Listener Feedback #71

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-207.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-207-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Music and Spinner.com, where you can get free MP3s, exclusive interviews, and more.

This is Security Now! with Steve Gibson, Episode 207 for July 30, 2009: Listener Feedback #71. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show that covers all things security. Steve Gibson is here, of GRC.com, our security guru, man who discovered spyware, coined the term spyware, writes all those great security tools and of course is the creator of SpinRite, a fantastic hard drive maintenance utility that is a must-have. Hey, Steve. A good day to you.

Steve Gibson: Hey, Leo. Great to be with you again. Episode 207. This is the one before the last one of our fourth year.

Leo: Our penultimate episode of the third year.

Steve: What? No. No. We're nearing the end of the fourth year. So...

Leo: Yeah. So penultimate episode of the fourth year.

Steve: Yes.

Leo: Wow.

Steve: Yes.

Leo: Holy camoly. Wow, that's great. Well, congratulations on four years.

Steve: Here, as I'm going through the mailbag, as I did for today's Q&A, so many people appreciate the fact that we're turning these out as reliably as we are. I mean, they absolutely - they know we will go through any means necessary so that there's always a Security Now!, new Security Now! episode every week. And so far we're batting a thousand.

Leo: And credit to you, because it certainly isn't me. I miss episodes of shows all the time. No big deal. But today we've got a good one. We're going to catch up because last week, where we normally do Q&A, we didn't. So we've got a bunch of questions and answers.

Steve: And a bunch of errata, really just a whole bunch of interesting stuff I know that our listeners are going to get a kick out of.

Leo: Well, let's get underway.

Steve: Plow right in. Well, first of all, you had news about the iPhone texting exploit that we talked about last week.

Leo: Yes, indeed. You know, this is - they call him Safari Charlie. Charlie Miller has made his name cracking OS X. Twice now he's won laptops in the PWN to OWN competition by finding exploits nobody knew about in OS X, and certainly that weren't patched. So he claims he's found and will reveal on Thursday - so as you hear this, he may even be revealing it right now...

Steve: Turn off your phone.

Leo: ...at the Black Hat conference, a technique, yeah. Essentially, and one question that we had last week is, you know, he had said originally it affects 2.2.1. He didn't say exactly it affects the latest version, 3.0; but he did say it affects all iPhones, which tells me it does in fact affect all iPhones. He can send out a series of invisible SMS messages in his hack, ending with one that has a single square character. And at that point he has absolute control of your phone. He can make phone calls. He can make money by sending text messages to premium services which will then get in your bill.

Steve: He can turn on the camera or the microphone.

Leo: He's got complete control.

Steve: See where the phone is. He can read out your GPS to find out where the phone is located.

Leo: And the real scary thing is that no word from Apple on a patch.

Steve: No.

Leo: They don't have a whole lot of time left. You know, so Apple, please. And one of the things Charlie says is if you get a text message with a square in it, turn off your phone right now. That's the only fix. He said somebody could pretty quickly take over every iPhone in the world with this patch. The other point that he made which is kind of sad is that he's told Apple about this a long time ago. He says, "I've given them more time to patch this than I've ever given a company to patch a bug." So...

Steve: Well, and also the fact that they did the v3 rollout, knowing that this was a problem, and didn't fix it for v3.

Leo: It's very scary, very frustrating.

Steve: Yeah. And so what's the status on pushing versus pulling these patches?

Leo: You know, I didn't find out. I've never had a pushed patch. It's always been pulled. So...

Steve: You have to go get it and update it.

Leo: ...that means you have to go to iTunes, yeah, you have to go to iTunes and synch. And iTunes will say there's a patch, and then you have to accept it, and you have to install it.

Steve: Well, so what we can do for our iPhone-using listeners is just put them on alert that there's big news happening Thursday. It's not clear whether there will be clear details about how to exploit this. That is to say, it's not as if, when this is revealed, suddenly there will be exploits. But enough has leaked out already that other people have good clues about where this problem lies. So again, be on alert for updates from Apple and apply this ASAP.

Leo: Incidentally, at the same talk they're going to reveal a vulnerability in Windows Mobile SMS. So it sounds like SMS is a vector for attack and not, because it's such an old technology, not very well defended in any platform.

Steve: Well, it's hard to excuse it, really. I mean, I would say it's a simple technology. I mean, it's just text records of 160 characters maximum. I mean, it's trivial. And so, I mean, but the vulnerability is what it always is, which is you've got a communications buffer which is receiving data, and obviously there's parsing problems with displaying characters and fonts or who knows what their boundary conditions are that are being exercised. But you have a device that's connected to the Internet, or in this case the telephone system, and it's able to receive something from somebody else that is able to exploit defects in the reception code.

Leo: He discovered the Windows Mobile flaw on Monday, so it's not like Microsoft's had any time to respond to that one. That doesn't sound as serious, either. That's scary.

Steve: Well, we do have an interesting, out-of-cycle update from Microsoft. By the time our listeners hear this on Thursday, the Tuesday update, which is the fourth Tuesday of the month - we normally have Microsoft patches, as I'm sure all of our listeners know, on the second Tuesday of the month. And I made the comment last week that, due to the fact that the month began on Wednesday, this was the latest second Tuesday of the month possible. Now we're at the fourth Tuesday of the month, and Microsoft has just released two critical patches.

Essentially what - and this is the first time we've run across this. There's a patch to Internet Explorer, but almost more significantly is a patch to the Visual Studio tool set which is used for creating ActiveX controls. What happened is, it turns out for quite a while there has been a bug in the so-called Active Template Library, ATL, which is one of the toolkits used in Visual Studio for producing ActiveX controls, which in turn are invokable by Internet Explorer. The flaw in ATL, the Active Template Library, allows for kill bits to be ignored in ActiveX controls.

We've talked about kill bits often because this is the bit which can be set which prevents an ActiveX control from being invoked by Internet Explorer. I was lamenting last week that Microsoft didn't default them to being disabled and then explicitly enabled when you knew that it was a control that should be, that made sense to be invokable by Internet Explorer. Instead, dumbly, I mean, from a security standpoint, Microsoft has them all enabled by default, and so you kill them individually once you discover that they can be exploited. I mean, it's just completely backwards.

But what's worse is that the toolkit from Microsoft has a flaw, meaning that all ActiveX controls that anyone has ever written using this flawed library contains the flaw, which now people have found a way to exploit. Meaning that it's a way, after you turn on the kill bit, saying whoops, we found a vulnerability in this control, use the kill bit to prevent Internet Explorer from being able to invoke it, meaning that a website you visit is able to exploit you through that channel, now there's a way to ignore the kill bit because of the flaw in the Active Template Libraries. So these two updates, MS09-034 and 035 got added, technically added to the second Tuesday of the month updates. I think they went from, like, 21 through 33 or something through 33. Now they've added 34 and 35. So they're doing it as an update to this month's patch batch.

The first one is an update to IE that you definitely want to do because what that does is that prevents this flaw in the ATL from being exploited. So by fixing Internet Explorer, what they've done is they've updated IE so that it renders these bugs non-problematical, even when you've got ActiveX controls that were built with a flawed ATL, the Active Template Library. And 035 fixes the Active Template Library to remove the problem, even though Internet Explorer, once patched, will no longer allow that problem to be exploited. So I'm seeing a little yellow shield down in my tray which has been there for a day or two. I've not yet installed these because I'm not using IE for anything other than getting itself patched. So basically that's sort of strange. You use your browser only to patch itself.

Leo: Well, and other parts of Windows.

Steve: But that's what I'm doing. So I imagine that our listeners will have seen that. Reboot may be necessary after installing this. So find a time to do it, but do it because it will help keep you safe on the 'Net. And Microsoft has that new weird Exploitability Index indicator, and they're calling this "Exploit Code Likely: Functional code execution is easy and reliable to create." So...

Leo: Oh, geez. It's nice of them to tell us. It's easy.

Steve: Yeah. Just to let you know, it's probably going to be a good thing to patch.

Leo: Geez. Easy and reliable. That's something that Microsoft might want to shoot for.

Steve: Easy and reliable. Wouldn't it be nice if it was just easy and reliable to use Windows, instead of rating the malware as easy and reliable to create.

Leo: I think they're going to change that pretty quick.

Steve: Yeah.

Leo: I don't think that language is right.

Steve: Literally the verbiage on their security page.

Leo: They're going to have to fix that, I think.

Steve: Also I just wanted to note that Windows 7 was RTM, was Released to Manufacturing.

Leo: Yes.

Steve: The Final Release Candidate is still available for free download, and you can get a key.

Leo: You won't get the RTM version, though.

Steve: No. They're not making the RTM version available except to their so-called "partners," you know, people like Dell and HP and so forth, who need to have it in order to begin making sure that they're going to be integrating it into their product flow. End-users, though, I wanted to mention, can get the release candidate, which is free, and the security key. We're expecting Windows 7 to be released in October. But for me, at least, we know I'll be waiting until October of 2010 because, much as it is nice, it's new. And new means bad. So I know that there are people who are jumping on it. Lots of people are excited. But even so, it's not something I'm going to be jumping on because we'll wait for it to settle down.

