is a popular hacking kit that the black hat people are using in order to, for example, get into people's machines using unpatched vulnerabilities in Windows.

So people were saying, wait a minute, how did people get into 50,000 websites? There was initially not anything obvious that they had in common. They had completely different servers, some running Windows with IIS, many on Linux and UNIX running Apache or other web servers, different automation, some were running .NET, some active server pages, some PHP, so it's like it's very heterogeneous. But someone noticed they all had the same management software. They were using a system called Plesk.

Leo: I've used that. It's excellent.

Steve: Yes. It is the second most popular remote website, remote server management, remote site management.

Leo: It's a PHP-based sysadmin tool. cPanel's another one, yeah.

Steve: cPanel is No. 1 most popular; Plesk is No. 2. Turns out that Plesk had a known vulnerability that was fixed months ago. But before that, people were able to get in and acquire the server management passwords, which unfortunately Plesk was storing in the clear.

Leo: Oh, dear.

Steve: So even after Plesk was updated months ago, the people used it pre-update, that is, bad guys got in, got the management passwords, the master management passwords for those servers. So when Plesk was updated to fix the problem, the passwords had already left the barn, to mix a metaphor.

Leo: The password has left the building.

Steve: The password has left, yes. So anyway, what happened was 50,000 websites were defaced. And what people need to do, I imagine this is old news for anyone who actually is in charge of any of those websites, you have to change all the passwords because the bad guys have got your passwords using a vulnerability in Plesk that is now old. So there you go.

Leo: The real problem with Plesk is your provider usually has to update that. And they often are slow to do so. So you may...

Steve: Correct. I don't think they'll be slow this time.

Leo: Maybe not, yeah.

Steve: Well, and it's a simple thing to do. They update it, and it fixes that for all their customers who are using remote admin on their services. So that's a good thing.

Now, I have to go a little bit off topic. I'll make it brief because we've got Q&A to get to. But I just did want to mention a couple things. I tweeted some links just now for the podcast, so those are at my @SGgrc feed in Twitter. So Twitter.com/SGgrc. One is a wonderful "Prometheus" parody. And "Prometheus" has been out long enough that I can now release...

Leo: Spoilers, right, yeah.

Steve: You have to see it, if you haven't, Leo.

Leo: I haven't.

Steve: It is the essence of what we were talking about was disappointing about the movie. And so this is a sort of a pep talk, pre-landing consultation of somebody in charge to this group of - we see that they're not that impressive when they actually get on the ground.

Leo: Yes.

Steve: And it's wonderful. So I won't try to...

Leo: Unfortunately, I'm looking for "Prometheus" parodies on YouTube, and there's dozens.

Steve: Yes. And what I tweeted was this was my favorite of the so many deservedly created parodies.

Leo: Guess it kind of begged to be parodied.

Steve: Yeah, you just can't tweet, you can't Google "Prometheus parody" because there are too many of them. But this one that I have in my link is...

Leo: It's a pre-prequel, is what they call it, the pre-prequel.

Steve: That's the one, the pre-prequel. Well, because "Prometheus" was an "Alien" prequel.

Leo: Right. So before the prequel, there's the prequel.

Steve: Yeah. And, oh, it's just wonderful. So people will love that. On Monday I saw "The Amazing Spider-Man." And it's interesting, as I've talked to people about it, many people have heard it was bad. I loved it.

Leo: Oh, good. I haven't seen it yet. Okay.

Steve: So I just wanted to say I loved it. I liked all the Spiderman movies. I liked the new Batman. And I should mention that this is a restart of the series in the same way that the new Dark Knight series is a restart. And so it starts with Peter Parker before he's been bitten and so forth. And I thought it was the most effective 3D I've seen. Of course "Avatar" and then "Prometheus" in 3D. "Prometheus" in 3D just didn't do it for me; but this, it wasn't overdone, but the depth, I was conscious of the depth of field photographically. The things that were further away were also nicely out of focus, so you knew what you were supposed to be looking at, and it was kind of right there in the middle, and things closer to you were out of focus. They did a really nice job.

So if anybody - the point of bringing this up is, if anyone has been dissuaded because they heard it was bad, I loved it. I thought it was great. So I just wanted to say that. And speaking of great, two non-sci-fi things. "The Newsroom," which is a new series on HBO? Wow. I love Aaron Sorkin. And I liked "The West Wing." It was that dialogue that normal people don't actually speak. And in fact he was interviewed by Colbert last week, and Stephen Colbert said, "You realize, Aaron, nobody talks that way." And he says, "Yeah, I know." But anyway, I watch each episode twice, it's so good.

Leo: Sometimes you have to, they talk so fast. You miss stuff.

Steve: Oh, it's just wonderful dialogue. I just love that. And then just a blast from the past: After 20 years, "Dallas" is back.

Leo: No. Don't tell me you love "Dallas."

Steve: Oh, I do. And Larry Hagman still has it.

Leo: He's in it? He's not J.R.?

Steve: Yes, J.R. is back. And Patrick Duffy, and Linda Gray, and Ray. Now, they of course have had kids, and the kids are grown up now, and the show is mostly about them.

Leo: [Geezer voice] "Well, you better go get him now 'cause you're in trouble, J.R."

Steve: Anyway, those two shows are the top two new dramas of the season. Both have already been renewed for a second season. HBO has already committed to a second season of "The Newsroom," and "Dallas" is the No. 1 show now running, nearly seven, 6.9 million viewers per episode.

Leo: Wow.

Steve: So anyway, I watched it in the old days.

Leo: What channel is "Dallas" on?

Steve: It's on TNT.

Leo: I will have to watch it.

Steve: Ah, there's our music [old "Dallas" theme].

Leo: It's not the same theme, is it?

Steve: Yes.

Leo: They kept the theme?

Steve: Yes.

Leo: So it's a pure nostalgia play, then.

Steve: Yeah.

Leo: Because this is the most '70s theme ever. Wow. That's funny. I'm going to have to watch it. I haven't been watching that.

Steve: Yeah. I have to say, now, Larry, J.R., has flown off in a helicopter and left John Ross sort of in charge, which I realized is the way he negotiated his contract. He says, okay, I'll be there for the first three episodes to get this thing going, but then I'm...

Leo: Right, right, right. He is 80 years old.

Steve: Yes. But I'm not kidding you, Leo, it is just so fun to see him still. Even the old...

