SECURITY NOW!

Transcript of Episode #160

Listener Feedback Q&A #49

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-160.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-160-lq.mp3

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

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 160 for September 4, 2008: Listener Feedback #49. 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 where we explain how the Internet works and why it's so very dangerous to be out there without protection. Steve Gibson's here from the Gibson Research Corporation. Hi, Steve.

Steve Gibson: Yo, Leo. Great to be back with you again.

Leo: The king of security; creator of SpinRite - the ultimate disk recovery and maintenance utility - and many great free security tools like ShieldsUP!; and of course long-time host of this show, now entering our fourth year of security podcasting, or netcasting.

Steve: Yeah.

Leo: So today is a Q&A.

Steve: We have a Q&A. It's been a very quiet week, thankfully, on the security front. I have a couple things to talk about that are just little tidbits about security, a very short SpinRite mention, following up on - actually it's sort of related to last week's...

Leo: That was a wild story. Man.

Steve: That was, yeah. We heard from some people who were skeptical about its reality. And, you know, I just read what we received. And so I leave it up to people to judge for themselves. But, I don't know, it seemed to have a lot of facts. Either the guy was a very, very competent creative writer, or it was true.

Leo: So any big security updates? Any Windows updates? Anything going on out there?

Steve: The big news of the week, of course, is Google's new browser.

Leo: Chrome.

Steve: Yeah.

Leo: I've been using it. I like it.

Steve: Yeah, well, we have - there was a ton of people who wrote in. They went to GRC.com/feedback. And I want to continue to encourage people to do so and really to thank everyone who does because I get a lot of great ideas and tips and pointers and a sense for where our listener base is and what they want to hear about. Everyone wants to know what I think about the security side of Chrome...

Leo: Of course, yeah.

Steve: ...and what Google has done. So, of course, this is only a couple days ago. I have had no chance yet to take a good look at it. In fact, when I got your email, Leo, saying hey, I got back early from the airport, you want to do our recording now, I was just in the process of creating a new VMware box...

Leo: Oh, you are paranoid.

Steve: No, it's not that as much as I don't like to install things that I may regret installing. Because Windows is way better, XP now is way better than earlier versions of Windows in removing the junk that gets installed. But it's like, eh, it's just sort of wear and tear on a Windows system. So for something that I'm not at all sure I won't immediately say, oh, I'm glad I didn't install that on my actual hard drive, I just stick - it's so easy to create a little VMware world and stick it in there and use it there. And there are places where it turns out you have to. For example, when I was working on all this cookie stuff that I'll be returning to once I get the DNS stuff put to bed, Firefox 2 and 3 cannot coexist on the same machine. And interestingly enough, Firefox 2 and IE have cookie interaction.

Leo: Oh, that's really surprising.

Steve: There's some cookie collision. It was, like, bizarre. I thought, what...

Leo: You didn't expect that, yeah.

Steve: You know, I thought it was my problem. But anyway, so I've got little VM worlds for everything because in many instances you need different versions - in fact, I've got IE 5, 6, 7, and 8 also in different VMware because, again, IE can't - different versions of IE won't live in the same machine, either. So it's very useful. But anyway, that brings me to a point. So just to wrap up the issue on Chrome, we absolutely will do an episode. The early news is there are some problems. Naturally, unfortunately, Safari remains - Apple Safari remains the only browser to, by default, have third-party cookies disabled. Google's are enabled. It does provide you with the option.

However, the guys in my newsgroups immediately determined that - using my not-yet-public cookie analysis system - that Google is also subject to what's called "cross-context leakage," meaning that it does not block outbound cookies, it blocks them inbound. Which is really not what you want because it means that if you were to get a cookie in a first-party context, like you went to a site, like for example PayPal redirects you through DoubleClick and then back to PayPal, well, in that redirection hop you have a first-party relationship briefly with DoubleClick, during which time, if you allow first-party cookies as you typically do, you would get one. Then, unfortunately, both IE and Safari and Chrome, they block incoming third-party cookies, not outgoing third-party cookies. Which means that then, even though you've said I want third-party cookies blocked, when you are at other sites you're leaking DoubleClick third-party cookies, which...

Leo: That's not good.

Steve: ...is not what you intend. So, and I also noted - I haven't even gotten it loaded yet. But I quickly, from the initial comments I saw in the newsgroups, there is no site whitelisting/blacklisting for, like, cookie handling and maybe other provisions. Again, I haven't looked at it closely, but that...

Leo: No, and even the setting for third-party cookies is a little odd. It says...

Steve: Yes, it's got some strange wording.

Leo: It says restrict how third-party cookies can be used. Not block third-party cookies. And then it doesn't give you a policy, doesn't say how to edit the policy. It just says, you know, restrict how they're used. Well, I don't know what that, you know, what does it - what restrictions am I placing on it?

Steve: The most compelling concept is that they are talking about sandboxing. They're saying that individual tabs are - they essentially create browser instances per tab so that, first of all, if a tab crashes, you don't crash the whole browser. And that does happen in IE where it's like, oh, now I'm hosed, and I've got to shut down all of IE. So that's good. But they are also talking about restricting what the code in this window can do. I mean, they're using the term "sandboxing." So the question is, okay, what does that really mean? The other thing that I liked is, in fact I just read when I was going through the notes for today's Q&A, someone talked about - in fact it was a comment about Chrome, hey, I like how quickly it launches. He said, I don't ever launch Firefox because it takes so long to start up.

Leo: Yeah, Chrome just pops up, wow.

Steve: And I was thinking, what? And it turns out, then he confesses, he's got so much add-on gunk...

Leo: It's the extensions, yeah.

Steve: Yeah, he's loaded so many extensions in Firefox that it's slowing it down. And he says, I don't load Firefox unless I know I'm going to be surfing for at least 15 minutes. Otherwise, you know, it's not worth waiting for it.

Leo: Or take out something. That's not a fair comparison at all since no extensions exist in Chrome at all.

Steve: Well, but there will be add-ons and plug-ins. And they comment that the sandboxing could be defeated by plug-ins and add-ons that would be crossing that boundary. So that's something to be concerned about. But also apparently there's some sort of process monitor where you can see how much RAM each of your different pages and/or plug-ins and add-ons are taking up. So they're enforcing some accountability so you can say, oh, look how fat that page is versus this page.

Leo: Oh, even more than that. According to the comic book, anyway, you can say, if a process fails or causes a problem, you can say who did it, which you can't do in Firefox. And that will really help in eliminating the buggy extensions.

Steve: So at this point...

Leo: And it's multithreaded. Which you ought to love. You've got that four-way Xeon that doesn't do anything.

Steve: Sitting around, give me something to do.

Leo: Well, hey, I think a multithreaded processor, I mean, that's where you're seeing a lot of the speed improvement.

Steve: Yup, yup. So we got Chrome, and we'll be doing a comprehensive analysis of it. I wanted to mention that a number of different news outlets covered the increasingly good news for people, which is increasingly bad news for the likes of NebuAd and Phorm. NebuAd has lost their CEO. He wandered off to go somewhere else. But they've apparently also lost all their customers.

Leo: Ah-ha.

Steve: Like, yay.

Leo: Couldn't happen to a nicer bunch.

Steve: And Phorm's stock has fallen 75 percent since its peak, which was 11 days after their announcement. Everyone figured out what was going on, and it just collapsed. So it's like, good.

Leo: That's encouraging because people who say, oh, get over it, privacy's dead, you're never going to be able to have privacy ever again, there's an example of, if people are aware of it and stand up and say we don't want this, we can actually defeat this stuff.