So Adobe is back in trouble once again, in a couple ways. There is a critical vulnerability, and this is unpatched, a critical vulnerability in the current versions of Flash Player, v9, which, well, yeah, Flash Player v9 and v10, for Windows, Mac, and Linux operating systems. There's a vulnerable DLL that's the offplay.dll component, which is in Reader and Acrobat for Windows, Macintosh, and UNIX. It definitely can be used to cause a crash, and potentially allows an attacker to take control of affected systems. There are no patches available. Adobe has said they're going to try to get something out by this week, by the end of this week, so like the end of the July-ish. So keep an eye on Reader and Flash and Acrobat for updates. Maybe have it checked.

Adobe also came under some fire for the downloadable most recent version of their Reader not being the patched one. That is, it turns out they have an official protocol for the single-dot versions to be available for download. But the two-dot versions, for example, 9.0 or 9.1 will be what you can download. But if there's a 9.1.1 or 9.1.2, as is the case now, where there are vulnerabilities fixed in the two-dot, what you're downloading is still 9.1. And you must then update its security after downloading it. They're not making the fixed one the one that you download. And so they're under some heat for that. I wouldn't be surprised if they changed that policy since it means that you then need to wait for the player to update.

I think probably all of our listeners are security-conscious enough that when they install something like this, they immediately go under the Help menu and check for updates. And they'll find, oh, look, there are some, from the thing I just freshly downloaded. But the security community is upset that Adobe by policy is making a known vulnerable version downloadable from their site.

Leo: It should check immediately and update immediately, automatically.

Steve: Yes, and it doesn't.

Leo: Yeah, that's just weird.

Steve: Also in security news, Network Solutions, you probably heard, Leo, had a massive credit card breach. More than half a million debit and credit card accounts, by their count 573,000 credit and debit card accounts over a three-month period, from about middle of March, March 12th through the beginning of June, were exposed. It was - Network Solutions found malware on the eCommerce hosting servers...

Leo: Inexcusable.

Steve: I know, that 4,343 hosted customers are using for their merchant and eCommerce websites. These are typically, you know, your smaller mom-and-pop stores where it's just like, oh, yeah, set me up with eCommerce, one-click eCommerce, and I'll pay my monthly fee, and that'll get me a shopping cart, and I can sell things. Well, unfortunately, malware has been there for three months recording every credit card transaction which these 4,343 customers have transacted. Obviously this has been fixed now.

There's no clear widespread agreement from a legal standpoint on the reporting of this kind of breach. I think about 43 states have some legislation which requires in the event of a breach like this that the people who are potential targets all be notified. So Network Solutions has said on behalf of their 4,343 customers, their hosting customers, that they will take responsibility for notifying all of these 573,000-plus clients. And they're making free TransUnion credit monitoring available for 12 months to allow the potential victims of this to keep an eye on their credit because of course this is potentially a serious privacy breach.

Now, there has not been any indication that the cards have been used. It may very well be that they're in a pool waiting to be sold; they haven't actually been put into play at this point. So, I mean, upon receiving a notification, if I were one of those 573,000 people, I'd call my credit card company and say, okay, we need to kill this card and change my number and issue me a new card, so that you avoid that. Although, at least in the case of credit cards, not so for debit cards, you're indemnified against that.

So that's good. And then in just recent breaking news it turns out that v9 of BIND, which as we know is the major DNS server on the Internet, it's just news happening today, on the 29th, it's been - ISC, the author and publisher and maintainer of BIND, have said that there is a way to crash master servers, master DNS servers running BIND v9. There are fixes available. Updates are available. So anybody who's responsible who has a master, not a slave, DNS server on the 'Net may want to update to the latest one. Essentially it involves an exploit that's been found in the so-called Dynamic Update Messages that the server can receive. For example, in GRC's configuration, I have a master server which is private, and I've got packet filters which prevent there from being any public access to it. So even though I'm using v9, I'm safe.

Leo: Of course if they're using BIND, Level 3, you know, your hosting service is using BIND, then you're not safe.

Steve: No, I am because - and they are using BIND. But they're...

Leo: Or unpatched BIND, I should say.

Steve: Yeah, but they're running slave servers. That is, their servers are slaves of mine. So that periodically they, being a slave, check in with my server.

Leo: Ah, so they're not the canonical servers; you are.

Steve: Exactly. So they periodically check in with me for any updates.

Leo: That's probably what we should do. Because that's what happened to us yesterday.

Steve: And it's very convenient because it means that when I make a change, I'm able to push it to them instantly. I'm able to send them a dynamic update message, and they immediately update themselves.

Leo: And because you're not publicly visible, you're not hackable.

Steve: Exactly.

Leo: That's a good - we should probably implement that because I believe, you know, our domain name servers at SoftLayer were brought down yesterday, I think, and really took us off the air. Not only, I mean, all the servers were running. If you knew the IP address, you could get there. But if you didn't, the DNS didn't work. And that just doesn't mean you couldn't get to TWiT or my blog. You couldn't get the podcasts, either. So iTunes got confused because iTunes can't see where the feeds are coming from. So that's something we have to address, as well. SoftLayer, by the way, this affected a lot of sites.

Steve: Yeah, well, everybody who is hosted by them.

Leo: And Bear is telling me, our sysadmin is telling me that's part of what happened yesterday was this BIND flaw.

Steve: Ah, okay. Well, I need to tell our listeners about something else which is really disturbing. This was reported recently in CNET News. And that is, Buy.com and Orbitz and other commercial sites have been linked to what they're calling "controversial marketers." And I would say it's even worse than that. Reading from the CNET report, which is probably the easiest thing for me to do, it says: "Thousands of web shoppers have complained that 'mystery charges' are showing up on their credit card statements."

Leo: Oh, boy.

Steve: "And have accused those who operate so-called 'web loyalty' programs of duping them into signing up. As a result, the U.S. Senate Commerce Committee is investigating Vertrue, V-e-r-t-r-u-e, WebLoyalty, and Affinion, companies who make 'cash back' and coupon offers to consumers and charge those who enroll in their loyalty programs."

But here's what got me about this, Leo. This is what stopped me cold, was that when you're, for example, at Buy.com, and you're moving through the purchasing process, at one point you get to an intercept page that says "Big $10 Off Coupon," and they're asking for an email address. And that stops you from completing your purchase with Buy.com. Many users just think, okay, well, what is this? And they look at it, and it's like, okay. Then they'll, like, put in a scrap or a spare or a throwaway email account just to get on with the purchase. What they've done is to agree to this program. And literally in the fine print it says that they will be charged for this service. Now, the user may think, oh, that's not a problem because I'm not giving them my credit card information. It turns out that this is a behind-the-scenes deal with companies like Buy.com that provide your eCommerce credit card information to this third party without any additional permission. And in Buy.com...

Leo: Oh. Oh.

Steve: Yes.

Leo: That's my credit card. You mean they don't ask ahead of time? They don't say do you mind if we share your credit card number with a third party?

Steve: Down in the Buy-com privacy statement...

Leo: I'm not buying anything from them anymore.

Steve: I know. It says, "We reserve the right to use or disclose your personally identifiable information for business reasons in whatever manner desired."

Leo: But credit card? Your credit?

Steve: Yes. It says, "If you think that anyone who unwittingly signs up to one of these programs must be an eCommerce rookie and that it couldn't happen to someone as savvy as you, take care that your overconfidence doesn't cost you. Josh Lowensohn, a 26-year-old CNET reporter and longtime Web shopper, this week found that a credit card he rarely uses was billed $12 in each of the past eight months by WebLoyalty."

Leo: Oh, I've got to look at my cards. Oh.

Steve: "Last November, after almost completing a purchase at Buy.com, Lowensohn was presented with an advertisement that asked him for his email address." And they show a sample of this on the CNET page. "He couldn't quickly find a way to get past the page and said he remembers thinking he would type in one of his rarely used email addresses just so he could complete his transaction. Lowensohn was confident he couldn't lose anything because the advertiser didn't have his credit card information. But WebLoyalty didn't need Lowensohn to charge his credit card. WebLoyalty CEO Rick Fernandes said Buy.com - for a fee - enabled his company to charge Lowensohn directly."

Leo: This is appalling.

Steve: It's phenomenal. And so the next subheading is "Web Loyalty to Whom?" "A 10-minute Google search turns up thousands of stories similar to Lowensohn's. Apparently, many consumers are unaware that for years now, e-tailers such as Buy.com, Orbitz, Fandango, and hundreds of others have given web loyalty programs, also known as post-transaction marketers, access to their customers' credit cards. Some online shoppers don't realize that when they enter their email addresses into these ads, they are opting into the programs and authorizing the charges."

Leo: Unbelievable. Shocking.

Steve: "Jeff Wisot, Buy.com exec, was quoted as saying, 'We have a longstanding relationship with WebLoyalty because we think they provide value to our customers.'"

Well, what's happening is, WebLoyalty is paying Buy.com behind the scenes for credit card information from people who purchase from Buy.com.

Leo: Wow. Wow.

Steve: So I just wanted to...

Leo: I want a list of all the retailers, etailers doing this so that I can not use them.

Steve: I know. I know. I wanted to get...

Leo: I'm stunned that they - I can see, you know, when I hear "personal information," I think email address. I don't think my credit card information.

Steve: Yup. And so people are finding charges on their cards, monthly charges being made from companies they never directly gave the information to.

Leo: And what are these charges for? What am I getting?

Steve: It's some sort of, like, coupon offers. And then you start getting email spam from these people.

Leo: And they charge me for this.

Steve: Yes.

Leo: So, holy cow. And they don't say they're going to charge you. I mean, this seems like it's borderline illegal.