Leo: Here's the new theme [new "Dallas theme]. They did update it. They at least got rid of the wocka-wocka-wocka guitar there. Oh, yeah, this is much more 21st Century. But it's the same theme, same melody. That's great.

Steve: Yup.

Leo: Wow.

Steve: Even when he was the colonel, was it a colonel on "I Dream of Jeannie"?

Leo: Oh, yeah, yeah, yeah. Major. He was Major Nelson.

Steve: Major Nelson.

Leo: I think he became Colonel later.

Steve: He was a good actor.

Leo: Yeah, Hagman's a good actor.

Steve: Yeah, he really is.

Leo: Now, if they redo "I Dream of Jeannie," I'll be watching.

Steve: As long as they don't use Barbara Eden. I think she's probably a little too far...

Leo: Well, yes. [Geezer voice] "Hey. Hey, Astronaut Nelson. I think I left my teeth in the capsule."

Steve: We don't want to see her in her Jeannie outfit, though. Just have her maybe in a nice pantsuit, that would be good.

Leo: Oh, dear.

Steve: So, okay. Finally, sci-fi books. I know that many people did follow my recommendation for the Lost Fleet series, which I really liked because remember that we had this Commander Geary, who was a hundred years in suspended animation. They found his capsule, revived him just in time to use his long-lost knowledge of large-scale fleet maneuvers in order to rescue the Alliance. And so we had six books: "Dauntless," "Fearless," "Courageous," "Valiant," "Relentless," and "Victorious." Then we ran out. Some people may have been glad. But he has a new series called Beyond the Frontier. I just finished yesterday "Dreadnaught," which is the first of those. And then "Invincible" I have in hardback because it wasn't available for Kindle, but it is now.

So for any listeners who want more, I just wanted to let everyone know that there's two more books now out. I'm less excited about them. There was much less battle and much more feeling that, unfortunately, the author, Jack Campbell I think is his name - I didn't write it down, but I think it's Campbell - it feels a little bit like he's stretching it out. Like okay, come on, let's get going. It's, like, way political. And this was a little - I was impatient as I was reading "Dreadnaught." So I don't recommend it highly. And so there you go.

I did get a nice note from a listener, Brian Semingson, who's in Indio, California. He said, "Hello, Steve. I'm an IT manager professionally, so that means I'm the IT fixit guy for everyone who knows me." And of course many of our listeners and you, Leo, know how that is.

Leo: Oh, yeah.

Steve: "And that brings me to SpinRite. A family friend's PC would freeze on the XP splash screen every time he attempted to boot it up. The only thing I was told was that the computer froze up while their kids were using it. I was thinking I would have to spend the time to get their files off and then reinstall XP, which also meant buying the restore disks, since they didn't have those, either, and it was no longer possible to boot up and get into the machine to create the restore disks. I thought, well, I'm going to try SpinRite. This could save me a lot of time. Plus I've been wanting to try it anyway since I started listening to Security Now!. I ran SpinRite at Level 2 against the drive, and it only took about three hours to finish. Restarted the computer and" - now, he says "boom," but I think he means in a good way.

Leo: One doesn't know with "boom."

Steve: Not that it exploded. "And, boom, loaded right up normally. I was able to create restore disks from the computer's utilities in case it happened again, and was able to give them their computer back the next day. Everybody won on this one. You have a happy customer. I'm happy since SpinRite made this an easy fix. And my friends are happy that they got their computer right back anyway. Thank you, thank you, thank you, thank you." And thank you, Brian, for sharing that.

Leo: Very good. All right. I think you will like these questions, Steverino.

Steve: You know, the world is amazing, Leo. While you talking, I just checked my Twitter feed, and someone named Free, or with the handle FreeJAC, J-A-C, in Canada, tweeted me the link to the BlackBerry sounds that I miss from the past.

Leo: Oh, you're kidding.

Steve: So he's listening in real-time.

Leo: Holy cow. Yeah, because you didn't mention it on the show, this was pre-recording, that you forevermore wanted to keep your own sounds because once you'd lost your sounds. And he sent you the BlackBerry sounds?

Steve: Yeah. I changed BlackBerrys, and the new Blackberry had different sounds than the old BlackBerry. So it's like, oh, I miss those sounds, because I had them all set up to respond to different things. And I couldn't find them. I couldn't get them off. So thank you, FreeJAC. I appreciate that.

Leo: I'm going to have to - did he give a link that we can use? Because I might want to download those, too.

Steve: Yeah, it's BlackBerry App world, BlackBerry's 5.0 sounds. It's fun because the item description says "Download the 5.0 BlackBerry sounds heard around the world for years everywhere: Lightspeed, Sonar, Classic Phone, the entire set."

Leo: Wow. I'll probably recognize these.

Steve: Oh, and he said, "These sounds are not preloaded in BlackBerry 6 or higher, and the set is available free for all users to download here." No, you're right. You will certainly recognize them because I was hearing other people's phones doing that for years. It's like, oh, I know that sound.

Leo: Well, I had a BlackBerry. In fact, I had BlackBerrys from the moment that they were just pagers, just those big pagers with a keyboard, to the BlackBerry Curve. And then this thing called the iPhone came out, and I never used a BlackBerry again. And I have a feeling there's a lot of people like that.

Steve: Yeah, except I'm still, as you know...

Leo: You don't use a BlackBerry, do you?

Steve: Oh, my god. That's what you're hearing go crazy like a squeaky toy.

Leo: That's a BlackBerry?

Steve: Yes.

Leo: Like a BlackBerry phone?

Steve: My best, the best communication device I have ever owned. Absolutely.

Leo: What are you going to do when RIM goes out of business next month?

Steve: I'll buy a few more and have them in storage. I'll stick them in the refrigerator along with my Palm Pilot.

Leo: Wait a minute, wait a minute. Which BlackBerry are you using? The Curve?

Steve: I've got something late model, 9650 or...

Leo: Oh, yeah, that's a Curve. Wow.

Steve: It's got the 640x480 screen, really nice high-res screen. And it's got the new little touchpad instead of the ball. I had to replace the ball, the little roller ball.

Leo: I liked the ball. That's the Bold. You have the Bold. That's what you have.

Steve: I had the Bold. You're right, I had the Bold. And now I've got the Curve. And...

Leo: No, no, I think the - you had the Curve, and now you've got the Bold. I think the Bold - I don't know. Does the Bold come later? Or is it a Torch?

Steve: I think it's the...