Steve: Yes. And, I mean, and again, it's a perfect example of, okay, no one would have a problem with this if it was opt-in. That is, if people voluntarily signed up in return for some benefit to them. Instead this was all on the benefit of the publisher that was going to be getting higher ad revenue on the promise that the advertising would be more tightly targeted, and therefore they could get a higher dollars, CPM dollars. So anyway, the good news is these guys are falling on hard times fast because there's enough awareness now and enough concern about privacy and security that they can't, you know, they couldn't sneak around under the cover of darkness and get away with this.

And then lastly, I did want to mention to anyone else who's using VMware, when I fired my VMware workstation up, it said, hey, it's been a while since we checked for updates. Actually it's been a while since I fired it up, so it hasn't had a chance to check for updates. When I did, I found there had been a change. I was using 6.0.4. We are now at 6.0.5. And one of the things that they have done, it was a security update largely. There were three major things. But one thing they did I really liked. It wasn't a bug fix. It was a policy fix. They are setting - VMware is now setting the so-called "kill bits" on all of their ActiveX controls. So in VMware they are using ActiveX controls as just part of their object glue for their solution. But they recognized proactively that, much as is the case for all ActiveX controls, and we've discussed this on a number of instances in the past, IE can be asked to invoke ActiveX controls that exist, even if they were never designed to run in IE, in order to exploit any behaviors, not even necessarily any problems, but behaviors. And you might imagine that VMware has some powerful ActiveX controls.

And so they said, okay, we're just turning on all the kill bits on all of our controls because none of them were ever meant to be used in Internet Explorer, so we're going to prevent them from being used in Internet Explorer. Which as a policy is brilliant, and everyone should do it. I mean, anyone producing an ActiveX control which is not intended to be an add-on or a plug-in to any browser, ought to go to some lengths to make sure theirs can't be exploited. It just - it makes sense for them. They'll avoid the bad press of being part of some exploit. And it certainly makes sense for any end users who would like to be using these controls safely.

Leo: Yeah. Yeah, absolutely. Do you have any - you mentioned at the beginning, and I want - is this a good time to bring up the SpinRite thing?

Steve: Sure.

Leo: Because, you know what, we're subject to this kind of mail all the time, you know. And you never can really validate that it's true or not. So as I'm listening to you last week I'm thinking, boy, this is a really amazing story, but who knows if it's true. Did you have people write in saying, hey, I was a Navy SEAL, this couldn't be true?

Steve: No. I heard both ways. Some guy who was just Mr. Sour Grapes wrote to the office, and Sue forwarded it to me, saying oh my god, how gullible could you possibly be? I'm not going to believe anything you ever tell me again. And it's like, okay, well...

Leo: There was no evidence either way.

Steve: Thank you for your email. Actually I didn't bother responding to him because, you know, he's made up his mind. Yeah, I mean, there was no evidence either way. Our listeners know, based on the testimonials that they have written and that I have read, that it's entirely possible. I mean, it could have happened. It's not...

Leo: Oh, sure. Yeah, there's no question about that.

Steve: I mean, you know, the space station has a copy of SpinRite because they've had problems with their laptops when they're in orbit, and it's a little hard to send the drive to Fry's or to go pick up another one. So, I mean, it works. We know it works. And it would be very cool if this were true. I hope it was true because I would love the idea that it was helpful in the field. And I mean "in the field."

Leo: Yeah, really.

Steve: Really in the field.

Leo: Yeah. Well...

Steve: My email that I got this week, it was written by someone who heard us last week, and the subject was "SpinRite Saves Many Lives." And this is way toned down. I don't think anything will be the same as last week's. But he said, "Hi, Steve. Yes, SpinRite saves lives. Or saved lives. I work for a large medical group, and we have lots of doctors who read X-rays from their homes after hours. One day last week one of our doctors called me and stated that his computer would not boot up and was stuck in the Windows screen. He was going to need it the next day to read X-rays from home for a large hospital. So I started SpinRite on his machine before I left for the day. Like magic, when I returned it to him the next day, it was up and running perfectly. You saved me many hours reloading Windows and various programs with tricky configurations. I called the doctor to let him know how great your program is and how much time you saved me. Thanks again, Steve."

Leo: Well, there you go. See? It does save lives.

Steve: So, well, a little less dramatically this week than last week, but yes.

Leo: It cures broken bones.

Steve: It does.

Leo: Well, that's great. And, you know, there's no way of knowing one way or the other whether a story like that is true. And, you know, we're not gullible, but we don't have any reason not to believe it, either, so...

Steve: Well, yeah. And we could call it well-written fiction. I don't want anyone else to do that. Please do not send...

Leo: Do not make up stories.

Steve: Do not make up fantastic-sounding SpinRite stories. You know, then I'll start being suspicious. So I'm not soliciting that at all. I would rather - all I want is real testimonials from real life. I think next week I'm going to tell how SpinRite saved 200 kittens. So that's...

Leo: Is that a true story?

Steve: Yeah, yeah, yeah, I have it.

Leo: Oh, we're getting out of control now, I've got to tell you.

Steve: Okay.

Leo: Speaking of reading, Steve, I'm going to - you have to listen to these as I read them to you. How about that? And answer these questions.

Steve: You're going to be audible, Leo.

Leo: You're going to be an auditory listener.

Steve: Yeah, you're definitely audible. I'll be an auditory listener.

Leo: Auditory listener on this one. Question numero uno from John Skauge in Bergen, Norway. He says he's not SATAsfied with SATA. See, there's a visual pun you might not get if you just listen to it. Hi, Steve and Leo. Love your show. I've been listening to it every day when I ride the bus to work since May of this year. I've had two new Samsung SpinPoint F1 1TB SATA2 drives. One of these drives crashed after a week of normal usage. The other one lasted longer but started to disappear from the system, at random it seems. I also have two Samsung 250GB drives which work fine, something SpinRite also tells me. Now one of my 250GB drives has started disappearing from the system as well, but SpinRite reports surface scanning level 4, which I also used on the terabyte drives, to have no faults on either of the 250GB drives. Currently both drives seem to work after restarting the system a couple of times.

I recently upgraded my machine. My setup, except for my hard drives, is a Thermaltake Toughpower 850-watt power supply - wow, 850 watts - and an Asus Geforce 9800 GTX with 512MB of VRAM. Could the new power supply be responsible for the behavior of two new drives, or just bad luck on my part? My old PSU was a Tagan with 480 watts of power. Why are my drives disappearing, he asks?

Steve: You know, it really does sound like a power supply-related problem.

Leo: Really. As opposed to, say, an OS problem?

Steve: Yeah, I mean, I'm not sure, when he says his drives are "disappearing," what he means. I mean, I've had - I mentioned to someone else that I had been unimpressed with the design of SATA connectors.

Leo: Yeah, they fall out really easily.

Steve: And, yes, wouldn't you think in this day and age, Leo, well...

Leo: A locking connector, please.

Steve: Well, now, of course the tradeoff was that the SATA, the connector spec was designed to be hot-swappable.

Leo: Right, right.

Steve: So they're hot-plug connectors, the idea being that you don't need a case or anything else around the drive. Basically you just - you put the drive on rails or you use a case where the drive just slides in with a little, you know, a minimal enclosure around it. And so the drive itself plugs into the back plane where you're going to have your RAID or whatever. So they were, you know, they were trying to come up with a low-cost solution. But I'm very unimpressed with the SATA connector that was designed just in the last couple years. It's like, oh, please, guys. You know, and you're right, why couldn't you do it - when you have a cable connection, why not have some optional latches on the side so that a cable plug to a SATA drive would lock in and hold itself?