Steve: I'll send you the link, Leo, to the story, which you'll want to put in the Twitter feed and all so...

Leo: I will. I'm going to tell everybody about this one. This is appalling.

Steve: Yeah, it's a long story with lots of information. So...

Leo: This is on CNET, huh?

Steve: Several pages on CNET.

Leo: Thank you, CNET, for bringing this up. I'm going to talk about it on the - in fact, let's get you on the radio show this weekend to talk about it.

Steve: That's a good idea because...

Leo: Shocking.

Steve: ...it's a huge, much too broad a brush.

Leo: Unbelievable. Yeah.

Steve: In fact, try Googling "Buy.com, Orbitz linked to controversial marketers."

Leo: Geez, Louise.

Steve: See if it comes up.

Leo: I haven't used either of those in a while. But I have to think that many others are doing this.

Steve: I've used Buy.com in the past.

Leo: Yeah, in the past I have, yeah. Oh, my goodness. Well, that's kind of shocking.

Steve: Yes, in fact, if you put into Google "Buy.com, Orbitz linked to controversial marketers"...

Leo: Yeah, no, I found it, yeah.

Steve: ...which is the title of the story, it comes right up.

Leo: Wow. That's a shocker. Thank you, Steve, for bringing that one to our attention. Hmm. Orbitz has some comments on here, it sounds like. I'll have to look, scroll down and see. Greg Sandoval is good. He's a smart guy, so, wow.

Steve: Yeah. So that's our security news.

Leo: There's one more, I just want to warn you. This just crossed the wire, literally, from Wired News. And thanks, Virgil, for posting this in our chatroom. Two noted security professionals - you know, this week is the Halloween of security because of Black Hat coming up; right? Black Hat and DEFCON right after it.

Steve: That's actually a good way of putting it, the Halloween of security.

Leo: This is when the pranks begin. Two noted security professionals were targeted this week by hackers who broke into their web pages, stole personal data, and posted it online on the eve of the Black Hat security conference. Dan Kaminsky was one of them.

Steve: Whoops.

Leo: Kevin Mitnick the other.

Steve: Ooh, goodness.

Leo: They say, the intruders say they were hacked because they considered them to

be poseurs who hype themselves and do little to increase security. I disagree, at least in the case of Kaminsky. I mean, he's been really, really great, most recently on this DNS hole. But I have to say, maybe he needs to look at locking his site down. Holy cow. Anyway, I just thought you might want to know that security researchers are being targeted by Black Hat, ahead of Black Hat, to kind of bring attention to it, I guess.

Steve: That is interesting, indeed.

Leo: Holy cow. Mitnick says it's his webhost, and I'm moving.

Steve: Yeah.

Leo: Geez, Louise.

Steve: I had a little bit of sci-fi news. While reading through the mailbag I ran across a note from Scott in Glasgow, Scotland, who wrote. He said, "Hi, Steve. I'm a regular listener of Security Now!, love it. You and Leo are fab. I really also like your sci-fi reviews and had this one to share with you: "Torchwood: Children of Earth," produced by the BBC as a five-part miniseries, a spinoff from the main TV series, "Torchwood." In my opinion, this five hours of sci-fi is the best production to come from the U.K. in the last 20 years. Take a look. Hopefully you will find yourself recommending it on the show. Keep up the good work. Scott. P.S.: Show aired in the U.K. on five consecutive nights starting on the 6th of July."

Well, I could not agree with Scott more. I watched it last week when it was airing on BBC America, and it was spectacular. It's available already on DVD. Mine's on the way to me. I would say that, if you're not a "Torchwood" fan, it's probably a little difficult to get into it. But...

Leo: You know, I started watching, like, in the middle of the season. So I'm going to go back to the beginning. I hear it's very good.

Steve: Yeah. And, I mean, "Torchwood" is really fun also. They had two seasons, both available now on Blu-Ray DVD, and "Children of Earth" is essentially a follow-up to the first two seasons of "Torchwood." I really would recommend that you see the original series first to understand the back story. But "Children of Earth" was - it was really good. I mean, it was just - it was really good sci-fi.

Leo: Great.

Steve: You know, I mean, bad alien sort of sci-fi. So, neat.

Leo: Yeah, yeah, can't wait to see it, yeah.

Steve: And I just wanted to mention for the record, I know nothing about this, but the pilot airing this Sunday on ABC of "Defying Gravity" is airing. It's, I don't know, again, anything the show. But a bunch of people are cooped up on a space ship which is on an extended voyage from Earth to Venus, I think is where they're going. And so I don't know if it's a reality show, or if it's sci-fi, or what it is. But it looks like it's relating to extended space travel from Point A to Point B by slow caravan style. No warp speed. So I don't know what it is, but it's this Sunday evening on ABC in the U.S. So I just wanted to make sure people who might be interested knew about it. I mean, my TiVo will be recording it, and I'll see if it's any good.

Leo: It's always worth a try.

Steve: And then a whole bunch of people that I ran across in our mailbag commented on jetlag.

Leo: Yes.

Steve: And my favorite one that caught my attention was a subject line, "Fists with your toes as a travel stress reliever." Bryce Shaskeen, Shaskink, Shas, Shasshinka...

Leo: I'll take your word for it.

Steve: Bryce knows who he is. He said, "Dear Steve and Leo. The fists with your toes line is from 'Diehard.'"

Leo: Right. Our chatroom knew that right away, by the way.

Steve: Oh, okay. It's about relieving travel-related stress, not jetlag. And then he goes on to cite literally verbatim from the movie. I don't know if he played it and transcribed it, or if he knows it by heart.

Leo: You can probably find it on the web.

Steve: And then the Richard Gere scene that I was thinking of, where I was - remember I said I kind of have this picture of Richard Gere. That was from 'Pretty Woman" where she's trying to get him to relax and to go for a walk in the park, and he takes his shoes and socks off, just like to not be so corporate and to walk around on the grass. And so those were his bare feet, so.

Leo: There you go.

Steve: Just in terms of errata, I thought that qualified.

Leo: There you go. Do you want to get started with our Q&A here?

Steve: I will. I do have a beautiful little SpinRite story from Matthew in Fresno. And the subject line, again, caught my eye: "SpinRite saved my marriage."

Leo: Okay. Okay.

Steve: He says, "Dear Steve. Just wanted to let you know that SpinRite saved my marriage. My mother-in-law came to me in a massive panic. Her laptop died with a BSOD, stating that a registry hive was corrupted. And of course she had no backup. She had lost all the pictures of our little girl that was just six weeks old. With my wife peering over my shoulder like a boss on a deadline, I researched the error and found the numerous pages Microsoft's knowledge base articles on possible solutions. Each solution required me to insert the XP CD and enter the Recovery Console and do a bunch of stuff to the file system where the registry is located.

"Of course, she didn't have an XP CD. So I rummaged through all my CDs, desperately looking for an XP CD that would work. Then I remembered SpinRite, and all those great stories you tell on Security Now!. So I figured, hey, can't hurt to try." And he says, "FYI, SpinRite was purchased as a site license where I work. I hope it's okay to use it on my home computer." Eh, not technically, but I thank you for the testimonial, so we'll call it even. "I put the SpinRite CD in and let it run on Level 2. It took a little over 17 minutes to finish and did not show any errors on the display. So I figured it wasn't the hard drive. I ejected the CD and rebooted the computer, just to see. During the boot process, Windows ran a chkdsk - hmm, that was new - then rebooted again. Then it finally booted into Windows with all our girl's pictures recovered, no registry hive problem."

Leo: Hallelujah.

Steve: He said, "I was immediately surrounded by hugs from both my wife and my mother-in-law. Thank you for this great product. Matthew in Fresno." And of course that...

Leo: Wow. And, now, back it up, Matthew.

Steve: That's, yeah, exactly, or tell your mother-in-law. Explain about backups to Mommy Dearest.

Leo: Wow.

Steve: And it's so often the case, again, I've said before, that SpinRite will apparently not do anything, that is, it can't report it because it's worked with the drive, recovered the problem, but the result was no error left behind. It didn't, you know, it was able to perform the full correction, fix the problem, relocate the sector, everything's good again. And so sometimes SpinRite doesn't get the credit that it deserves because it's unable to show it because it fixes it. But in this case it did.

Leo: Somebody wanted to know if SpinRite can be used on SCSI or SAS drives.

Steve: Absolutely. Yes.

Leo: It's the USB that kind of hides a lot of the information. But SAS or SCSI is not so bad?

Steve: Yes, exactly. I mean, SCSI provides a lot of information. You want the most intimate connection you can get. So if all you've got is a serial interface, well, that's the best it can do. But we've heard, we've had reports of it fixing Network Attached Storage drives. So it'll work at it until it is able to read the sector, or do whatever recovery it can. So often it's able to.

Leo: Now, this is going to air on Thursday, July 30th. But tomorrow is Sysadmin Appreciation Day. So I want to appreciate all the sysadmins out there, and especially our sysadmins, particularly Bear, who was working so hard yesterday when the DNS attacks occurred to get us back online. And Gordon, and Colleen really is a sysadmin, too. So thanks to everybody who's working on our servers. And Happy Sysadmin Day to all of you. Because I know a lot of sysadmins listen. I bet most people who listen consider themselves their own system administrator, if not for others.

Steve: Yeah, exactly.

Leo: Yeah. All right, Steve. I have questions.

Steve: Our listeners have questions and comments, and we're going to hear them now.