Leo: Wow. You are an old-fashioned guy.

Steve: Oh, I want a keyboard. I do not want, I cannot stand typing on a touchscreen. I just - because Apple hasn't done it right. If I press a key and slide my finger off, and it goes click, that means I pressed that key. Apple does not register it. They give me the sound, but they do not register the key. And I just - I guess the way I'm typing, I'm not lifting my finger off of it, I'm sliding it a little bit. And so I just - I can't stand it. I want pushbuttons. I want buttons. I love my BlackBerry. It's the best thing I've ever owned. That and my iPad. Those are my two devices.

Leo: Wait a minute. The iPad's the same as the iPhone.

Steve: Oh, I don't type on the iPad.

Leo: Okay. So you mean, when I hear those sounds like the Yabba-Dabba-Do, that's a BlackBerry, not your computer.

Steve: Oh, no. The Yabba-Dabba-Do, actually it's going to be moving to my BlackBerry soon because I thought it would be fun to be able to walk around and have that happen.

Leo: What a character you are, Steve.

Steve: But I like the squeaky toy, and Jenny has a sound, and so I know when she's sending me something. So, yeah.

Leo: That's cute.

Steve: Yeah, she likes her sound.

Leo: Question #1. No comment. Ahem. Steve, sometimes I feel like you're living in the 20th Century.

Steve: I'm quite comfortable there. I've got PDP-8s behind me.

Leo: He's using Windows XP.

Steve: I have TiVos with the PowerPC that are byte-swapped, TiVo Series Is that are modified. Mark Thompson keeps bugging me to switch to C.

Leo: No, but you have a point because, when something is perfect, just because you make a newer one doesn't mean it's better.

Steve: Oh, and frequently, I mean, we just talked about Cisco here with this ridiculous...

Leo: You don't have a rotary phone, do you?

Steve: Well, not plugged in right now.

Leo: Question 1, Dustin B, Seattle, Washington. He wonders about password system setup: Greetings. Longtime Security Now! listener. I've received a lot of advice over the years about personal password use. My questions today are actually how to best set up an account system such as a small-time web application developer. I don't believe you've talked much about the system side of enforcing user security. Password requirements: While we know the benefits of having our own long pseudorandom passwords, how far should an application go in forcing its users to use a secure password versus causing user frustration by forgetting their password? Is, for instance, more than five characters, including a number, enough? Does it have to be 12 characters with upper, lower, special characters, et cetera?

He's suggesting this is an invalid password message: I've noticed on failed login attempts the message is generally "Username/password combination not found." I find this very frustrating as I use multiple usernames and passwords across services and would like to know if the issue is simply I'm thinking of a different username, or if it's an old/different password. Is eliminating independent verification that the username was valid really needed to have a secure login system? So two questions: What do we need for passwords to be secure, what should we require; and, secondly, why doesn't it tell me which is wrong, username or password?

Steve: So, okay. My feeling is that I really like sort of what I would call the state of the art now, which is, as you're creating an account and for the first time defining your password, this page that you're typing it into is using JavaScript on the fly to look at your password, very much the way that my Password Haystacks page does, to rate the strength of your password. So the idea is it gives anyone who's creating a password a sort of a built-in tutorial. They can choose if they want to have a weak password. But if they do, then they're doing so deliberately, with foreknowledge of that.

And so my sense is I don't know that I like the idea, I mean, certainly maybe set a ridiculously low limit. You don't want a two-character password. So Dustin says how about greater than five with a number. So you could create whatever rules you want. The problem is users do chafe at specific rules. Certainly I hear from people all the time who are annoyed when things say they can't have a password longer than X. And that's, as we know, frightening because it implies that the password is being stored in plaintext in a limited-size field in a database somewhere because, if a password is being hashed, then it hashes to something always the same length, which is the bit length of the hash, regardless of how long the user's password is.

So for me, I like the idea of showing a meter where, as they're typing, and as they're using special characters and numbers and things, some JavaScript code is looking at the size of the alphabet that they have used so far times the length of the password that they have used, or actually raised to the power of, in order to give them a little bar graph, maybe change the color from red to orange to yellow to green, like how safe is the password that you've used? I like that because we're teaching at the same time, and we're giving them responsibility. We're not saying here's the requirements of anything that you type in here.

And the other thing, too, is that I've noticed, if you're going to have requirements, put them right there. Don't wait until the password the user types in and submits fails your requirements to tell them what your requirements are. If you're going to have some, let us know before you make us put one in that's not going to work the first time.

Leo: I know, I hate that.

Steve: Isn't that dumb?

Leo: It's so annoying. Oh, you didn't have - and almost everybody does this, by the way, Steve.

Steve: I know.

Leo: It's very common. Oh, you know, you should have a number in there. Well, tell me, for crying out loud. If you'd told me, I would have put a number in.

Steve: It's not like the bad guys aren't going to...

Leo: Even Apple does this. I think Apple does this. They say, oh, no, no, sorry, you have to have an uppercase letter. Well, if you'd just tell me ahead of time.

Steve: Yeah, then we'll do one.

Leo: But I do agree, we don't want to leak information about which of the two choices is wrong. I think that's a bad idea; right?

Steve: Oh, about Part 2 of his question.

Leo: Oh, you haven't got to that, yeah.

Steve: You're absolutely right. So he says in Part 2 he doesn't like the fact that, if you fill two fields in, typically email address and password or username/password, then submit them together, he doesn't like just getting a notification that something was wrong. He wants to be told, he's asking, is it less secure or worrisomely less secure to give the user more help?

Leo: Absolutely.

Steve: And I agree with you, yes, it is, because it allows one to be probed independently of the other. So that is absolute information disclosure which is not secure. I unfortunately, I mean, I understand the inconvenience. But Dustin, how are you not using one of the password managers like LastPass in order to solve the problem of multiple usernames and passwords on different sites? That's really the way to do it. So I understand he's doing it from the implementer's side now. The question is, I'm going to implement a system, what should I do? So he's asking can we tell them. It's like, eh, I don't think you should. And nobody else does. So, and there's a reason. It's not good because it allows you to probe one separately from the other.

Leo: Fortunately, that's something most sites do right.

Steve: Correct.

Leo: They don't come back and say, oh, your username's wrong, but your password's right.

Steve: Correct. And then lastly, by pure coincidence, I remembered three days ago somebody tweeted me a link, actually it's a devout listener to the podcast, on his rsum. He has as one of his self-certifications that he has listened to every Security Now! podcast twice.