Leo: How hard is that, yeah.

Steve: Because I agree, they're just not very stable. So that was my first thought. But when he talks about restarting the computer a few times...

Leo: That shouldn't fix it if it's a connection that's bad.

Steve: One of the things that people should be aware of is that, you know, he's got some high-speed, large, 1TB SATA2 drives. These contemporary drives are using more power than older, slower drives. And it can be that if power supplies are not beefed up in concert with increasing - for example, this GeForce 9800 GTX, that's probably got a couple hard drive connectors on the back of it, too, because it can't get enough power just from the motherboard. You know, the higher end of graphics cards, as I'm sure you know, Leo, they have their own hard drive connectors on them.

Leo: Oh, yeah. We had to buy a 1,200-watt power supply for UGM. 1,200 watts. That cost as much as a PC. It was 600 bucks.

Steve: So he's got a really high-end card that's probably got a couple hard drive connectors on it just for the video card. And it sounds like he's got four drives. He had a pair of SATAs and a pair of Samsungs. So it may very well be that his power supply either was or is, you know, not footing the bill. And these things are all made now in Taiwan or China. They're certainly checked initially. But you could also just have a bad, you know, like from the factory, an infant mortality problem with a power supply. Which is it's got, you know, high hum or bad regulation on the 5-volt or at the 12-volt line. His motherboard may be pulling a lot of power, too. So I would, I mean, this seems like something not about the drives but more like, you know, something the drives need. And what they need is power.

Leo: That's interesting. Huh. I've also seen the operating system lose drives. We get complaints all the time about Windows losing drives. So, yeah, who knows, with that one, who knows what it is? But it doesn't sound like there's anything wrong with the drive itself; right? I mean, that's the result of that SpinRite test.

Steve: Yeah, right, exactly. And if you power it down and up a few times, and then the drive comes back, it's like, okay, well, now, you're also restarting Windows a few times, so Windows is coming back. So maybe Windows has forgiven the drive. It just - it is difficult to know. But certainly we sort of take power for granted. And with graphics cards that now need two hard drive connectors of their own, and motherboards that are becoming more and more power hungry, where you've got that extra yellow cable to give it [indiscernible] 12 volts, it's the case that power is becoming really important. We're just sucking a lot of it. And heating our rooms, too.

Leo: Yes. I've got the AC on high today. Man, this stuff generates a lot of heat. A lot of heat. And now a public service announcement from Spencer B. in Utah, USA: Hey, Steve and Leo, I've been getting about five emails a day from GreetingCard.org. The URL in the message links directly to an EXE file called "e-card.exe." I know this is a huge problem. I thought it would be a good thing for you guys to know about it. Love your netcasts, listen to them devoutly. Keep up the great work.

Steve: I wanted, I mean, this is certainly an obvious thing for all of our listeners. But I thought it was just worth reinforcing, not so much for the people who listen to this netcast/podcast, but for them just to take a moment to make sure everyone they know and care about sort of thinks about this. I know that greeting cards are - unfortunately, it annoys me because my mom and some less tech-savvy friends of mine...

Leo: Yes, me, too.

Steve: ...are sending me these things all the time. And what pisses me off, frankly, is they're putting my email address into some third-party site that sends me the card. They're not sending it to me directly. They're like, oh, you know, would you like to send a card to Steve? It's like, yes, I would, here's his email address. Well, of course now the greeting card website has my email address, which is something that I guard and tend to treat as my private information. I don't want it spread around because that's of course how spam happens.

But more importantly, some of these cards, they really are nice. I mean, they're really beautiful Flash animations. I mean, it's like, okay, I can understand why somebody sent me this. It's an impressive, nice piece of work. The problem is this concept of greeting cards is becoming popular. And so an evil site like this GreetingCard.org, or that may just be a completely made-up site, but someone pretending to send email that is a greeting card sends you this link, and you're had success with it for the last ten times you've opened a greeting card, suddenly you click on this and, bang, you're infected with whatever malware this EXE file is installing on your machine. So...

Leo: Do we know it's malware, or just presuming because it's an EXE file that it's malware?

Steve: You're right, we don't know it's malware.

Leo: I mean, it could be a greeting card.

Steve: Get out your copy of VMware and fire it up, yeah.

Leo: Right. I mean, on general purposes I don't even, when my mom sends me these e-greetings, I don't open them. I'm sorry. You know what really bugs me is not merely that she's sending me this link in an email, which as we know is bad, but also that she's given my email address to some other third party without permission.

Steve: Yup, yup, yup.

Leo: I try to educate people on the radio show about this, but I have not high hopes.

Steve: It's worth also mentioning that there is a very high level of email now, just spam, which is reputing to be a misdelivery of a package, FedEx in particular, but also DHL and UPS, where the email says we attempted to deliver a package to you. Please click this link to open the invoice so you can see the details, who it was from and so forth, and we can arrange to reschedule delivery. And it's catching a lot of people who are like, oh, no, I missed a box of something? I want it. Again, it uses an emotional hook, something people, like, oh, someone sent me something, I need that, instead of something we don't care about, like...

Leo: These guys are really good at social engineering, at tricking you into doing something you don't want to do. It's just really the - it's the sad state of the world. And you've just got to educate everybody you know. I just say, you know, don't open attachments, don't click links in email.

Steve: Yeah. And I tell my friends not to send me anything.

Leo: Yeah, exactly.

Steve: Please don't.

Leo: Exactly. Lil Banchik, like that Lil Banchik in Long Island, New York, wants to know how long to wait: Steve, I've heard you say over and over, nothing is secure until people have had time to pound on it, to discover weaknesses. With Google's new browser, how long - again we're back to Chrome - in your opinion would be long enough, especially since the fine print in the EULA states that Google is allowed to install updates and patches at any time without warning. How long? How long, Steve?

Steve: Well, part of what Chrome is doing is interesting because Google has said that they will be providing the browser with a continually updated list of bad sites. So they're going to have a blacklist, essentially, in Chrome. And Chrome will be pinging Google for continual updates to that. And of course they're going to be doing security patches and so forth. So that's good. You know better than I, Leo. I mean, I know from our listeners this is immediately on everyone's radar. So in general is Chrome succeeding? I mean, has it been...

Leo: Well, everybody wants to use it. You know, of course, it just came out yesterday. We're recording this on Wednesday. It came out Tuesday. I downloaded it, everybody downloaded it, there's some really obvious great things in it. Although I think people are really concerned about the EULA, particularly the part about the EULA which says, even though you retain copyright, we retain the right to do anything we want with content you post using this browser and to distribute it to third parties. So that would mean, I guess, your email, your blog posts. That's a little scary.

Steve: Content you post with this browser?

Leo: Yeah. Isn't that a little creepy?

Steve: Wow.

Leo: You want me to read it to you? This is very creepy. Now, of course, I think - and I'm going to give Google the benefit of the doubt. This is the kind of language they put in EULAs to protect themselves against being sued by somebody who says Google, stop caching my data, because these things happen. But it says you retain copyright and any other rights you already hold in content which you submit, post, or display on or through the services - in other words, Chrome. By submitting, posting, or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and nonexclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any content which you submit, post, or display on or through the services. Furthermore, you agree this license includes the right for Google to make such content available to other companies, organizations, or individuals with whom Google has relationships for the provision of syndicated services and to use content in connection with the provision of those services.