Leo: Starting with a long question. You ready?

Steve: Yeah.

Leo: Here we go. FireXware, writing from somewhere in the frozen north - Canada - wrote with the subject "SpinRite and Security Now! got me a job and a new hard drive." Hello. I'm a Security Now! fanatic. I started listening only a few months ago. I finally caught up. Wow, in a few months to listen to 207 episodes is pretty good.

Impressive. I'm pleased to say I finally had a chance to use SpinRite in a real data recovery situation. Being 16 years old - aw.

Steve: I know.

Leo: I love that - and the only tech-savvy person in the house, Mom came to me with a laptop that wouldn't boot. I turned it on, saw the Blue Screen of Death instantly. I knew what to do. I pulled out my copy of SpinRite, let it run on Level 2 for an hour or so, and to my mother's amazement the laptop booted like new. This impressed her so much she wanted me to come into her office and help out with some other tech problems, also to develop some software for her to make her life at work easier for her team.

One of my tasks was to fix a laptop that would not connect to the network. I saw the network was secured using the terrible WEP protocol. This guy's been listening. I asked Mom for the password. And well, let's just say I started laughing harder than ever when I discovered their WEP key is the first five digits of the office phone number. Oh, dear. By the way, I was looking at what Dan Kaminsky's passwords were? His root password on his system was five characters. Five alphabetic characters. Dan. Anyway, sometimes even the smartest people do that. So that makes me feel better because I do stupid things all the time.

I was so shocked, I started talking about security with my mom, who is the most tech-savvy person in the office. I discovered every user used the same password, and it happened to be the password is the one first on the list of many of the password-cracking tools. They have lists, you know, bad passwords. No. 1 on the list. Using the knowledge I gained from listening to your show, I wrote up a quick proposal that described the threats and vulnerabilities the network is susceptible to, and how to fix it. After the manager of the company had read this, he hired me to fix the security holes. 16-year-old kid.

Today I've earned enough money working that I'm able to afford a new terabyte hard drive which I've been wanting for ages. I will definitely be SpinRiting it periodically. Thanks so much for your amazing piece of software and equally amazing source of security and insecurity knowledge.

I also have a question. I love the concept of small is beautiful. Every line of code I write goes by that motto. I think that's good. Functional and elegant. I would love to learn how to program in Assembly language. I understand the basic instructions and how the register and stacks work. However, I'm confused by the infinite amount of flavors of Assembly language there are. I would like to know which flavor is your personal favorite for writing on Windows machines, and if you know of any resources to hone my skills in developing a GUI application in Assembly. Once again, thank you very much. Wow, what a nice, nice letter.

Steve: I just really liked that. I loved that he was 16 years old and out there getting going and doing the work. To answer his question, he referred to, he says, "I love the concept of small is beautiful." Well, that's the name, SIB.zip, of a little ZIP package that I have on GRC off of my own personal page at GRC.com, where I have all of the source for a simple, complete little Windows executable, with all the source code, written specifically as a little demo of here's a simple application written in Windows. To answer his

question, I'm using Microsoft's Assembler, MASM, M-A-S-M. And there's a tremendously useful site, MASM32.org, that I would recommend to this listener and anyone who is interested in getting started. They've put together a complete, essentially turnkey package of all the files that you need that you can download and install that sets you up to write Windows applications in Assembly language.

Leo: So there's really - there's only one Assembly language. What he's talking about is the Assembler.

Steve: Well, and actually the different Assemblers do have differences in the Assembly language. There's one machine language. So the actual machine language is fixed by the chip itself. But you could have different ways of mapping, you know, ASCII Assembly language down to the binary of machine language. So, for example, some assemblers use, for example, in an add instruction, you add two things where the second one is added to the first one. But you could also, in Assembly language, express it where the first one is added to the second one. So Assembly language can vary in terms of the way you express what you want the chip to do.

Leo: That makes sense; right.

Steve: But it ends up always assembling...

Leo: There's only one machine language.

Steve: ...[indiscernible] binary code.

Leo: Yeah, yeah, yeah. Although, you know, I mean, Intel has a specification for the Assembler code most people adhere to. I mean, it all looks pretty much the same.

Steve: And that is exactly what MASM is. If you look at Intel's PDFs, which are freely available and downloadable, their spec is what Microsoft implemented for MASM.

Leo: It's MASM32.com.

Steve: Oh, dotcom, you're right, dotcom, not org.

Leo: Actually, Bobcat, thank you for catching that. Good catch in our chatroom. They're so quick. Chris in Australia wonders about the new attack on AES-256. Oh, I haven't heard about this. I thought AES was really secure. I'm sure you'll cover the new attack on AES that reduces the complexity for recovering an AES-256 key to 2^119 - okay. I'm a little, feel a little bit reassured - and possibly less. See Bruce Schneier's blog. I've read that the attack does not affect AES-128. Why is that? And if this attack cannot be modified and applied against AES-128, does that mean that

AES-128, with a complexity of 2^128, is now more secure, I guess, than AES-256, since 256 has been reduced to 2^119? That makes sense. Is 128 the way to go?

Steve: Well, okay. Here's the problem. There's been a lot of conversation over in the GRC newsgroups about the strength of AES. And for example I already have a CryptoLink newsgroup that's been very active where people have been suggesting things and discussing things, and I'm working toward getting ready to start coding that. And so people have said, well, gee, Steve, will CryptoLink support AES-256? My original answer was no because there's just no need for it. 128 is so many bits long in key that, I mean, we're just - I have to always remind people that the numbers, like even though 128 is only twice as big as 64, in terms of the number of permutations of keys, every single bit you add doubles. And when you double something 64 times, it belies the complexity that results. So AES-128 is absolutely as safe as you could ever need.

But there is the U.S. government says that 192 and 256 are - they've got, like, ratings of secrecy. I can't remember now what the designations are. But it's like top secret, or super secret, or secret. And just these are arbitrary, that's nonsense. But that's the nature of some of the things that government does. So since the technology is there, it's like, okay, why not let CryptoLink run in 128, 192, and 256, if that's what people want? And so it's like, okay, fine. So 256 is incredibly strong, I mean, like ridiculously strong. It's there because we could do it.

And essentially the idea is - we did a whole podcast on the way the Rijndael cipher works. Schneier agrees, Bruce Schneier agrees that this in no way weakens the use of AES-256 for encryption. What this is, this attack is a subtle, purely theoretical weakening. And the word "weaken," there's no way not to use the word. But unfortunately it's the best word we have, but it does not convey the truth. Bruce agrees that it is theoretical, and it will probably always remain theoretical. It's way out in cipher land where the cryptographers operate.

And this is called a "related key attack," where if somebody had access to the keys, you could make small changes to the keys, changing only a few bits, and map how the so-called "key schedule" changes. You may remember that in a symmetric cipher like AES there's a key setup where you feed it a key, it runs the key through a bunch of pseudorandom tables which are established by the definition of the cipher to create sort of a - it's also called "key expansion" sometimes. You take a relatively small key. You run it through these pseudorandom tables, and it expands that to a bunch of keying material. And it's then you use the keying material for each round that you run the cipher through. And AES has a number of different rounds, depending upon the length of the key.

Some earlier attacks, so-called "attacks," again, in quotes, were only applicable with so-called "reduced rounds," where you, okay, you didn't really use AES because AES specifies how many rounds to use. You use the machinery of AES with a reduced number of rounds. And again, this is a way that cryptographers, operating out in crypto land, have of sort of creeping towards an answer. It's like, okay, they're just learning more about what this cipher does, what its characteristics are, how it acts, how it operates. And so this related key attack says that there have been other related key attacks which have been more limited in scope. This one is more general. And the idea is we can take a key, make a few bits of change out of the 256 bits of the key, and track how those changes propagate through the expansion of the key and learn something about it. And what we learn is that not as much changes as we were hoping.

So what you want in a so-called, like in a theoretically perfect cipher, is any changes in

the bits of the key completely change the action of the cipher in a way that can't be predicted, can't be penetrated. So this is purely, at this point, sort of a theoretical weakening such that it turns out that the 256-bit length is not as strong in the presence of somebody manipulating the key. Okay. The only time that might be useful is when the cipher is being used in a hash function where the data that you're hashing, depending upon the hashing algorithm, might provide input to the keying input of the cipher.

Remember that a cipher, if we view it as a black box, has a key, and then it's also got data. So the data is the block width, or the block length of a cipher. And the key length varies. So it's only in the case where you have a use of the cipher where you might have control over the key or know what the key is that even then this represents any weakening. But in all normal uses, for encryption, for example, in a VPN, or in SSL use of AES, there what is always secret is the key. And no one monitoring the channel, no one trying to crack it, has access to the key. The key is specifically what you're keeping secret. So there's no ability - the protocol, as we've talked about SSL, for example, generates the key in a way that prevents anybody from controlling it. The ends use pseudorandom generators to create their pieces of the key. And then they communicate in a way such that no one monitoring this is able to get the key, let alone control it or change a few bits of it or do anything with it.

So this doesn't apply in any way to normal symmetric use of AES for encryption and decryption. It's only theoretically interesting in cases for - really just for cryptographers. So this is like way out in academic cryptography. Because the words like "weakening" and "attack" are the way these guys talk in their academic papers, it generated some headlines. And Bruce isn't worried.

Leo: Good.

Steve: So that's the story with this AES attack.