Leo: It takes at least two times, frankly. It's like "The Newsroom." You've got to listen twice.

Steve: Yeah. So in this case, I just tweeted the link to it. He's a guy up in Canada. I can't quite remember the name now, .ca, although the link I tweeted is not his normal main website. But anyway, the point is that he has an absolutely beautifully assembled page of here's how you process and store users' passwords. So Dustin, go check my Twitter feed, Twitter.com/SGgrc, and not far back because I won't be tweeting much, I never do, you'll find a link to a page where I agree with everything there, actually because it's what I've said.

Leo: Is this the CrackStation page?

Steve: Yes.

Leo: CrackStation.net?

Steve: Yes. And because there he is a Security Now! listener, very technical. Actually his site and his home site, I poked around there for a while, lots of neat stuff. And he refers to the Personal Passwords Page and everything. But it is all the advice on one page with the password-based key derivation function, hashes, hash tables, rainbow tables, I mean, he just lays them all out. So in one page there is the advice for how to set up a secure password system using all the best practices that we know of.

Leo: And it's Defuse, Defuse.ca.

Steve: That's the site.

Leo: This is his business, I think. It looks like, anyway.

Steve: Looks like he's a good guy. And definitely...

Leo: He's a security guy, yeah.

Steve: Definitely a listener.

Leo: Yeah, I love that.

Steve: He's got our JavaScript, or zero JavaScript, menuing system, too, because his menus worked for me with no JavaScript. It's like, oh, that's always cool.

Leo: Oh, he's serious. He's serious about this. Article and code written by Defuse Cyber-Security. Moving on to our next question, which comes to us from the Netherlands. I like this one. And I'm going to butcher your name, so my apologies in advance: Anne Stellingwerf in Apeldoom, Netherlands - she's @AnneSt - tweeted this question about buffer bloat: What would be the effect of one CoDeling router in a chain of non-CoDeling routers? Does position - whether it's at home, the ISP, the Internet at large, or the destination - matter?

Steve: I loved the question because I forgot to explicitly address it when we talked about CoDeling our routers.

Leo: I guess it'd be germane because if your Internet service provider CoDeled, for instance, that would be protective; yes?

Steve: Well, here's the problem. It's a problem, and it's a good thing. What we really want is this beautiful CoDel active buffer management technology to be ubiquitous. We want it to be the way buffers - any buffer that exists is managed this way because the system doesn't have knobs and dials, doesn't need tuning. It's adaptive. It works across any speed of bandwidth, I mean, this is the answer to managing buffers. The problem is, even one unmanaged buffer somewhere can cause a problem. The problem is we want to minimize our delay. We want to minimize having an oversized buffer filled and being stuck full because then it means that all the packets going have to wait through this long queue, and the inherent rate-throttling technologies that we have and that work beautifully, they're not getting the signaling that they need for slowing down in order to manage the buffers. So technically even one non-CoDeled buffer somewhere between the two endpoints can cause a problem.

But practically, the good news is, the only big problem we have - remember the reason typically that you're going to have an overloaded buffer is it's at a pinch point. You are going from high bandwidth to low bandwidth. And where that happens most often is from a very high-speed local network which people have at home, through the pinch point of their ISP, out onto the Internet. Once you get on the Internet, you're dealing with

BigIron fast routers that are able to keep up with the bandwidth of their links, so you're not having buffer bloat problems there. Where the buffer bloat is occurring is at home. And that's the one router that you have control over.

So the answer is, yes, in theory, non-managed buffers anywhere can be a problem. But the need for management occurs only at the pinch point, where you go from high bandwidth to low bandwidth, because that's where you're going to get a backlog. And what you'd like then is that backlog to be minimized by having intelligent drops of packets that then signal the protocols to throttle themselves. That keeps everything interactive, and you don't really lose much bandwidth. And you have that at home. So there's hope, without needing the rest of the Internet to update itself.

Leo: Yeah. Or your router, to put spyware on it.

Steve: Yeah.

Leo: Oh, god.

Steve: Oh, god.

Leo: Preston, Silicon Valley, found a security vulnerability, but now what? Chief Explainer: First, to get it out of the way, listener since May 2008. Went back and got caught up. SpinRite owner. Favorite podcast of all time, yada yada yada.

Steve: Let me interrupt you for one second. Everybody starts off their posting.

Leo: They all say that.

Steve: And I have started to cut those out because I get a little embarrassed that, like, we're reading them endlessly every week. So I'm going to just - I don't want anyone to be offended if that gets cut out from their question.

Leo: We reserve the right to edit, just like a newspaper, for clarity and content.

Steve: We're happy to be told that we're doing a good job, and I appreciate that.

Leo: Rush Limbaugh asks his listeners to say "ditto." So we can just - you could just say "ditto."

Steve: And in fact, Preston's - this is already long, but it was a lot longer. And so I wrote, I already wrote to Preston and said, Preston, I really liked your question, I want to include it, and I'm paraphrasing it to keep the intent, so just -- because I don't like to edit people's stuff because they sent it to me as they wanted it to be sent. So anyway, okay. Continue. Sorry.

Leo: I have no compunctions about editing people's stuff. In late 2010 I downloaded a copy of Cain & Abel and was playing with it on my home network, implementing a man-in-the-middle attack on SSL, and I discovered that I could see my PayPal credentials in the clear. That night there was no sign of anyone else on the 'Net knowing of it. But by the next morning the news was out that others had seen it, too. I felt proud to have discovered something independently. But it raised the big question in my mind: What would I have done with that information if no one else had reported it?

Now, fast-forward to last month: I was at a conference on mobile banking where there was a talk given by Andrew Hoog, the CIO of viaForensics, a security firm specializing in mobile apps. He told a story of how they found a vulnerability in the PayPal app where all traffic was being sent securely, but the app wasn't checking the identity of the certificate to make sure it belonged to PayPal. We're sending it securely, we just don't know who to.

Steve: Yeah.

Leo: Thus a man-in-the-middle attack would be trivial. After his talk I asked him if this happened in late 2010, and he said it did. He said they found it about three weeks earlier, and he recounted the story that, even though viaForensics was an established security company, PayPal chose not to believe them at first and tried to ignore them. The only way to get them to look into it was to document it in step-by-step video.