Steve: See, now, you're using the term "services," though. Are we sure that that's not their online web-based things to which people would be posting content? Because there I could see everything you've said makes sense. If it's like, you know, Google Calendar or some blog where you're posting content to a Google-hosted web facility, as opposed to through the browser, using the browser as a conduit.

Leo: You know, I'll have to go back and look at the part of the EULA where they define services. And it may be that they are - I don't see why that would be in the EULA for Chrome, however.

Steve: So explain to me, what do you think the excitement is? I mean, we have Firefox and huge adoption of Firefox. And it's popular and been pounded on. We're at v3, and 3 looks good. What's the attraction of another browser?

Leo: By the way, "services" refers to Google's products, software, services, and websites.

Steve: Wow. That's nuts.

Leo: Everything. Everything. The attraction is several fold. I think, you know, we had this debate yesterday on MacBreak Weekly. And Merlin Mann was very adamant. Why do we need another? But let me tell you why Google's doing, I mean, one credible reason that I think shines some merit on Google is that they want to have a browser that does really, really well on cloud computing.

Steve: Yup, on Google sort of stuff. Because clearly we know that so far basically all of their services have been hosted through other people's browsers, through IE, Firefox, and Opera.

Leo: Right. So if you use Google Docs, or you use Gmail, or any, frankly, any JavaScript-based web application, it runs much better in Chrome. They are using a very, very fast JavaScript engine. It's the fastest one out there.

Steve: Ah, interesting.

Leo: It also is the only browser I know of that's multithreaded. So that speed is not phony. It's real speed. And it also has built-in Google Gears, which means when you're not online these cloud computing programs like, say, Google Docs, still can be used, still persist. And of course that's very important. So all of these things they feel - I think they could credibly say, look, we just don't feel other browsers do a good job of this, and we want Google Docs to succeed, so we're going to make the browser that this stuff needs.

Steve: Well, I do know that it looks pretty clean. I mean, it just has a nice, simple, clean...

Leo: Beautiful. It's Google, yeah.

Steve: ...interface. I really like that.

Leo: But then many others point out, yeah, but what is Google's real business, it's advertising. Google is essentially creating a giant spy on your system.

Steve: That's a concern, too, yes.

Leo: That's a completely legitimate concern. So, you know, I'm torn over this. And I have to say that EULA is just - might be the thing that puts me over the top. I think they put it in there because they don't want to get sued over caching, which they have been before.

Steve: And depending upon where the SSL happens, I mean, if you're using an SSL connection, then even though you're using their browser as the portal, I guess they could scrape it off before their browser encrypted what you posted. I mean, they certainly could. But I don't know, I mean, that does seem a little too all-encompassing, too sweeping as it's written right now.

Leo: Yeah, I see these EULAs all the time, and people are always complaining about them. It's not at all uncommon to have these kind of blank, you know, the lawyers are going to say, look, we're going to protect you against all exposure, so you'd better put all this wording in there. But what they don't realize is some people do read the EULAs. And in this day and age, all it takes is one person with a blog to read the EULA, and everybody knows about it.

Steve: Yeah. Well, all of our listeners do now.

Leo: They do now. Ryan Sullivan, attending college in New York, wonders about the campus network security: Hi, Steve. I'm a freshman in college - I guess he's just going to school now - an avid listener, so of course I want to make sure I'm secure on my college network. Yes. I don't know much about my college network other than it's a Cisco network. Everyone has to use their college email address and password to log in via VPN over IPSec/UDP to get access to the Internet on campus. I would assume this is a good way of keeping unwanted people out, even though it's single-factor authentication, especially since my college makes us change our passwords every 60 days. But what I'm more concerned about is the other students on the network. I go to a very high-tech college, so most students know their way around computers very well. I want to know, how can I be safe on my college network? Is there any way another student already on the network can do anything to me or get any information on me? Or am I just being paranoid? Thanks for an amazing show. Keep up the great work.

Steve: I thought this was a great question because it leverages a lot of what we've talked about and learned over the years of the podcast. First of all, I'm impressed with wherever it is he's going. He doesn't tell us where he's going in his note. But essentially this means that every single student must have presumably the Cisco VPN client installed on their, you know, the computer in the dorm room or on their laptop, and that literally all the traffic, all the student traffic, at least, crossing the Internet on the campus network is encrypted. So Cisco's got good, state-of-the-art VPN technology. It means that in order to get on the campus network at all, you need to log onto their VPN client that establishes an encrypted connection to a back-end VPN server which is the way you're able to get out then onto the Internet or onto the campus's own Intranet.

So the only vulnerability is, because all the traffic is encrypted completely on the 'Net, the only vulnerability is, as he says, as Ryan mentions, the single-factor authentication which is occurring at his laptop. So it's his laptop that he wants to protect. I would say use, for example, a power-on BIOS password. It's somewhat annoying, but it is stronger than using a Windows password. And you probably want to use a Windows password also because it is the laptop which could get, for example, a fellow student could install a keystroke logger in order to capture Ryan's authentication as he's typing in his username and password. And that would allow somebody else to pretend to be him. And it very well may be that the campus is logging the network activity per student based on their log-in credentials. So you want to probably prevent someone from being able to impersonate you to the rest of the people on the campus. But the only real point of vulnerability that I can see is at his laptop and his own log-in credentials. It's, again, it demonstrates strong security policy that the campus is also enforcing a 60-day password change. I mean, that's...

Leo: Yeah, that's amazing, yeah.

Steve: I mean, it's teaching all of the students good security practices, which is good to see. You can imagine when they eventually wander off into the corporate world, if someone says, oh, yeah, we never bother changing our passwords, it's like, what? You don't change them every 60 days? We did that when I was a freshman.

Leo: Yeah, even in college. I think what he's saying, though, is it's that age-old issue of when you're on a network, if other people can get into your system. In other words, because you're on a shared network, don't they have unusual access to your hardware? Or does a VPN prevent that? So when I go to a hotel - we talked about this the other day. And I used the hotel's network. Everybody else in the hotel, unless they've done something special to segment it, can see that I'm there. And anything I'm sharing is visible to them. They're on my Intranet.

Steve: Yes, if you don't have encryption. But the VPN...

Leo: Because we're using VPN it's safe.

Steve: Exactly. You have encryption from you to the VPN server. Now it's not clear at that point, once it becomes decrypted, then is there visibility to other laptops or other machines on the network? It might well be, for example, that you could still scan the network. Your scan would go through the VPN tunnel, come out the other end of the VPN tunnel, and then start sniffing around for IPs. I mean, it's a function of, like, where have they installed NAT? Is there NAT also going on so that everybody is also behind a implicit NAT router? So again, you're able to get out into the public segment, but then not back into individual private connections. So there's more that we don't know about how this is set up. But at least the traffic, no raw packet sniffing would function on the segment of the network that the students and faculty have access to because all of that, by virtue of policy, is going to be encrypted. And that's really great.

Leo: Makes sense. Martin Nothnagel in Berlin, Germany mentions that Microsoft is determined: Hi, Steve. I'm a longtime listener. I just want to drop you a short comment. In the last episode you and Leo talked about DEP, and that after Microsoft providing the base for secure software it is now the responsibility of the ISVs - the Independent Software Vendors - to develop DEP-compatible software. I just want to bring to your attention that Microsoft has some ways to force these vendors to use DEP.