Leo: Good. That's why we ask Steve these tough questions, so he can explain, it's okay, it's going to be all right. Now, here's one about jetlag. This show covers a wide range of topics, from sci-fi to jetlag to Vitamin D...

Steve: And I'm not even going to talk about Vitamin D until next week, Leo.

Leo: Okay, good.

Steve: Although I did take my second test this morning, as I took my first test a week ago Wednesday. I have my results from the first one. But I'm going to wait till we have results from one week of me laying out in the sun.

Leo: With a new technique. Well, I'm drinking - somebody, the company called Balance sent me some Balance Water for Travelers that has all these Australian flowers dissolved in it: she oak, grey spider, tall yellow top, crowea, bush iris, and mulla mulla. So I don't know if this is going to help. I'm still a little jetlagged. I'm still waking up early in the morning.

Anyway, this is John Hughan in San Francisco. He has a cure, he says, for jetlag: I heard the two of you, especially Leo, sometimes have trouble with jetlag. I'm going through a hellacious jetlag coming back from China. But every time I go those long, you know, Australia was the same thing last year. Those 15 time zones just will kill you.

Steve: Yeah, see, I don't move very far, so I'm not having that much problem with jetlag.

Leo: That's a long way.

Steve: You're doing big chunks of the globe.

Leo: I used to do Toronto every month. That wasn't a problem.

Steve: No, no.

Leo: I got a little tired coming...

Steve: And I did it with you. We really didn't even notice.

Leo: No. Though I have to say, always harder recovering, coming West, or going East is harder than coming West. In other words, coming back from China was worse than going to China. Going to Europe is worse than coming back from Europe. For me. He says: I wanted to mention a book that I've used that has helped eliminate jetlag, no matter what direction I'm traveling in or how many time zones I've crossed. I've done up to 10. Evidently it's based on a

handbook that the military uses, and it primarily involves eating certain kinds of foods at certain times starting a few days before the flight. The book is called "Overcoming Jet Lag" by Charles F. Ehret, E-h-r-e-t. You shouldn't have any problem finding it on Amazon or other booksellers. See, the problem here, I want to see a double-blind study. The problem is there's a huge mind component in this.

Steve: Sure.

Leo: So all of these cures, as long as you believe they're going to work, are going to work.

Steve: Well, and you want them to work because you bought a book. And so it's like, oh, you want the book to be right. For what it's worth, we put "Overcoming Jet Lag" into Amazon search. And sure enough, you can find a bunch of used copies of this for $4 and some odd cents. It is available on Amazon for anyone who's curious.

Leo: But of course after you spend all that time getting jus the right foods in ahead of time, I'm sure that helps, just because you've invested so much in it. I would like to know more. I'm going to do - I have to - you do your Vitamin D. I'm going to do my jetlag study.

Steve: Okay.

Leo: John Kennedy from Metairie, Louisiana asks Steve to touch the bleeding edge. Yikes. Hi, Steve. I'm a long-time SpinRite customer and Security Now! listener. On the Security Now! netcast, I often hear you comment that you do not use current software versions because they are unstable and unproven. Some examples come to mind, your comments on sticking with XP and FireFox 3.5 even though - actually you didn't say 3.5. You said 3.0, I think.

Steve: No, and he means not going to 3.5, even though 3.5.1 is available.

Leo: Oh, all right.

Steve: I think.

Leo: You're using, just to be clear, XP and 3.0; right?

Steve: Yes, and happily so. 3.0.12.

Leo: As a computer consultant and software developer for the past 25 years, I appreciate, respect and agree with your position. From a consultant's perspective, I do not like my clients using the latest versions of products or patches for the same reasons you mention. Patches. When he says "patches," that worries me. However, as a consultant I have responsibility to use and test the new versions of software and patches to insure their benefits and side effects, thus becoming the guinea pig.

As I listened to your latest - I'm the guinea pig here, by the way. I use everything. I like it new. I like new, shiny stuff. As I listen to your latest Security Now! episode, a thought hit me: I wonder if Steve would consider breaking from his policy and providing review and analysis of version updates and patches. Of course, by "breaking policy," I don't mean using these updates in your production environment. I was thinking more in terms of using a virtual or test machine solely for evaluating updates. I believe your perspective and the level of analysis you bring would be of tremendous benefit to your listeners.

Right now, I believe most of the information that surfaces with each software update is from a journalistic perspective. It would be great to have technical information and review from a respected and trusted person such as yourself. I always thought that's what journalism was supposed to do. I think what he means is the journalists tend to be rah-rah about this stuff now. Please give this some thought and consideration.

Thanks for your work on Security Now!. Looking forward to your other works in progress. Comments?

Steve: Well, if I didn't have a day job.

Leo: [Laughing] Yeah, who has time to do that?

Steve: We're talk- yes, we're talking about, I mean, I appreciate John's suggesting that maybe I would be a good person to do this. And I have done it inadvertently, for example, when I made the mistake of updating my Windows XP to Service Pack 3, and it hurt me, and I told everybody ouch, be careful, I got hurt, don't you get hurt. But those are expensive and inadvertent things for me. I made the mistake of trusting a service pack which, you know, obviously is like a set of patches, as John was talking about. The problem is these - generally these things are tested before Microsoft lets them go, for example, or Mozilla lets them go. As far as anyone knows, they're releasing something that's working. So it takes boundary conditions to find the problems. It takes a large number of people, all pounding on it in different environments to find those situations where it may not work.

For example, Service Pack 3 worked for many people, most people, and other of my systems. Not, unfortunately, just my main one. And Microsoft's bugging me about it now all the time. You really should install Service Pack 3. It's like, you know, I tried that. Didn't work for me. So I would - conceptually I love the idea. But there's just no practical way for me to run a production environment and a non-production environment because it's only by using these things that you find the problems, and by that point it's often too late. So, and especially when we're talking about security. I don't want to run with something which is potentially lowering my security because I'm proud of the fact that my defensive walls are as high and thick as they are, and that I'm able to get the work I need to get done, done, without things crawling in, and not having experiences like Dan Kaminsky.

Leo: Dan Kaminsky, yeah.

Steve: Exactly.

Leo: He says, if you go out on the battlefield, you're going to get shot. So Steve says, I'm not fighting that battle. I understand that. What about, though, I want to...

Steve: Well, no, I've got my armor on. And someone says, yeah, but...

Leo: You're not going to take it off.

Steve: ...we want you to see if those bullets are pointy or not.

Leo: Yeah, how do they work? But it does make me nervous that he says "patches" because - and I understand this is an issue because...

Steve: Patches have hurt people.

Leo: Yeah. But at the same time, don't you run a pretty big risk by not applying those patches?

Steve: Yeah. I do think there you begin to tip, you reach a tipping point where it's like, eh, it's probably better to patch and hold your breath.

Leo: There's no perfect solution on this. Steve doesn't use JavaScript. I do. There you go. I'm just living on the cutting edge. And by the way, you know, knock on wood, not been hacked yet. Andrew McKinnon in Brisbane, Australia - although I'm worried about my iPhone in about 24 hours - wonders about his iPhone's Internet address: Hi, Steve and Leo. My question relates to the iPhone. Basically, until a month ago, my iPhone was reading my IP address as 144.233.xxx.xxx. However, on recent days it's been 10.1.xxx.xxx. Am I right - I think I know the answer to this. Am I right in assuming that my iPhone is now being proxied by my ISP as this seems a private address from a router, much like I find in my home netcomm. Funny thing is my iPhone only does this in certain areas, and it's always on cell networks. Oh, okay. I thought he was using WiFi. He says, no, I'm not using WiFi. If my ISP is proxying my traffic, what's the purpose of this, and why do they only need to do it in certain areas? Well, that's interesting. Let me look at my iPhone IP address. What's going on there, do you know?

Steve: Yeah, it's, I mean, it's nothing surprising. In one case, that 144.233, his phone was given a public IP by...

Leo: From the ISP.

Steve: Yeah, exactly, by whatever ISP and region he happened to be in.

Leo: In this case his ISP is his wireless carrier, of course.

Steve: Exactly. And in another case, located somewhere differently, he had a 10.1.xxx.xxx IP. I know that when I was using - Verizon is my carrier, and I was using a wireless broadband card. And in fact one of the problems I had with OpenVPN that caused me some concern was that - I think it might have been, in fact, when I was in Vancouver with you, Leo. I received there a 10-dot IP address that was the same network subnet as I was using at home. And so OpenVPN, that uses a routing table in order to route packets, was confused because it thought I was at home and wasn't able to route the packets out the VPN to my network at home. So, and that was another one of the things that I said, oh, I'd have a better solution for that, and I'm going to write my own. But all this is, basically, is an ISP who's got you behind NAT. It's not necessarily a

proxy, although it is also the case that some cellular systems will proxy, for example, web access, and that their web proxy is designed to deal with the presumably small screen of a telephone. It may rescale images down.

Leo: Right.

Steve: So it's minimizing its bandwidth. It's not sending you a big, huge PNG file that then gets scaled in the phone. That's dumb. Instead it's scaling it on a high-speed, high-performance server down to a small physical size, then sends a much smaller file down to your phone. So there you are seeing web proxying for the benefit of an improved web surfing experience. But in this case it looks like in one case you were behind NAT, and the other case you weren't.

Leo: Yeah, I don't think the iPhone browser Safari does that web proxying. We know Opera does, and a few other browsers.

Steve: Yep, and I know that I have the option on a Treo to do that or not, like to - they call it "extra web acceleration feature" or something like that.