If enterprises treat a known security company like this, I wondered what steps a little guy could take if they found something like this in the future. I suppose the white hat thing to do would be contact the company. And by the way, not necessarily a good idea, and I'll tell you why not.

Steve: Uh, no. Yup.

Leo: But what do you do if they don't listen? Just release it to the wild? Sell it on the black market? Do nothing and let someone else take the credit? No, no, and no. I'll let Steve answer this one. But I'm champing at the bit. Steve and Leo, I love the show, especially the series on how a computer works, and I look forward to each new show every week. Sincerely, Preston in Silicon Valley.

Steve: You go, Leo.

Leo: No, no, come on. You're baiting me now. Actually I do know people, there's a guy you probably all have heard of named Adrian Lamo, who considered himself a white hat hacker and broke into a number of places, including The New York Times, then offered up the information, saying look, you're insecure, I've found an insecurity, and he was arrested. Our friend Randal Schwartz of FLOSS Weekly claims he was doing the same thing. He was also arrested. So it's very, very risky.

Steve: Randal got arrested? Wow.

Leo: Randal has, yeah, Randal has a conviction, I believe. So this is a very risky thing to do. It is not a good idea, if you're not an established security firm, to just walk in the door of some company, say you've got a flaw here.

Steve: Yeah, unfortunately.

Leo: They may not take it lightly.

Steve: Yeah, what I would say is, the way I would summarize that is, unfortunately, many companies do not react the way we think that they should when they learn of a problem. They literally shoot the messenger, when that's not the mature thing to do and doesn't help them at all.

Leo: So what should you do?

Steve: Well, that's a great question. And I think the answer that I would have for Preston is, when he says what should one do, what I would do is I would contact, not the victim company, but contact a reputable security firm.

Leo: That's what I would suggest.

Steve: Yes, and tell them. You're losing the glory. You're not going to get any great prize anyway. If your motives are to be a bad guy, and you want to sell it on the black market, well, good luck. I don't know how to do that, but these things are valuable. We know that. But if you're a listener to the podcast, hopefully a white hat hacker, and you're playing with Cain & Abel or whatever, and you find a problem, I would say, yeah, turn it over to a legitimate security company. First of all, they'll verify it. And then they no doubt have established channels to large enterprises where they can say, hey. They're able to even say we didn't find this ourselves. This was found by somebody else, just a random user of the service.

Leo: Who shall remain nameless.

Steve: Yes, who wanted us to notify you because he wanted it to be taken seriously. I think that's the right protocol.

Leo: Just to complete the story so that people don't have to kind of some strange thought about this, Randal was working for Intel, did some pentesting at Intel. He was charged by the state of Oregon for compromising their security. Intel prosecuted. He was convicted on three felony counts with one reduced to a misdemeanor. But, and I'm very happy to say this for Randal, a few years ago his arrest and conviction records were sealed, expunged, and he is not a felon any longer, so he can vote and all of that. And he says this was his complete mistaken, you know, I was just doing pentesting for Intel.

Steve: I mean, I can't think of a nicer guy.

Leo: I know. Randal's a sweetie. Now, it's more complicated. He was doing pentesting in a system he no longer administered. It's a complicated story.

Steve: Look, it's a little gray, maybe.

Leo: It's a little gray. I don't think he was in any way hacking. Adrian, same story, where you might say he did break into The New York Times. He changed some stuff on their servers. Nevertheless, it is a risky thing to do to go to a company and say, hey, you've got a problem, I found it. But you go to a security firm and let them do it, and generally speaking they have channels. Not that they don't get ignored, as this guy did. I remember talking to Matt Conover at w00w00 Security. They found a significant bug with a major operating system's company, told them about it. For months the company never fixed it. This happens time and time again.

Steve: Oh, well, and how many times have we talked about people notifying Microsoft and being really frustrated that six months later they still haven't addressed something that they have found.

Leo: It was Microsoft.

Steve: And it is very frustrating.

Leo: And finally w00w00 released the - this is what often happens. These companies get frustrated. Six months in, they start seeing the exploit in the wild, and they say, look, we've got to release it now. And that's usually what forces the company to finally fix it. And it's why often - always be suspicious if there's a fix a week after you hear about an exploit.

Steve: Yes. Not the week before.

Leo: It usually means they've been working on it.

Steve: Not the week before.

Leo: The week after.

Steve: The week after.

Leo: It usually means they've been working on it. Rene Matthiassen, Copenhagen, Denmark - I love our international listenership, viewership - wonders about missing security frameworks for cloud computing: My question is, when everyone's talking about cloud this, cloud that, it's worrisome no one's talking about security frameworks to support best practices for cloud computing. Basically, all vendors or suppliers can pretty much do whatever they find fit for their purpose. There isn't any security standard in this area. Each time I ask vendors for cloud services about which security standard they are using, they either try to explain something ridiculous, or just look back and blush, "I got nothing." Is there something on its way? Or is this just the Wild West? Thanks for putting a good show together week after week. Rene, Copenhagen.

Steve: So it's absolutely the case that everybody's making this up as they go along. And what this question put me in mind of was something that I've always found interesting, Leo, and that is, this is always the way it's been. I don't know what attorney wrote the first software license agreement. But that first software license agreement said we have no responsibility, we the vendor, no responsibility whatsoever for what this software does or what you may do with it, how it behaves, how it behaves in the past, now, or in the future, and we're really not even sure where it came from, but you owe us money.

And that's the way all software agreements have always been. This amazing ability that our - I want to say "our industry" because I'm of course a software vendor. The software business has always been able to get away so far with taking no responsibility whatsoever for what its product does, which just strikes me, when I remember that fact, as remarkable. You know? Nobody else could do that. I mean, you've got consumer protection, and you've got all kinds of regulations, and...

Leo: But it's always after the fact, even in that space; right?

Steve: Yeah, and that is a very good point. It's one of the points, actually, that Paul Vixie brings up that we'll be talking about next week, is the way everything seems to be done afterwards, not beforehand. But it is just an odd thing about this industry. It seems to be powerful enough and confusing enough that no one really knows how to regulate it or control it. And it's moving so fast, I mean, the whole cloud thing has just sort of exploded. After being possible for a while, the incredible lack of cost in mass storage has allowed all of this. It's what enables storage to suddenly all move limitlessly to the cloud. And bandwidth. The explosion of bandwidth has allowed the data to get there and back. And suddenly we're dealing with a new model that we didn't have just a few years ago. So, yeah, it's all new again.