For instance, the Windows Logo Program Requirements and Policies state - this is that thing, if you want to sell software that says, you know, "Certified for Windows." In the category of image printer drivers, the requirement is printer driver components run with Data Execution Protection enabled and with UAC, User Account Control, enabled as a non-administrative user. So in this example, to get that Windows Logo Certification, printer drivers shipping in 2009 or later must be able to run with DEP enabled to become a driver signed and certified by Microsoft. It is a long-term process, but Microsoft is slowly tightening the thumbscrews.

Steve: Yeah, I liked this. And I had forgotten to mention that, that Microsoft is, for example, that policy you just read is effective June 1, 2009. So everyone has plenty of time. That's a year from now. But Microsoft has made it very clear that, you know, everybody get your act together. If you want us to sign and certify your drivers - and as the OS tightens up, of course, signed drivers is going to become a requirement also.

Leo: Yeah, it already is in Vista 64-bit, yeah.

Steve: Exactly. So, I mean, this is a good move. And I was wondering if, you know, didn't this mean, or does it mean that, long-term, Windows will end up being more secure than the open source platforms? And because the open source platforms by definition don't have these kinds of enforced requirements. And I think that, while that may happen, in general Microsoft is just educating the world. They're raising the bar, and if nothing else they're finally setting an example for some things that can be done right by policy. It's always necessary to excuse them for making mistakes. Anyone can make mistakes. Microsoft has made plenty of them. But still, they're saying, look, this is the way things need to be done. And so you can imagine that the non-Microsoft OSes are incented then to say, oh, we have that, too; we're doing that, too. We're working on enforcing these policies and technologies which are clearly beneficial to security. Because it would be bizarre, frankly, if Windows became the most secure operating system in the world.

Leo: But not a bad thing. I'm all for it.

Steve: Not a bad thing.

Leo: I'd vote for it. It's only right, if it's the most used operating system in the world, that it become the most secure operating system in the world.

Steve: That would be nice.

Leo: Don't think I'm rooting against that by any means. Kashyap in Hyderabad, India - wow, I love it that we have such an international audience - had a request for Security Now!. He says: Hi, Steve. I'm a security professional working in India. We would be extremely grateful if you could enlighten us in depth on the less known but very effective cross-site request forgery.

Steve: Well.

Leo: Well.

Steve: This question, as I was reading the mail, I thought, wait a minute, you know, we did a whole episode on that.

Leo: We did?

Steve: Well, on cross-site scripting, which was the same sort of thing.

Leo: Oh, it is.

Steve: Yeah. And so I want to take this opportunity to let this listener and all of our listeners, to remind them that GRC now has a site-wide search and a Security Now! search, that is, that you're able to restrict. And for curiosity, I put GRC.com in. Right there on the page in the upper right-hand corner was a search box. I put in "cross-site scripting," hit the Search button, and there was, like, PDFs and text pages and references to our podcasts. I mean, so I just sort of wanted to give people a heads up, not about this topic, but about anything that they're curious about. You and I now, Leo, have been doing this for 160 weeks. We've covered a huge range of topics. Elaine has transcribed them all. Google has found them all and searched and indexed them all. And so if you just go, if you're wondering about some topic in security, GRC.com, and just put your question into our search box. And it will instantly find for you our presentation on those topics, both in audio format and in text format.

Leo: It's a great resource now. I mean, with that many shows there's just no end of stuff. So cross-site request forgery is basically the same as cross-site scripting.

Steve: Yeah, it's just a different term for the same concept.

Leo: Okay, got it.

Steve: And we did a beautiful podcast.

Leo: I remember, yeah. I remember, yeah. Terry Voth in Toronto, Ontario would rather WPA than WEP. Well, who wouldn't these days? He says: My son got a Nintendo DS - oh, I see the problem already - probably the biggest driving force in North America to run WEP, since it won't run under any other wireless security mode. Fortunately the podcasts had me trained well enough to flinch when my - I can just see it - when my son asked me to switch things to WEP. Maybe if a Pavlovian response describes an involuntary response to a potential reward, we should call a Gibsonian response an involuntary response to a potential security threat. I like it. I had a Gibsonian response.

I recalled the Y configuration that Steve suggested - that was with three routers - looked at the two working wireless routers I had, and started scheming on a way that I could get WEP up and running without buying a new router. And maybe I have it. All right, so let's visualize this now. This is let's see how good an auditory learner you are. All routers I've bought recently, all Linksys, have had DMZs, or demilitarized zones. That's where you take a part of the network and say, hey, you're just outside the bounds of the router. Any traffic can come and go. What if I hooked up my secondary/WEP router to the DMZ port of the primary/WPA router? If I understand it correctly, nothing from the DMZ WEP will have access to the rest of the network. We can still use the secondary router's firewall, protecting from the WEP network from the Internet. The only risk I can see is the neighbor hacking in, using my bandwidth, stealing my son's Pokemon. Tragic, I'm sure. But considering my financial and identity information are safe, I think I could live with it. Any holes I've missed? So he's saying you don't need to use three routers in a Y configuration. You could do two. Is he right?

Steve: No.

Leo: Yeah, that's what I thought.

Steve: No. Unfortunately, first of all, the DMZ port is sort of a - is a new extra feature that some routers have, which is like a lower configuration responsibility for the traditional DMZ configuration. Now, a real - and all of these are sort of poor man DMZs. As you stated it, Leo, a real DMZ, short for demilitarized zone, a real DMZ on an industrial strength real firewall is its own interface, essentially on its own network, which is outside of the network that you're wanting to protect. And there's inherently no traffic flow from the DMZ back into the other interface of the firewall, and those are policies enforced by the firewall.

Unfortunately, these consumer routers have a - they're really misusing the term "DMZ." All it really means is that unsolicited traffic goes to that port, or to that IP address. Traditional DMZs have been software-configured in the router interface, the idea being that you may have wanted, for example, to run a web server or an FTP server or some kind of traditional Internet service that you wanted to make available to the outside world. Well, that inherently means that your router, which would normally block unsolicited incoming traffic - remember that, as we've described NAT routers many times here, the way a NAT router works is that only by traffic egressing from the internal network to the outside is a path created, a little bit of memory in the router that allows traffic returning from the exact same destination to be routed back to the same computer in the private network which originated it.

So the idea is that unexpected traffic, unsolicited traffic, hits the router. The router inherently has no expectation of receiving it. That traffic, because it's unsolicited, wasn't the result of initial outgoing traffic that created a return path. So what - inherently a service, any kind of a service on the Internet is by definition a recipient of unsolicited traffic. Google doesn't know I'm going to be sending them traffic. I just do. And because they're a service, they accept that unsolicited traffic and respond to it. So the idea was that this so-called "DMZ" was initially set up in routers where you could configure, manually configure one of your machines' IP addresses to receive that DMZ traffic.

Now, it gets a little tricky, though, because you are normally configuring a certain IP to receive unsolicited traffic, saying this computer runs this service. I want it to receive unsolicited traffic. The problem is, routers assign IP addresses based on pretty much the order in which machines appear as they're powered up after the router is on. It uses DHCP to assign them. So the problem is that, if you configure an IP to receive traffic, you need to make sure that that computer is always at that same IP. There are ways to do that. You're able to assign IPs to MAC addresses, the MAC address being the hardware address of the computer's Network Interface Card. So you bind an IP to the MAC address, and then you bind this DMZ routing to the IP.