Leo: Right, right. It's possible that your Internet service provider, your wireless provider does something like that. That's an interesting question. Why would it change from place to place?

Steve: Well, I think it's just different carrier setup in one location or another. So it's just, you know, it says, like, okay, I mean, it really doesn't matter technically what your IP address is. For example, you never really paid attention to it, Leo, and you're about as techie, you know, a user as there is. So it's just my phone works, it's got an IP, the traffic's coming back to me. Andrew was saying, hey, you know, why is it different and what does that mean? And so, I mean, technically it means that they're just different setups for the way the traffic gets back to you. One is back through a NAT, where certainly that 10.1, as we know, the 10.1.xxx.xxx, that address cannot go out on the public Internet because 10 is one of the nonroutable networks like 192.168 is a nonroutable network. There is no - if packets were sent out on the 'Net that were destined for 10, or that came from 10, there's no way that the packets would ever get back to you because 10 is a reserved private IP space. So as your phone's packets, which are coming from 10.1, go to your ISP, they are then NAT'd back to some public IP that allows them to go out on the 'Net, come back to that same point, and then get turned back into 10-dot as they cross through the wireless link back to your phone.

Leo: Just as a router does.

Steve: Exactly like...

Leo: It's a router.

Steve: Exactly, yes. And we know, for example, there are even some cable providers that have their customers behind NAT. So even cable modems sometimes get a private IP because the ISP presumably is running short of IP space and has NAT'd all of their clients, all of their customers.

Leo: Question 6, Kevin Ghadyani from Overland Park, Kansas worries about the number of HTML errors and warnings on the Security Now! page of GRC. Steve, when he runs it through the W3C validator he gets 13,853 errors and 24 warnings: I thought you would've fixed yours because you're like that, but even MSN.com validates. I'm extremely surprised to see this and hope you'll fix the errors over time. I've never personally seen so many errors in my life. I run a site, badmarkup, which I use to talk about this stuff. And when I get some time this year, sometime in October, I'll be going around looking for this stuff. Please don't let me have to discuss GRC on the site. I think you should discuss GRC, Kevin. Why are you getting all those errors?

Steve: Absolutely. Well, this comes up from time to time. We'll see postings in the newsgroup. Somebody will have run a page, just because they have spare time, I guess, through the W3C validator, and it just explodes. I mean, somewhere there's smoke coming out of a validator in Sweden or Stockholm or somewhere.

Leo: I've never seen anything like it! Yikes.

Steve: 13,853 errors. My pages are designed to work. And, for example, there's all kinds of tricks that it's necessary to play in order to make things work on old and new browsers. GRC's script-free menuing system, which was developed painfully over the course of many months with a huge bunch of testers in our newsgroup, manages to work beautifully on every web browser. But it's a validation nightmare because of all the tricks I had to play in order to work around differences between web browsers. If web browsers all worked correctly, then, yeah, one batch of HTMl would work everywhere. My stuff is designed, not to validate, but instead, huh, to work. And it does.

Leo: Well, I mean, in theory the idea of validation is that it would work on all platforms that were compliant. So is it the platforms aren't compliant, or that...

Steve: Yes, it's that there are subtle differences, for example, in the way Safari handles CSS from IE. And so you can give the same code to two browsers, and it will look different. And when you're trying to design something as tight as the menuing system, where spacing and positioning and, I mean, it really has to be geometrically perfect, it turns out you discover how nonstandard browsers are from one to the next. I mean, remember that IE8 even has a list of sites where it falls back to IE7 because in IE8 they're more standards-compliant than they were in IE7, which breaks sites which were deliberately tuned to work under IE7. So, you know, who's fault is that?

Leo: Right.

Steve: I mean, I have - if someone does hold their breath and pinch their nose and stick

the Security Now! page through the W3C Validator and actually look at the errors, they'll find they're not big things.

Leo: What are they?

Steve: They're little things, like I put quotes around numbers in some cases where they're not supposed to be, or I used old margin callouts on image tags, which used to be supported, but aren't anymore.

Leo: That's what I thought it probably was, is that you're using HTML 1.1, for instance. You're using an old HTML.

Steve: Yeah. I code my stuff by hand rather than have some big prophylactic web authoring thing so that my code just looks like some horror. If you've looked at some of these pages, you can't read them. Mine is all legible because I wrote it in Notepad. But I did it very carefully, and it works. Doesn't validate worth beans. But it runs on all browsers.

Leo: You might be able to, I don't know...

Steve: Leo, you know what?

Leo: You don't care.

Steve: I don't care.

Leo: That's the bottom line.

Steve: I have so many more pressing...

Leo: You might be able to put in your prologue code something that will tell the validator, oh, no, this is a valid 1.1...

Steve: If I just told it to buzz off. Oh, no, you can't do that, either, Leo. It breaks other things.

Leo: Moving along, Question 7, Mike V. in Greeley, Colorado. He *really* wants security. NOTE: I am totally okay with you reading this on the show, he says. Hey, Steve. I'm only 14 - I love it, all the kids that listen - but I love your podcast, and every episode is a journey into the complex world of security. I'll second that emotion. I wish I could say that I've listened to every one of your shows, but I just

started tuning in in March. Well, come on. Don't be a slacker, Mike. You can just listen to a couple of hundred episodes all at once. I have a system for mobile USB security. I wanted to make sure it was totally safe. I've encrypted all my files on my USB drive with TrueCrypt, with a password from your Perfect Passwords system. Sounds good so far.

Steve: Yup.

Leo: The password for that is stored in a text file on a drive, actually on the same drive, which I encrypted with 7-Zip, which is what you were recommending; right?

Steve: Yup.

Leo: Oh, no, you recommended the PKWARE ZIP program.

Steve: Right, SecureZIP.

Leo: SecureZIP. The password for that zip file is another Perfect Password, which is stored in a text file on a separate thumb drive I always carry with me. This is the problem with the Perfect Passwords, they're not memorable. So you kind of have to write them down or store them somewhere. So he's trying to get around this problem. THAT text file is in a zip with a password that I've memorized. So tell me, he says, am I going too far with this encryption? I don't hang around computer hacker conventions too much - too much - but I am worried about people getting to my passwords through Firefox Portable and Google Chrome Portable. Do you think this is a viable method, or is there a better way to make the USB drive 100 percent secure? Thanks for the show. Best wishes for the future. Mike V. Hmm. Seems like it's inconvenient, I'll say that much.

Steve: Well, and actually it isn't that secure. It sounds good. Because he's got a whole bunch of the Perfect Password gobbledy-gook that he's sort of encrypted in a chain. But the problem is, it's a chain. And at this point 80,000 listeners know what that chain is.

Leo: Right.

Steve: The end of the chain is a simple password that he memorized. So really that defeats everything else.

Leo: He should just use that simple password for TrueCrypt.

Steve: Well, any one of our listeners - well, no. You don't want to use a simple password for TrueCrypt because that's the vulnerability of TrueCrypt, the only vulnerability, is brute force. And so if he has a simple password for TrueCrypt, then it could be brute-

forced. The problem is, 80,000 people now know what his protocol is. So there was some obscurity there until we read this on the show, which he's totally okay with.

Leo: That's called, by the way, security through obscurity. And maybe he's obfuscated it. Maybe he doesn't really do it that way, or he left out a step, or...

Steve: Well, so the problem, though, is that the end of this chain, I mean, the reason I liked this question is that it's a perfect model for something that seems secure, but when you think about attacking it, it says whoops, wait a minute. The end of that is a memorable, memorizable, simple password. So everyone knows the protocol now who's listening to the show. So all any of us would have to do is try to guess the password for the final zip...

Leo: They'd have to have physical access to the other key, too.

Steve: Excuse me?

Leo: It's on a separate thumb drive, so they'd have to have some physical access, as well.

Steve: Right, right. So we - but presumably, now that we know that, there's no protection for any of his so-called protocol that he has. So we guessed the simple password to unzip that file. That gives us the password for the 7-Zip, which we use to unzip the password for the TrueCrypt, and then we have the access to the USB drive.

Leo: So he's really trying to make it obscure by complexity and obscurity as opposed to genuine security.

Steve: Correct. And I would argue that...

Leo: Well, what do you want him to do? Memorize a Perfect Paper Password?

Steve: Or take the Perfect Paper Password, and then customize it in use. So, for example, cut and paste it into TrueCrypt, and then make some changes to it that only he knows. So he's essentially done a multifactor authentication. By starting with the root of a Perfect Password, he's got something full of debris that cannot be brute-forced. But by then making some changes, putting a couple extra characters in, in places that he memorizes, which is easy to do. You've broken it so that you just can't use the Perfect Password. You have to use the Perfect Password plus some changes that only he knows.

Leo: Oh, that's clever.

Steve: And that's extremely secure.

Leo: That's the problem, and this is the whole issue with secure passwords. The more secure they are, the harder they are to remember.

Steve: Yeah, exactly. And we have an interesting suggestion about that coming up.