Leo: It's technology.

Steve: It's continuously new.

Leo: We just throw it up against the wall, see what sticks, fix it after the fact.

Steve: And we'll say we're sorry.

Leo: Exactly. Well, I think about Dropbox and the fact that we found out kind of later that they actually had the security keys, things like that. And it's just - there isn't a standard. I don't think you could really make a standard, reasonably, ahead of time.

Steve: One thing that we're doing on this podcast, by establishing things like TNO, Trust No One, and Pre-Internet Encryption, we're saying, although we're not part of any standards-making body, we're helping to raise the awareness of this is clearly the way these things should be done. We have no ability to compel people to do it. But on the other hand, when we look closely, as we have in our cloud computing series, what are these companies doing? Are they TNO or not? We're certainly helping to influence companies to, I mean, we're seeing the influence of our pressure.

Leo: And you did this before with ShieldsUP! where you effectively convinced router companies that the best way to behave was in stealth mode, which stood for something they didn't even - you coined the term.

Steve: Yeah, that was my word.

Leo: Yeah. So I think that that's appropriate. I mean, that's one of the ways this happens, which is watchdogs and people with an interest in this kind of at least propose, well, this is what we think should happen.

Steve: And point to instances where it's not happening.

Leo: Right. And then let the market decide. The market will tell you.

Steve: Yep.

Leo: I think this is not a broken system, but it is good to be aware of that's how technology works. And it's because it happens so fast. You don't want a governing - look how long standards take. You don't want a governing body setting standards before things happen. You want to try stuff.

Steve: And they'd so often be wrong.

Leo: And they could do it wrong. Look at WEP.

Steve: Yeah.

Leo: John Couzins, Blackpool, England wonders about password salting versus password strengthening: Hi, Leo and Steve. Big fan of the show, blah blah blah blah, bah blah blah blah blah blah. I'm currently - that's what I'll say from now on, not "ditto," just "blah blah blah." I'm currently in my last year of a Cyber Security Masters at Lancaster in U.K. I'm hoping to focus my efforts on securing virtual environments. Wow. Anyway, do you not feel that, while salt can be used to further secure hashed passwords, specific password hash algorithms like PBKDF2 would be more effective in preventing situations occurring like the LinkedIn breaches? John Couzins, Blackpool.

Steve: You know, I forgot we had this question. This must be the reason that I tweeted the link to the Defuse.ca guy's page because...

Leo: Yes, yes. That's about salting particularly, yeah.

Steve: Exactly, and the use of - so he's saying, yes, we have got salt. And in fact this is the same thing that the form, was it formworks, form...

Leo: Formspring, Formspring. You had me confused, too. Formspring.

Steve: Formspring, right. This is what they were doing is they were salting and using secure hashes.

Leo: They were doing it right; right?

Steve: Yes. But they were not going through a password-based key derivation function, this PBKDF2, which is to say doing it many times. It's one of the things, for example, that WPA got, the successor to WEP, which you just reminded us was so badly broken and poorly done. The WPA spec, remember, has a 4,096 iteration PBKDF2, where they take the user's password and the SSID, using the SSID as the hash, essentially, and iterate on that 4,096 times to create the final result. So John, yes, you essentially go to, again, Twitter.com/SGgrc, get that link, and there's the answer. That guy did a beautiful page that just lays it all out.

Leo: Jim Hartz in New Brunswick, New Jersey wonders and worries about a backdoor to Symantec's PGP Whole Disk Encryption: I use OS X Snow Leopard, he says, and utilize whole disk encryption via Symantec PGP. I have been told this implementation of PGP has government backdoors to decrypt data. Any insight as to is this so? And, if so, any recommendations on an alternative? Thanks for the great podcast and helping to keep my drives running with SpinRite. Can't wait for the next version. Backdoor in Symantec's PGP?

Steve: Yeah. I just had to say no. I mean, I don't...

Leo: It was open source. I don't know if it is still.

Steve: Yeah. I don't know either way. But it feels - of course we don't know who's told him this. He says, "I've been told this implementation of PGP has government backdoors." Doesn't that sound like something that some weenie posts on a forum somewhere?

Leo: Sounds like something Adam Curry would say.

Steve: Yeah, it just...

Leo: We don't know. It's an easy thing to say.

Steve: Yes. And I would be very surprised. But to answer your question, Jim, TrueCrypt.

Leo: There you go. Open source.

Steve: TrueCrypt, we know, is open source. It's cross-platform. Those guys have nailed it. I've lost track of what version it's at. It's at 6 or 7 or something. It solves the problem. So if you have any concern at all that there might be something funky going on, I absolutely wouldn't think so at all. To me that, "Oh, yeah, that has a backdoor," sounds like something you read where script-kiddies are posting nonsense on forums. It's like, okay. I see that kind of nonsense all the time. But TrueCrypt is your friend; and, end of story, they've nailed it.

Leo: TrueCrypt is your friend. But it's funny because you've come around. Because I've said for a long time the only encryption to trust is open source. It's the only way you can be absolutely sure. And I know that there's some commercial encryption technologies you've talked about in the past. But I think we're in agreement now. If it's not open source, you don't know. And I would say, for instance, one response to this would be, well, Apple's got full disk encryption, FileVault, you could use that. But again, you don't know, and no one can know, what's in there.

Steve: I guess what I like is sort of the hybrid, where someone - and I'm seeing this more and more - someone says we're selling a product that incorporates encryption, and we need this to be ours. But here's the protocol, and here's an open source implementation that demonstrates that this is what we're doing.

Leo: Yeah, but you could still have a backdoor tacked onto that open source implementation. I want to see all the code. I want to be, in fact, if you really care, you want to be able to take the code, look at it, then compile it and use that.

Steve: What that does say, then, is that you really can't do commercial crypto.

Leo: That's my feeling.

Steve: Which is to say that crypto has to just be given away. It has to not be where your value is added.

Leo: That's where I've always believed that. Let's move on. Patrick McAuley, Guelph, Ontario, Canada wonders about bandwidth and whether it's best to take the top measure. This is what you recommended last week, not take the average, but take the highest. That's the max you can get. He says he just listened to that: Responding to one question about checking your online speed, you said we should test our speed several times, then take the highest reading as our actual bandwidth. But I'm wondering, couldn't this be misleading for people who get to the Internet by a cable connection?