Anyway, you can see how complex that is. Imagine if you simply had a hole on the back of the router that said "DMZ Here." Well, in that case, all those problems are solved. You can simply plug the computer into that hole which is the DMZ port, and by virtue of the preconfiguration of the router, it will receive unsolicited traffic. So you could see that this has become a popular feature on some consumer routers.

Leo: Oh, so when he says "DMZ port," there really is a DMZ port.

Steve: Yeah, exactly. It's a DMZ port.

Leo: Oh, because I'm used to doing it, kind of assigning it to the - by IP address.

Steve: Exactly. And so this is a feature that he's talking about. The problem is, it's not on its own net. It's not on a separate network. So you've still got the problems that allow this to be exploitable. I'll remind people that WEP, the security - the so-called "wireless security" that made Terry flinch when his son said, "Hey, Dad, can we change our home network to WEP because I want to put my Nintendo DS on the network..."

Leo: His Gibsonian response.

Steve: Yeah, his Gibsonian response was, "Uh, I'd rather not, son."

Leo: No, no, sorry, no, no.

Steve: Anyway, so the problem is that WEP is really badly broken. In fact, that was the last topic, the last show we did on that was really "[Even More] Badly Broken WEP" because now it takes less than a minute to crack the key using freely available software that's available on the Internet. So anyway, the problem is it's only by performing true subnet separations, where the nonsecure network is on its own subnet, and those two subnets, the secured and the unsecured, are joined by a third, that's the only way to prevent cross-network leakage because there are, again, freely available tools that will allow you to do ARP spoofing, Address Resolution Protocol spoofing, which essentially allows somebody across the street to pretend to be the gateway for your network and receive all the traffic coming to and from your entire household.

So it's really something you want to avoid. And I don't know of any way to do that securely, and I've spent a lot of time thinking about it, except to have three routers - one that does the Y'ing function, and the other two to just do NAT'ing function - to essentially create one-way valves. And because ARP traffic is always constrained within the local network, ARP traffic never crosses a router boundary unless it's specifically set up to do bridging, which is not something that any consumer routers are able to do.

Leo: Okay. The Y solution would solve it, right, the three-router solution?

Steve: The three-router Y configuration would. And I will mention that routers are now so cheap, you know, I mean...

Leo: 40 bucks, another 40 bucks, dude.

Steve: Exactly.

Leo: And there is, and I think this would work, too, Nintendo sells - no, maybe it wouldn't work. Yeah, maybe it would. They sell a little USB WiFi key for use with the DS. And the idea is you plug it into a computer's USB port, and it shares the computer's Internet access with the DS. So, but I think that wouldn't solve the problem because - no, it wouldn't.

Steve: Well, because what you've done is...

Leo: Connected to the computer.

Steve: Well, yeah, you have just created a probably very insecure hotspot wired into that machine.

Leo: Right into your computer, yeah. So don't use that, either. And I presume that any newer hardware that has WiFi is going to support WPA. The DSes have been out for a while, and that's why it doesn't, I'm sure.

Steve: Well, and...

Leo: Is it cheaper? Is it cheaper to implement WEP than WPA?

Steve: No. It's just history, really. Because remember that WPA also uses RC4, which is a very lightweight, I mean, RC4 is a fantastic crypto. There's nothing wrong with it except that it was done wrong, it was implemented wrong in WEP. So that, for example, if you just throw away the first 256 bytes of pseudorandom data that RC4 generates, RC4 is a pseudorandom stream generator. But because it uses mixing within a small pool, that pool doesn't randomize itself initially. And that allows for bad keys to be created, which are, like, extra nonrandom. And because we know the beginning of the packet contents, by taking all that together, both the white hat and the black hat security guys have figured out how to just crack it. But all WPA does is fix those implementation mistakes, so it is not more computationally difficult to implement WPA. I think that it just wasn't a big enough issue. And I'm glad that we're making it a bigger issue because, boy, toys like the Nintendo DS need to be able to support the same security that the rest of a security-aware household is running.

Leo: Edward Hanson in Rexton, New Brunswick, Canada switched to OpenDNS. We were talking about that the other day because of the DNS vulnerability. He says: Hi, Steve and Leo. Several years ago, as soon as it was available in my area, I upgraded from dialup to DSL for my Internet connection. I then added a D-Link DI-604 router to the mix after hearing you tout the benefits of routers on Security Now!. Up till a few weeks ago when I heard your discussions about DNS, my router had been configured to use my ISP's DNS settings. Since then I've reconfigured it to use OpenDNS. That's where my question comes in. For some reason, maybe because it's an old router, the only way I could manually enter the server addresses for OpenDNS was to toggle from Dynamic PPPoE to Static PPPoE. Does this make my system any less secure? He also has a question about ShieldsUP!: Every time I run a test, the site reports "full stealth." Does that mean I'm completely invisible to and safe from Internet miscreants?

Steve: Okay. First part, dynamic versus static PPPoE. PPPoE stands for Point to Point Protocol over Ethernet, which is the protocol that DSL often uses. The very, very first DSL just used static IP address assignment. I've got a friend who still has five static IPs, and he loves them. He's never letting them go, he hopes. And if he were to change anything they would take that away because they're not liking having him tying up five IP addresses when IPs have become increasingly difficult to obtain. So PPPoE is like - Point to Point Protocol, which is the original PPP protocol, was what dialup used, where you would inherently establish a modem connection and then, over that dialup link, the Point to Point Protocol was defined to assign your machine its IP address and DNS and other services. So a variation of that is PPPoE, which, rather than using a dialup, it uses an Ethernet connection, thus DSL, but a similar protocol. So to answer his question, it does not make his system any less secure. It might make it a little more brittle in terms of the ISP doing something, assuming that it's set to dynamic, and then he's got it set for static.

Leo: Yeah, that's what I was wondering. Because if he's using static, he's going to have to put a static IP address in. It may stop working at some point.

Steve: Precisely. So it's not less secure. But if it stops working, then he'll have to switch it back to dynamic, get the IP address that is now being assigned, and then switch it back to static, and then put those same values in. That's what I meant when I said it might be a little more brittle because he could lose his connectivity. But while his ISP does not have strong DNS servers, I would say it's worth using strong DNS servers until his ISP gets their act together.

Leo: Yeah. So it's because it's using Dynamic PPPoE, one of the things it wants to do is not only dynamically set the IP address, but dynamically set the DNS servers.

Steve: Precisely. Essentially, you know, we're going to do a show here on DHCP shortly because we've talked about it several times. I want to talk about how very comprehensive the DHCP service is. It does much more, can do much more than just give an IP and DNS stuff. But..

Leo: A lot of times, though, you'll have a setting, you know, you can set DHCP. But then you'll say, I don't know if it's an override, but you can still set the DNS settings. Who wins in a case like that? The DHCP server or the manual settings I've put in there?

Steve: Oh, your local settings always win.

Leo: So if you're allowed to put those in, then you don't have to worry.

Steve: Yes. And in fact, for example, many people who've configured Windows systems will be familiar with that dialogue in Windows where you have two separate sections of "obtain my IP address separately" or "allow me to specify it," and then separately you're able to say, no, I'm going to provide my own DHCP servers. So, for example, other people with different setups are, well, in fact, even Edward, come to think of it, if he's - we don't know that he's a Windows user. And I don't know whether the Mac...

Leo: Oh, he could do it in Windows. He just wants to do it in the router so it applies to all the systems.