Leo: Oh, good. Well, let's get to it. I mean, sometime. This is another 16 year old. Question 8, Scott in Upstate New York makes a brilliant observation about Firefox Privacy: I'm 16 years old, and I've been listening to Security Now! since Episode 25. Your show has taught me everything I could ever want to know about security and how my computer and the Internet works, to boot. Keep up the great work. Anyway, a few episodes ago you discussed how Firefox remembers how you zoomed the page of a website you visited. I had noticed this in the past, but I didn't know it was a "feature." The question is, could this be a security or privacy concern? Firefox retains the zoom setting even after you have cleared private data. Therefore, it must be saving the websites you have zoomed somewhere. This cache denies you the plausible deniability and privacy provided by clearing histories, cookies, et cetera. I poked around about:config, but this sheds no light on my question. So is it a security/privacy concern, or am I blowing it out of proportion? By the way, no SpinRite yet. My parents won't buy it until something fails. But you can guess what I am going to do with my first paycheck. Well, that's an interesting - boy, that's an interesting point.

Steve: It's brilliant. I mean, that's why I said I think this is a brilliant observation. So Scott has noted that, if you change the zoom level on a website, Firefox remembers it. We talked about that as a feature. He noted that that isn't forgotten when you clear your personal data. And arguably, it should be because you lose, as he said, plausible deniability about never having been to the site before.

Leo: So it's a per-page setting. It's not global. It's for every page you visit there's a different setting.

Steve: It's a per-site setting.

Leo: Okay.

Steve: Yeah, per website. Or maybe per page. I think it's per domain. I would imagine that's what Firefox would...

Leo: In any event, it's somehow, somewhere, storing the name of a domain and your zoom settings.

Steve: Yes. There was a really interesting privacy hack that went around maybe about a year ago where there was a way that JavaScript could test links to see whether you had visited them or not. Remember how on many browsers a link that you have visited will be a different color. And there was a way to get JavaScript, just by itself, to, like, check

the color of a link that it itself created, sort of off-screen, and that allowed it to determine whether you had ever been to a given page.

Leo: Wow.

Steve: So it was a really interesting privacy hack. And this is sort of similar to that. So I just wanted to give Scott a tip of the hat. I think that's, I mean, he's thinking like a security and privacy person.

Leo: Now, we don't know where this information is stored or how accessible it is.

Steve: I haven't pursued it. I just loved the question. And I assume that, given the way this is written, looks like Scott knows what he's doing. He talked about clearing the private data and realizing that Firefox remembered zoom settings, which said, oh, someone's been to this page before and changed the zoom.

Leo: Yeah, they should clear that, as well, shouldn't they.

Steve: Yeah, they should.

Leo: Yeah. Patti Clark, who was, oh my goodness, an early CompuServe employee in Knoxville, Tennessee, remembers with us. We were talking about our CompuServe email addresses. I was listening to Episode 205 on Lempel and Ziv when my ears perked up on the CompuServe segment. I spent most of the 1980s as an employee of CompuServe. You were correct when mentioning that CompuServe was a time-sharing company, and H&R Block was their parent. The computers behind the Consumer Information Service were DEC System 10s and 20s. That's what they called - CompuServe was called CIS.

Steve: Right.

Leo: I had the pleasure of working with one of the system programmers who had pulled together a handful of games and created the forum - precursor to bulletin boards and chat rooms - software. The idea was indeed to do something with all of that computing power that was sitting mostly idle during the evening hours. It surprised management when it took off and ultimately became what the company will be known for in history. AOL bought CompuServe from H&R Block some time back. Back then, modems started as 300 baud acoustic couplers - that's what I used to log onto CompuServe when I first started doing it - then later 1200 and 2400 baud modems were comparatively fast. Everything was text-based. Yeah. We were on the "bleeding edge" when we brought email to larger corporations and the federal government. Sorry, my reminiscent hat has slipped on. Anyway, I enjoy your program, and I learn something new each week. Thank you, Patti Clark. 75106,3139.

Steve: I just thought that was neat.

Leo: Yeah.

Steve: And, you know, I don't know what it is, but the nostalgia factor for me, like remembering taking the Series 500 phone, that was the number of the standard blocky telephone that we had at the time, and pushing it down into the acoustic couplers.

Leo: Yes, they had little suction, little kind of rubber things that you would - so it would seal the noise out.

Steve: Yup.

Leo: Wow. And 300 bits per second was the fastest that could go, that system could go.

Steve: Yeah. I mean, and there your - that was 30 characters per second, and you could just sort of see it painting the line, the way they still do in, like, kind of hokey B-grade sci-fi movies where the text comes out slowly.

Leo: That's how I played...

Steve: So very cool.

Leo: ...Colossal Cave, Crowther and Woods' Adventure. They had an extended Colossal Cave that I played quite a bit, many, many hours, on 30 characters a second.

David Cox in Colorado Springs reports Security Now! almost killed him. Hi, Steve. I began listening to Security Now! shortly after you and Leo began with Episode 1, while I was stationed in Cornwall, England with the U.S. Navy. I drove one of those tiny Smart cars back then, you know, the poor man's Mercedes. It was called "Smart for Two," and they are slowly growing in popularity now here in the States. Actually I got - I reserved one, and it came, and I said, nah, I'm not going to buy it.

Steve: Yeah.

Leo: Kind of seemed a little dangerous. Fantastic gas mileage; easy parking anywhere. No, I haven't totally lost it. There is actually a point to this ramble. So I'm driving to work early one morning on those very small, windy English roads, listening to the latest Security Now! episode. It was dark, rainy, foggy, and I was completely lost in the show. Suddenly, less than 30 feet in front of me, a big lorry - a.k.a. a big-ass truck - went flying past me from right to left. I had been driving this road for

several years already, and I knew my turn was up there. But as I said, at that time I wasn't in England driving to work. Rather I was sitting somewhere in Irvine at a Starbucks with my Venti Caramel Macchiato, totally engrossed in what Steve and Leo had to say about information systems security. By the way, I was the Information Assurance Manager for my duty station at the time. What a nice story.

Steve: Isn't that neat?

Leo: So back on this wet road, in dark fog, I suddenly snapped to reality, yanked the steering wheel counter-clockwise as hard as I could, and miraculously found myself directly behind the truck that had woken me up from security school. I don't know how the car didn't flip over, or how I avoided the oncoming traffic, or why my driving instincts were so damned good that one early morning. All I know is I lived to listen to many more of your shows, which incidentally have since gotten me through the diagnoses of leukemia, a bone marrow transplant, and now lung disease and possible double lung transplant. Oh, David, I'm sorry. Your shows have kept me sane and given me something fun and informative to look forward to each week. I for one applaud you for not missing a single episode. I am also a loyal SpinRite owner and user. It has saved my bacon a couple of times, although it didn't help Dad on his RAID-configured system. I'm guessing operator error. Well, keep up the great work, and I am really, really looking forward to CryptoLink! As a side note, what do you know about DNSSEC? It appears to be DNS with authentication added for increased security. Maybe a short mention, or is there enough for a dedicated episode in the future?

Steve: Well, first of all, I just wanted to thank David for his story. We get just such great mail in the mailbag from our listeners that it's just - I wanted to share some of these sometimes. We did do an episode on DNSSEC. It wasn't only dedicated to just that one topic. It was something about Google. It was, like, two topics in one show. It's around Episode 161. I did, I went...

Leo: You can search it, and I'm sure you could find it, search the transcripts.

Steve: Yes. I went to the Security Now! page. We have a search box in the upper right. Put in DNSSEC, there's two pages worth of hits. One of them is me talking about, when Leo asks me, well, so what are we going to talk about next week, and that's when I talk about I use DNSSEC, and Elaine transcribed the acronym. So it's around there. It's Google something and DNS Security is the topic, is the formal title of the podcast. And so by all means check it out because DNSSEC is coming.

Leo: Yes.

Steve: Thank goodness.

Leo: Not soon enough. And that's thanks to Dan Kaminsky, by the way. Robert

Altman in Los Angeles - oh, no, I'm sorry, I was thinking of the director. It's Robert Antman in Los Angeles has a thought about Perfect Passphrases: Dear Steve. Thanks for providing the Perfect Passwords service on your website. This password generator - by the way, it's GRC.com/passwords, folks, GRC.com/passwords. This password generator is perfect for many applications, such as generating a pseudorandom WPA password. That's a really good use for it for your WiFi. But it's not so perfect in other applications, such as generating a pseudorandom passphrase for typing into TrueCrypt, because - as we said - it's almost impossible, at least for me, to memorize this long string of random gibberish. It's especially difficult if you plan on changing your passphrase periodically. As an example, if I wanted a pseudorandom passphrase that provided 128 bits of entropy, and I restricted the character set to alphanumeric characters only - a-z, A-Z, 0-9 - the passphrase would have to be 22 characters long. And he does the math: (128/log2(26+26+10) = 21.4). So here's an example. I'm not going to read it. Trust me, it's 22 characters of gibberish.

Steve: Yes.

Leo: I claim it's much easier to remember a passphrase consisting of random words, random English words in my case. Would you consider coding a Perfect Passphrase generator for your website? Actually, you know, a lot of operating systems, I know Macintosh does this for you. There are a lot of programs that'll do this for you. Macintosh, you can ask it for a memorable password, and it'll give you kind of random language words with punctuation and stuff stuck in there.

Steve: Right.

Leo: Anyway, he says: The Second Edition of the Oxford English Dictionary contains entries for - as you know, Steve has this over his right, or left shoulder, right shoulder, so he knows this - 171,476 words. If you could obtain a list of the most common 65,536 English words, that's 2^16, you could then take 16-bit chunks of your pseudorandom number generator and use it as an index into the word list. Oh, that's a good idea. Display that word and repeat the process to produce the random passphrase.