Here in Canada, I use Rogers Cable, and they advertise "SpeedBoost" as a benefit. Comcast in the U.S. has the same thing under a different name. That's absolutely true. The idea is that when you first connect to a site, for instance Netflix, they'll boost your speed well beyond your normal bandwidth for the first minute or two if that bandwidth is available. This is great to speed up the initial buffering on Netflix, but it can give a very misleading reading if you use a site like Speedtest.net to check your speed. If your ISP provides this feature, would you not be better off taking the average of several readings as a more accurate value for your bandwidth?

Steve: Well, okay. So here's the problem. We have a situation where our bandwidth is not constant. And the question then is what is it that we're trying to measure? Do we want to measure the SpeedBoost effect, or do we want to measure the post-SpeedBoost nominal speed? If we take the average, then we've sort of got neither of those. We've got some that was boosted, and so our number will be skewed high from the average. So I guess I don't know what to suggest except to be aware of what's going on. Maybe, if there's any way to look at the speed initially and separately after SpeedBoost has been removed? I guess sort of...

Leo: The SpeedBoost after the first couple of minutes doesn't do anything.

Steve: Perfect.

Leo: It settles down.

Steve: Perfect. In which case you'll have to be extra clever. The reason I said you want to take the highest measure over several different tests, and you would still want to do that, even if you have SpeedBoost, is that arguably your bandwidth is the best that your line, that your connection can deliver, rather than its current performance, which may be weighted down. Like I noticed, like, my cable modem slows down when people start getting home from work, for example, in a residential area, because they turn their computers on, and they start doing whatever they want to do. So it certainly depends upon time of day and the nature of your connection. A DSL connection probably doesn't have that same characteristic.

So if you care about this, get to know by doing lots of tests, and you'll begin to see patterns, and you'll understand. But keep in mind that you probably want to think in terms of, at any given time, what is the highest you can get in those circumstances because I think that's your real bandwidth, your actual bandwidth.

Leo: Yeah, it's really two numbers. If you have SpeedBoost, it's two numbers. It's what that SpeedBoost peak is, and then what your sustained throughput is. And it's good to know both. I mean, SpeedBoost is valuable. As he says, it fills the buffers fast. If you're just doing web pages, it makes web pages pop up. In the Comcast implementation, it's the first 25MB. Well, that's going to be plenty for a web page to load very quickly.

Matt's sentiments from Auburn, Washington were echoed by so many listeners: Steve, I know this is a heated topic, but since everyone else is giving you their opinion, I wanted to, as well. For anyone who complains that episodes are too long, why don't they just hit the Stop button? Those of us who want to hear more, but can't because there is no more, don't have an option. It's sad every time you have to stop before finishing your questions, or can't go into as much depth as you want to. Believe me, tens of thousands of people listen to you because you have that depth to go into, which we can't find anywhere else. So I say 'tis better to have more, and let people stop when they want to, than not to have enough. I can't begin to understand why people would spend the time to write you to shorten your podcast when the Pause button is right there. Thanks for listening, and keep on talking. Matt.

Steve: So I just wanted to acknowledge all the people that have written. This was one question or statement from among so many that I found in the mailbag when we were discussing this. So I just wanted to thank everybody. And I think Matt's probably right. I think we found about the right formula. You and I, Leo, nominally have two hours. We screw around and talk a little bit and get recording maybe about 20 minutes in. And so we're generally - and then typically I sort of pace the things. I've got my eye on the clock. We've got 10 minutes to go right now, and we've got two questions left, so we're right on target for a greater than 90-minute podcast. It's funny, too, because some people have said, "I remember when those were 30 minutes." And it's like...

Leo: They were, briefly, very briefly. I don't actually want to say it that way, as the owner of this network. Let me say something a little different. I do appreciate the feedback about podcast length. We always are paying attention to what people tell us, and he of course has the right point. You could listen to less. But I don't think people are saying that. I'm thinking they're saying, not that they want to cut you off or that they want you to be less than thorough, but that they don't need the podcast to be that long or whatever, and I listen to that. Whether you listen or not is another matter. But I listen to it, and in fact it is too long right now because I'd like to get these done a little quicker. And there's a number of reasons. One is we have a schedule. The other is I'd like to eat lunch before TWiG. But also, there's also the issue of, well, how much material do you want to put in a podcast? How much content do you really need in a podcast? I don't ever, and we never will, want to shorten stuff as broadcast media does just because it's got to be six minutes. The topic should go as long as it needs to go. That's absolutely the case.

Steve: Yay.

Leo: But then there's other issues, as well. And I certainly don't, believe me, I love to hear from people. And if it's your opinion it's too long, I will listen to it, absolutely, as well as his opinion, that it's not long enough or whatever, or it's just right, or hit the Pause button if you don't like it.

Anthony in Melbourne, Australia shocked Steve with this news: Steve, on SN-358 a listener was unimpressed with Microsoft's recommendation to close down all browser windows to clear all logon sessions, et cetera. It's kind of surprising. This may be true for Internet Explorer, but ever since Firefox 4, all sessions including SSL are saved. Oh, I didn't know that.

Steve: I didn't either.

Leo: Try it for yourself. Close down Firefox, then reopen it. Hit History and click "Restore previous session." You should now be logged in to all your previous site sessions. What?

Steve: Yes.

Leo: I had a difficult time finding out how to disable this, and eventually came across a page on MozillaZine. It's a long URL. Actually, if you search for "browser sessionstore privacy level" in MozillaZine's knowledge base, that should probably be sufficient. I hope you can mention this to Security Now! listeners.

Steve: Okay, now, I was very surprised.

Leo: Yeah, wow.

Steve: What we're talking about, and we've discussed this many times, are session cookies. When you log onto a facility, you are given a cookie. Hopefully this has been done over SSL, and the cookie is flagged with a secure flag, so it will never be transmitted unless you have an SSL connection. Your browser says before it adds the cookie to its query headers, is this secure? And if the cookie is flagged secure, it will not include that cookie unless it's going to the intended domain that the cookie is set for, and the connection is secure. That guarantees that men in the middle, nobody sniffing or snooping can see what the cookie is because, once you've logged in, that is your token that keeps you logged in as you move through the site, as you post, as you browse, as you do whatever. You keep reasserting your authentication to the server because, as we know, web-based surfing is sort of event-based. It's individual queries and replies.