Steve: Right, right, right, right. But just so we finish that thought, because you and I just jumped ahead here, even though his router is offering to specify his DNS servers, he can certainly use the Windows dialogue to configure whatever DNS he wants to. And it will then ignore what his PPPoE connection is providing, and he'll be able to override those settings.

Leo: Yeah. Okay.

Steve: And the second part of his question was...

Leo: Oh, yeah, ShieldsUP!.

Steve: He's using ShieldsUP!, and it says "full stealth." He asks, "Does that mean I'm completely invisible to and safe from Internet miscreants?" Well, let me tell you exactly what it means, and then you can decide about the miscreants. What "full stealth" means is that, no matter what ShieldsUP! sent to you - I send out a broad spectrum of probes, ICMP, funky packets on illegal ports like port 0 that doesn't really exist. And some things respond to it. Some routers will send back a ping to ICMP, even though they are otherwise told to be full stealth. What I did in the second-generation ShieldsUP! technology was I created a completely wide-open scoop. And when I'm probing a remote IP, I'm looking for any traffic of any sort coming back from that IP. And so I'm casting a wide net. And so the only way you can get full stealth is if, in response to everything that GRC spews at your machine, nothing, not a single packet of any kind or description emerges from your network back to us. So, I mean...

Leo: Now, he says am I completely safe from miscreants. No.

Steve: And that's my point, exactly, is that if you're out on the 'Net messing around...

Leo: You can still mess up, yeah, yeah.

Steve: ...somebody can get your IP and, for example, blast your IP with a denial of service attack. Now, they won't know that you're still there because you are completely stealth. That is, nothing they do to try to evoke a response from you will function unless you are exposing something, like deliberately. But even through NAT, any traffic would have to be coming back from the same remote source, so the NAT router would route it back to your system. So "full stealth" means that for unsolicited traffic you are absolutely invisible. But again, if you expose yourself and your IP, someone could still blindly flood that IP and hold you off the 'Net.

Leo: Yeah.

Steve: And of course we've got spam, and we've got...

Leo: Yeah, there's plenty of other ways you can invite people in.

Steve: ...all kinds of other bad things that can happen, right.

Leo: In fact, I would say it's not a particularly common attack that somebody sniffs around and finds a vulnerability on your system and then gets in. Nowadays, you know, if you open an attachment, you're making the connection. If you click a link in an email, you may go to a website that now says, oh, good, we've got a port 80 connection going, and by the way, take this, and sends you an exploit. So there's all sorts of ways you can invite these guys in that this isn't going to prevent.

Steve: Yeah. And in fact I would go a little further and to say mostly what ShieldsUP! nowadays is intended to do, and what full stealth is to do, is to provide you with information. You know, people may not care about their router responding to a ping or not. This just tells them whether it does. And so it's not saying "full stealth protects you," it's just saying "full stealth," that means you're full stealth. You know, if that matters to you, then we're happy to confirm it.

Leo: Yeah, it's a part of your overall security strategy.

Steve: Profile.

Leo: But it's not in and of itself sufficient. You need to do other things, too.

Steve: Right.

Leo: But it's a great start, and it's why we use routers. Mike Graham in Hopatcong, New Jersey rolls his own DNS with something called TreeWalk. He says: Hi, Steve and Leo. What are you laughing at?

Steve: Your stoned voice.

Leo: Ah. Should I do that?

Steve: Rolls his own DNS.

Leo: Rolls his own, man. Hello, Steve and Leo. I once used a free utility called TreeWalk DNS - I won't keep it up - and installed a local DNS service right on the local machine. At the time I used it to replace my ISP's crappy service, but discontinued using it when I changed ISPs. Maybe now is the time to reconsider this and return to using it. Have you had any experience with TreeWalk? Would using it help with the DNS security problems that are around? Also in their forums they said it is not vulnerable to DNS spoofing attacks because only the local machine can access it, so intruders are out in the cold. It makes sense to me. See it at ntcanuck.com. Are you familiar with this program, Steve?

Steve: Intimately, because it was developed on our forums.

Leo: Oh, you're kidding.

Steve: It's developed by a couple guys, and it is widely used among the security-conscious folk who hang out in the newsgroups at GRC.

Leo: Well, I'll be diggety-danged.

Steve: So, and just for the sake of any listeners who don't know about, like, real, old, traditional, non-web-based but Usenet NNTP-style forums, we run - GRC runs, I run - a bunch of really worthwhile security groups. I think the fact that they're not web browser-based tends to keep them more high end and sober, you know, we don't have flame wars and script kiddies and all that. Anyone with Outlook or any third-party news reader can just - it's news.grc.com is the name of the news server. I run it on a FreeBSD UNIX server. It's real INN news, just like the Internet used to use, I guess it still does somewhere. But anyway, yes, many of the people who hang out there are using TreeWalk. And they're all - actually they've been doing a lot of beta testing of my forthcoming DNS profiling facility, which will be added to GRC shortly. And they'll, like, manually configure their TreeWalk DNS, which is just BIND. It's a nicely packaged version of BIND 9, all fully patched, so it's got port randomization. But they'll, for example, configure theirs to use a single port and verify that GRC sees queries coming from a single port, meaning that it's not safe, and then they'll switch it back to using random source ports and verify that it's working right. So by all means, TreeWalk DNS is a very nice way of running BIND. I would say it's not for the faint of heart. I mean, BIND is a sophisticated...

Leo: Oh, yeah, no kidding.

Steve: ...sophisticated DNS server.

Leo: Didn't BIND have this problem, this DNS poisoning problem? I thought it did.

Steve: Well, yes. But, I mean, BIND are the servers that did get patched just recently. So it needs - you need to be using the latest version of BIND. Because in fact remember Yahoo! was way back on BIND 8. And they said, eh, there's nothing wrong with BIND 8, we're staying with it. Until Kaminsky came out with his news, and it's like, okay, we're abandoning all of our BIND 8. We're going to BIND 9.

Leo: Okay. So this would - would you have to download BIND to make this work, or...

Steve: Well, yes...

Leo: Because I see the latest version is from 2005, I'm seeing, of TreeWalk.

Steve: Then you got me. I didn't do any homework, just because I know that these guys are on top of this. So...

Leo: I wonder if it's just a front-end to BIND, and you still need to download the latest BIND.

Steve: That may very well be.

Leo: That would solve the problem if they did that.

Steve: Yeah, I'm running BIND 9 myself in my own little local FreeBSD machine, so I just - I've never messed with TreeWalk myself. But I know that a lot of people run it on Windows.

Leo: Well, it's a pain to install BIND. So if this makes it any easier, that would be certainly appreciated. Danny Howerton in Ogden, Utah brings us even more bad news about Wells Fargo passwords. You remember last time when we talked about what a lousy job Wells Fargo was doing.

Steve: Wait, it gets worse, Leo.

Leo: So I think what - the last time it was truncating them? It would only allow you to use a certain length? Anyway: Hey, Steve. After hearing about the poor password practices of Wells Fargo the other week, I was tempted to do some further testing with the way it works, since that's my primary bank. I found out the passwords are also not case sensitive. What? What? I called up Wells Fargo, got transferred to their technical department, where the guy confirmed that in fact they're case-insensitive passwords. He said he would submit a ticket to their security team...

Steve: That'll work.

Leo: What kind of security team do you have to submit a ticket to get them to do case-sensitive passwords? He said he would submit a ticket but doubted it would get changed unless a lot of people request it. This is where you come in. If we could spread the word and get enough feedback to Wells, we could possibly change this.