For example, to provide a random passphrase with 128 bits of entropy, you'd only need eight words. that's 128/16, like, say, "decompose ironic humid fizzle muslin purchase guacamole mazeltov." There, isn't that easy to memorize? No. I made that list by flipping open a dictionary and pointing at words at random. There are some who would claim the use of a passphrase consisting of ordinary words is susceptible to a dictionary attack, but that is not necessarily true. Provided that the words are chosen at random and you choose enough of them, a random list of words is every bit as secure as a random string of characters.

Steve: Well, he's exactly right. I love the fact that it was, you know, you might say it was susceptible to a dictionary attack because of course that's where you got the words.

Leo: Right.

Steve: Was from a dictionary.

Leo: However, you'd have to do a lot of dictionary attacks.

Steve: I want to, again, I like this because he's completely right. I mean, and his phrase - "decompose ironic humid fizzle muslin purchase guacamole mazeltov" - okay, that's 128 bits of entropy. Given that the words - given that you start with 128-bit, high-quality, pseudorandom chunk of bits, you take them 16 bits at a time, use the 16 bits to select one word out of 64K words, you're going to get something that is absolutely strong. It also, unfortunately, is a lot longer than a passphrase of gibberish because you're now using a word instead of 16 bits. And as we know, 16 bits is two bytes. Well, that's not two characters because characters don't occupy the whole 256-size alphabet. But it's maybe three characters or four characters. So you end up with something longer at the - I mean, you end up with something longer...

Leo: And more memorable.

Steve: Maybe more memorable, but...

Leo: Not a lot more memorable.

Steve: I guess it's, yeah, it's more memorable. I would say that, again, given that you were going to - if you're going to write something down, write down some gibberish, and don't write down your personal modification. This notion of making a modification to gibberish is very powerful because you get both complete protection from dictionary attack, and somebody looking at it has no idea how to turn it into your actual password. So you can - and not even any idea how to guess how to turn it into your actual password. That is, what customizations you make to it. That's very simple for you to remember, yet nobody can glance at this 22 characters of gobbledy-gook and have any chance of memorizing it. So in some senses it's stronger.

Leo: Right. Can I ask you - you may not want to reveal this. But what do you, you know, you have to come up with passwords. How do you do this? You're not using those 64-byte crazy strings, are you?

Steve: I often do.

Leo: For, like, websites and stuff?

Steve: I use my own Perfect Passwords for all kinds of things. And then I - and I record them in a text file.

Leo: But what about something you need to remember easily? You don't have anything like that, huh?

Steve: Yeah, then I record them in a text file, which I protect. Yeah, and then I have other algorithms that I use. I've got different ways of assembling things. We did, for anyone who's interested, who's joined the podcast late, some of the very first episodes of the podcast, back number 1, 2, 3, 4, we did a series on passwords that a lot of people really liked.

Leo: Listen to that again, yeah, that's really good. And just how to generate a good password, yeah.

Steve: Yes, I would really commend people to go check that out.

Leo: That would be required...

Steve: It's where we got our roots, Leo, where we began.

Leo: Yeah, required listening. Might be worth, well, there's no point in redoing it. People can just go back and listen to it.

Steve: It's there, yup.

Leo: Last question. Are you ready? Jeff, hiding out somewhere in the U.S., doesn't want to blink. "RFID in credit cards. Should I run and not walk away?" Steve, my Chase credit card was approaching its expiration date. I

received the new card in the mail. My new card came with a feature called Blink, a.k.a. an RFID chip. Now, the average person thinks that waving a card in front of a terminal instead of swiping is the neatest thing since sliced bread. But as an avid Security Now! listener, I'm not so sure about that. How much am I at risk? Should I wrap my card in foil or request a replacement without the RFID chip? I don't mind having this Blink feature as

long as I'm not at risk of losing everything in the "blink" of an eye. Good point, Jeff. What do you think about this?

Steve: I think it's the worst idea I have ever heard of. I mean, it is - Visa has been doing this for a while. They've got their little terminal where they've got some, I don't remember now what their marketing jargon is for it. But the idea is you just bring your card near the reader. The problem is, this RFID is a standard. And you're able to send a magnetic pulse to the card, a little radio frequency burst which engages a wire-wound antenna, powers up the chip, and then it modulates, it uses the incoming power to modulate the impedance of this loop which the transmitter is able to sense. Unfortunately, this is a standard. And so potentially any other transmitter is able to poll

your card while it's in your wallet in your back pocket. I mean, I just can't imagine anything more ridiculously insecure than this. It's phenomenal to me that this is something which has been allowed to happen. And, I mean, if we keep doing the podcast long enough, Leo, we are going to be talking about breaches of security from RFID credit cards.

Leo: Oh, yeah, definitely.

Steve: What I would recommend Jeff do is stick it in the microwave for about five seconds. That will...

Leo: You won't be able to wave it anymore, but...

Steve: ...nuke it. That will nuke the RFID chip. It won't hurt the mag stripe because that's oxide, which is not a conductor. And you'll have an RFID that no longer "blinks" at you or anybody else. Yet you'll still be able to use it and swipe it. It's just crazy.

Leo: You know, U.S. passports also have these RFIDs in them.

Steve: For what it's worth, ThinkGeek, one of our favorite sites, has a bunch of fun RFID things.

Leo: You can get a wallet protector and so forth.

Steve: Yes. If you go - and even a passport protector.

Leo: Right.

Steve: Now, the good news is the passports were designed so that their covers will block the RF information. So that a closed passport, as I understand it, if it's what I'm thinking of, a closed passport will not allow you to access its contents. You have to open the passport in order to then have access to the RFID chip inside. ThinkGeek is www.thinkgeek.com. If you just put in their search box in the upper right "RFID," you get a page of fun stuff. The first one is an interesting little kit. I have two of them. I've just not had any time to build them and play with them. It's an RFID experimentation kit, $99, that has an interface board with a USB interface to a PC that allows you - and a whole bunch of different shape little funky RFID things. I mean, even something you could implant in your arm if you were so inclined, and different shape RFID tags. They all work with this because the RFID standard has been established. And it would be one way to, like, literally, you could read out the RFID information in your credit card using this little experimentation kit. And that would be also a way of verifying that five seconds in the microwave was enough to kill it.

Leo: One of the people on the cruise with me is a security researcher, Shakil. And he had a passport wallet to shield his RFID. And actually it set off the machine because it's got metal in it. And we were talking about it. He said, one of the reasons I wear this is - and you can find this on YouTube. Some security researchers demonstrated that it's possible to read these RFIDs in the passports from a distance. And stupidly, the State Department has put in an identifier that says "U.S. Citizen" in it. So the video that you'll see on YouTube is a bunch of people walking by a trash can, and the trash can explodes when a U.S. citizen walks by. Not a difficult thing to do. So Shakil, as soon as he saw that, said I think I'm going to get a passport holder here. Yeah, this is something kind of incredible.

Steve: And for what it's worth, the other things on the ThinkGeek page are various types of shields. There's a wallet shield, a passport shield, credit card shield, a bunch of different shields. I mean, it just...

Leo: Completely legal to do that, by the way. You're still handing over the passport for them to read, for customs and immigration people to read. And they can open it up.

Steve: Sure.

Leo: But you don't have to be visible to the rest of the world.

Steve: No. And again, that's the problem. It's not the transaction that you intend. It's the transaction that you don't intend. And it is definitely possible to aim a focused radio beam at somebody and pick up the impedance change that the RFID chip is inducing at a distance. So, I mean, this is not rocket science. This is simple to do. It's just nuts that this is something that people are thinking, oh, great, now I don't have to swipe my card anymore. I can just walk past the teller.

Leo: Credit cards, though, are inherently insecure. I mean, you hand it to a waiter, and he wanders off with it for 10 minutes. I mean, the whole idea of a credit card is not so secure.

Steve: That's a very good point, too.

Leo: I mean, people, c'mon, we're giving it...

Steve: On the other hand, you know you're handing it to him. You're still in the physical world, and you're able to assess the security. There are certainly people you would not hand your credit card to.

Leo: Like Vertrue. Dale Poco has found the location in the Firefox profile folder of the

zoom settings, per page zoom settings.

Steve: Oh, cool.

Leo: It's in a SQLite database. So it is in the profile folder. And you just have to find a file called places.sqlite. And that's a standard, readable SQLite file that contains all the places you've been. Aha.

Steve: Isn't that nice.

Leo: Isn't that nice. Okay. Well, now we know. Steve, a great episode. Lots of information. I really appreciate you taking the time to answer these questions. We're going to do more questions next week; right?

Steve: Yes. That will be the final episode of the fourth year of the podcast. Another Q&A next week, and then we'll plow into our fifth year.

Leo: Fifth year. Amazing.

Steve: And I will have some news about Vitamin D. I'm going to go take my clothes off now, Leo.

Leo: Okay, okay. We'll turn the cameras off. You can find Steve at GRC.com, that's his website. GRC.com/passwords for the passwords. You'll also find the Security Now! page there with 16KB versions of the show for easy download, those of you who don't have the bandwidth, or the caps are getting in the way. Also transcripts, great way to search and read what Steve's talking about, read along with the transcripts. And all that great software that Steve does, much of it for free. And his bread and butter, of course, his day job, SpinRite, the world's best hard drive maintenance utility. It's a must-have if you have a hard drive.

Steve: It works.

Leo: It works. Steve, we'll talk to you next week.

Steve: Thanks, Leo.