All of this means - it's called a "session cookie" because, when your session is over, it's gone. And it's always been the case that it's not stored on the hard disk. It's kept in RAM as the session. And when you close the window, when you close the browser, that's it. It turns out only IE honors that. What happened, apparently, when they went from Firefox 3.6, which is where that ended, into this new era that began with 4 and has rapidly shot to 13.0.1, which is where we are now, they deliberately changed that.

Now, I immediately changed it back. I just don't like that. And I proved it to myself. I have a way of using session cookies on GRC where I assumed that shutting the browser down lost the session cookie. So I logged in with a session cookie. And, I mean, this is my code. I know what the cookie is. I can see it. And I shut down Firefox, fired it back up, and it still authenticated me. Which is like, whoa. Not the way it's always been. IE forgot me. I did the same thing on Internet Explorer, shut it down, came back up, relaunched it, it said I have no idea who you are. And Google remembered me also.

So I can see where this limits customer service complaints and so forth, where it's like, okay, this will just be easier for users. And it's one thing if you click the checkbox, like eBay has "Keep me logged in for the day" or whatever. And many sites allow you to manually say I want to stay logged in. Normally that checkbox is off by default. But what this means is you're staying logged in anyway.

So we all know, or long-time Firefox users know, in the URL bar where you normally type in http://, so forth, you can put "about:config," hit Enter, and that takes you to an amazing depth of optional configuration stuff. And there's a search bar in there on that page which you need. If you type "sessionstore," all one word, into the about:config page of Firefox, you'll still then see, I don't know, maybe 20 items. One of them there is "privacy_level." And I think I recall it defaults to zero. You need to change it to 2. I have. When you do, then Firefox behaves the way I think it should, which is closing it actually does cause it to release all of its session cookies, the way IE still works, but no longer the way Firefox or Chrome work, which really did catch me by surprise.

Leo: Yeah, because as you say, it's a session cookie. It should be only for a session.

Steve: Yeah. That's the way it was designed.

Leo: I mean, that's the expectation, yeah.

Steve: These guys decided differently.

Leo: I understand why they did it, because maybe people want to not have to log in again.

Steve: Well, actually I followed back, I backtracked why this happened. It's because of crashing. It used to crash, Firefox would crash, and people...

Leo: Ah, of course. So you restore your session after a crash. That's it.

Steve: Yup.

Leo: You're right. I get it.

Steve: Yup. And unfortunately it also restores it after a graceful shutdown, which I don't think it should.

Leo: Yeah, you could change that. You could say, hey, a shutdown erases that, doesn't save it.

Steve: Yeah. There is an option, actually, among those settings, for doing that, where a crash will still restore it, but a shutdown won't.

Leo: So that should be the default. Randy Hammock, KC6HUR, in Sun Valley, has our last question and our MacBook Pro Camera Tip of the Week. Do you tape over your cameras on your laptops?

Steve: I don't think I have any cameras on my laptops. They're old.

Leo: Another reason to go with old.

Steve: Right.

Leo: Regarding placing a sticker over the camera for privacy causing the light sensor not to function for keyboard backlight and screen brightness control, not true. Did we say it was?

Steve: Yeah, we did. Or a listener...

Leo: We were questioning whether it did.

Steve: A listener did, yes.

Leo: I discovered the light sensor is located in the place where the green camera active LED is. If I place my finger over the camera, nothing happens. If I place my finger over the LED holes - and by the way, this is specific, he says, to his MacBook Pro. It's probably different for different computers - the keyboard lights come on and the screen dims. Older MacBook Pros had the light sensor in the speaker grills, both of them. If you place a hand over both speaker grills, not just one, keyboard lights come on, and the screen dims. So go ahead, cover the camera for privacy, and you'll retain keyboard and screen auto light control. Thought your listeners would find this useful. Randy in Sun Valley.

Steve: And I do because cameras spying on people have been a recurring problem that we keep covering. Spyware turns cameras on. Even babysitting software that schools use, as we've extensively covered, turns the cameras on and spies on their students without their knowledge. So I really endorse the idea of just taking a little square of the sticky part of a Post-it note, a 3M Post-it note, and just stick it over the camera. If it's not something you use all the time, just cover it up because that seems like it's simple, and it's a physical shutter. And now you know, do not cover the little green light because you'd like your light sensor to still work. And then you've got a solution. Old school.

Leo: [Chuckling] Steve Gibson, he is old school. He's the definition of old school.

Steve: Yeah.

Leo: XP, BlackBerry, PDP-8s. You can hear this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1800 UTC, if you want to listen live. We'd love it if you do because I pay attention to the chatroom and all of that. And so it's a great kind of feedback mechanism.

Steve: And actually, Leo, there is 20 minutes of fun that our regular podcast listeners don't get, unfortunately.

Leo: Yeah. Like, for instance, I try to keep the diet information out of the show. We do that, we talk about our diets before the show.

Steve: Whether you're floating on the surface or not.

Leo: Exactly [laughing]. You can get this...

[Talking simultaneously]

Leo: Yes, exactly. You can get this show, not that part, but you get the rest of it on demand, after the fact, via our website or Steve's. Now, Steve has an unusual version. He has a 16Kb audio version for people with severe bandwidth impairment, or who are just cheapskates. You can also get a transcript. And we hear lots - you just talked about somebody who listens twice. You know what, you could listen once and read the transcript. That would be a good way to do it, too. The transcript is a great way to kind of follow along. All that's at his site, GRC.com, along with SpinRite, the world's best hard drive and maintenance utility, all the freebies he gives away all the time, GRC.com. And if you want to ask a question for our next Q&A episode, there's a feedback form there you should use. It's GRC.com/feedback. Steve is on the Twitter, @SGgrc. He's also got a feed for the very low carb contingent, @SGvlc. Steve, thank you so much. Always a pleasure.

Steve: It is always a pleasure. And we're going to have a great podcast next week with news from Paul Vixie and DNSChanger and the non-event. But I read what he wrote, and it was so good, I'm going to share it with our listeners. Then we'll discuss it.

Leo: I want to hear his defense of what I thought was an indefensible action on the part of the FBI. But if Paul Vixie, the father of DNS, says it's okay, well, that's different.

Steve: I don't think that's really where, I mean, he was called in because he was someone with such a reputation, and the FBI wanted to make sure it was done right. And he did help them get it done right. So we're going to have a great podcast next week, and I always enjoy this.

Leo: Thank you, Steven. Thank you all for joining us. We'll see you next week on Security Now!.