Steve: Okay, so this is a classic example. This has got to be - now, you've seen the warnings on secure log-in sites that say, "Warning: Passwords are case-sensitive."

Leo: Yes, as they ought to be.

Steve: As they should be because, for example, using random case or case that, like, first, third, fifth, or first, fourth, sixth, you know, whatever, you could easily use case-sensitivity to take a short phrase and give it much more robust security.

Leo: What was it you said last time, it's like another eight bits of encryption or something like that?

Steve: Well, it depends upon, yes, essentially, every character whose case you change doubles the strength of the password because it adds a bit, an effective bit of complexity, meaning that you have to try the password with that character low case, then try with it uppercase. And so if it's case-sensitive, and you've got a nicely long password, but then you also play some game with the case, maybe you uppercase the vowels and lowercase the consonants, you know, you make up your own rule. I mean, it's a nice way of strengthening a password. Well, clearly some people were having problems logging into Wells Fargo. So what did they do? Oh, we'll make it easier for them. And in the process they make it easier for the bad guys. Now you don't have, I mean, non-case-sensitive passwords are just similarly weakening the log-in. And remember what we heard before was that they don't even care if there's extra stuff added to the end. And the question was, how many characters do they consider significant? How many are they saving? So just, you know...

Leo: It's like an eight-character, all uppercase password. That's ridiculous.

Steve: Yeah.

Leo: That's just ridiculous. There's no reason for that.

Steve: And again, it is them buckling to the common consumer who is unable to log in. But you ask yourself, how upset will the common consumer be when their password is stolen and their bank account emptied because Wells Fargo's password policy is so poor. All you have to do, I mean, it's time to start training people about case sensitivity in passwords.

Leo: Unbelievable.

Steve: The real benefit.

Leo: Steverino, are you ready? The Savvy Observation of the Week. [Tim] Knittel of Lexington, Kentucky says: Hi, Steve. In Episode 156 a listener asked if he could bypass DNS by directly entering the IP address of the websites he wants to visit. This approach won't protect him from the DNS spoofing vulnerability, however, for a number of reasons. Really. Well, that's interesting. First, not all websites use relative links to navigate among the pages. So you could enter in 192.168.1.1, but when you click the link it's going to come back to you as example.com/mylink, not 192.168.1.1/mylink. A good point. In fact, my site does that. You could come in via an IP address, but we're going to rewrite the address for subsequent pages to be TWiT.tv. Second, all external links on the page will not be IP based. That includes subdomain links. So continuing the example above, a link might be coolstuff.example.com, even if you enter an IP address. You click that link, bye bye. Third, only the web pages that his browser loads are user-controllable in this fashion. All his other applications will use domain names - email, newsgroups, RSS readers, podcast catchers, Windows Update, et cetera, et cetera, et cetera. Nothing you can do to stop those programs from using DNS lookup because they do it automatically, transparently, without your knowledge or intent. In fact, this includes the browser itself if the browser is configured to automatically check for updates. Oh, of course, didn't even think of that. His point is DNS is just too integral a part of computing now to be successfully on the 'Net without it. So you're not doing yourself any good by entering in IP addresses. We should have mentioned that, actually.

Steve: Yep, that's why I thought it was a really good point, is that technically I got hooked, I got...

Leo: You answered his question.

Steve: Exactly. I got excited by the idea that you could use the IP address itself. And yes, you can get to the website. And frankly, then that first page that you bring up would work. But if the web, even if that original, if that real website redirected you to a URL, your browser would then ask for that website's domain name, get spoofed, and go to the wrong place.

Leo: Right.

Steve: So you're only safe if you go by IP and you notice that it stayed by IP when you're viewing that page. Otherwise, as Tim notes, you're back in using DNS. And I liked his point, though, where he says, remember, everything else uses it, too. DNS is just too integral a part of computing to be able to use the Internet without it.

Leo: Yeah. Good point, [Tim]. We should have said that. Marc Argent - or perhaps it's Marc Argent - makes the Very Good Point of the Week: Dear Steve, is there a way of checking a DEP alert triggered by, for instance, Flash, is an attempted exploit or just poor programming by Adobe? It seems to me that blindly disabling DEP could be a potentially dangerous thing to do. And I do want to point out, we did some research on Silverlight, and you can turn on DEP and still use Silverlight.

Steve: Oh, good.

Leo: Yeah. So if I'm using Flash, I've got DEP turned on, and I get a DEP alert, does that always mean somebody's trying to attack me?

Steve: Well, this is what I loved about his point was that I too glibly said, oh, turn DEP on, and then start turning it off when you have problems. And he says, well, okay, wait a minute. What if that problem is because of an exploit?

Leo: Because of an attack, yeah.

Steve: It's like, oh, yeah, that's a very good point, yeah. So anyway, I loved the point that he made. And he asks, is there a way for us to know? And it would - only by being careful about your observation. I mean, for example, did you get that when you launched some Flash on a website, in which case I would definitely be suspicious of the Flash that I got from the website might be exploiting a flaw in Flash. And then I would be inclined not to disable DEP. I guess for me, and this is why I didn't communicate this well at all, is when I'm using a machine that has DEP on, it's normally not 'Net-based things. It's just, you know, I'm dragging something around to a tray or firing up an app that's not 'Net based, and it says bang and blows up. It's like, okay, fine, this thing is not compatible. But certainly when you're doing anything with the Internet and/or email or running something you got from somewhere else, and that action causes the problem, then you absolutely need to think, wait a minute, maybe this is the whole point. It's protecting me from what would have just happened otherwise, which is what you want. You don't want to say, oh, look, here's another incompatibility with DEP and then disable it for that product from ever on. So I thought Marc raised a very good point that I wanted to make very clear to our listeners.

Leo: Good. Thank you, Marc. And that brings us to the conclusion of our 12 fantastic questions. We'll do this every other episode. So if you have a question for Steve, you go to GRC.com/feedback.

Steve: And please do. I really, really appreciate getting the mail. I will apologize again, as I do every time I talk about this, that I am unable to respond to, or frankly even to read, all the mail that I get. I checked it this morning to prepare these questions, and there was 450-some submissions from last time I checked it, because I empty it every time. So, again, I really appreciate it. I love reading them. I do read all that I can. And I find time in spare moments to read more of them. So please keep them coming.

Leo: And we should mention that often the question that we read on the air, even though we use somebody's name, is representative of a number of similar questions from a number of different people.

Steve: Very good point. Like, for example, many people wrote about Chrome. And so we will be talking about Chrome in sufficient, I mean, in all the depth we typically do about anything, as soon as I'm up to speed.

Leo: Good. Steve Gibson is at GRC.com. That's where you'll find the show notes, transcripts of the show so you could read along if you're a - what do you call that, if you learn by reading? A visual learner? I guess. You can also listen to the 16KB versions, which are very small files, good for downloading on dialup. It's all at GRC.com, as are all of Steve's great free programs like ShieldsUP!, and the one-and-only SpinRite, the ultimate hard drive recovery and maintenance utility.

Steve: Yay.

Leo: If you've got more than one hard drive, you need SpinRite. It is absolutely true. Steve, I thank you very much. A great show.

Steve: Always a pleasure.

Leo: Do you know what we're talking about next week, or is it going to be a surprise?

Steve: I've got a list of things. So I have to choose one from the list.

Leo: Pick one.

Steve: It'll be a grab bag.

Leo: Great. Hey, thank you, Steve.

Steve: Talk to you then, Leo.

Leo: Talk to you next time on Security Now!. Bye bye.