Listener Feedback Q&A #50

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-162.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-162-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 162 for September 18, 2008: Listener Feedback #50. 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 help you, yes you, protect yourself online, learn about privacy implications, and just generally get to geek out on computers with the king of security himself, Mr. Steve Gibson of GRC.com. He's like the Parkay/butter boy. He's got his little crown on. And - or is it Chiffon? I think it's Chiffon. Hello, Steverino. How are you?

Steve Gibson: Leo, great to be back with you, as we have for the last 162 weeks.

Leo: It seems like it's only been 161.

Steve: They just fly by, don't they.

Leo: They fly by. And...

Steve: Although last week has been a rough one. Even today the market's down again below where it was on Monday because of the AIG scare.

Leo: You know, we're very fortunate. In fact, this show in particular is very fortunate because, despite the economic downturn, advertisers have continued to support the TWiT network to the point where we're pretty much sold out. And we got approached by another company that wants to advertise on your show. And I had to say, you know, we've got three spots on here, and I can't put any more on.

Steve: Now, Visa was doing a relatively short buy; right?

Leo: When Visa leaves, we will have a new - and you will like this advertiser. I will run it by you, of course, as I always do. You get the right of approval. But I don't think you'll have any trouble with this company.

Steve: Well, good.

Leo: In fact, I think you'll be - oh, I'm going to say the name: VeriSign.

Steve: No kidding.

Leo: Yeah.

Steve: Oh, cool.

Leo: And I think it's really because of the focus that you've put on what they're doing with their secure log-in technology.

Steve: Actually I've got an email from one of the VeriSign guys, Gary, that I haven't yet even gotten to read. I've got it open...

Leo: I bet that's what it's about.

Steve: It may well be. A bunch of news on their end, so.

Leo: Yeah, but I think we've had to tell them yes, but you'll be waiting a little bit. We have, well, you know, people love you. You have been - Astaro's been with us for more than two years. Audible's with us for more than a year. Visa, who knows, they may not ever want to leave. And so I can't complain. I'm very happy. And despite the economic downturn, the good news is we're going to keep going with this show and all the shows on the TWiT network, as long as the advertisers and the audience

continue to support us as they have.

Steve: And there is no sign of us running out of any material. I have some - I am saving for the last some horrific new revelations about Google's Chrome browser.

Leo: Oh, interesting.

Steve: Yeah, yeah, yeah.

Leo: So what have we got? This isn't a Q&A episode.

Steve: Yes, it is.

Leo: It is. All right.

Steve: 162 is - and actually it's our 50th Q&A episode.

Leo: That's kinda neat.

Steve: Yeah, so you're going to want to fire up your email and grab a copy of the PDF.

Leo: I will. So, Steve Gibson, you want to save the bad news for later, or do you want to deliver it right now?

Steve: No, no, we've got plenty of bad news.

Leo: Oh, gee. Oh, god.

Steve: Throughout the entire show. I did want to mention that there was the Apple OS X 10.5.5...

Leo: Yes, came out.

Steve: ...has just been released.

Leo: 33 fixes.

Steve: I know, a huge number of things. Even the ability to - they fixed - there was a way that users could log in without a password, or change another user's password.

Leo: What?

Steve: Oh, yes.

Leo: Oh, my goodness. I didn't know about that. Wow.

Steve: So a ton of vulnerabilities, arbitrary code execution problems, denial of service, and some DNS cache poisoning. So they've addressed that which we knew they were - we were hoping they were going to. And so they have...

Leo: Yeah, they did a fix in January which didn't fix it.

Steve: Right. Right.

Leo: So it's a good thing they came back.

Steve: And they also did some fixes for some of their stuff, some of the open source components that were really not their problem; but, you know, it's in their system, and they're shipping it, they provided it, so they've got to take some responsibility for it. Also in the bad news category I wanted to alert people, there have been some huge problems under Windows after the iTunes 8 update.

Leo: Oh, Blue Screens of Death.

Steve: Yes, Windows is Blue Screening of Deathing...

Leo: Oh, I like that.

Steve: Blue Screening of Deathing...

Leo: A little participling, but that's good.

Steve: Blue Screen of Deathing, yeah, just one "ing." Blue Screen of Deathing. It's caused by a newer version of a GEAR add-on. You know that GEAR is a well-known provider of drivers for CD and DVD burning. And so in this newer version of iTunes, Apple is installing a new ASPI module, GEARAspiWDM.sys. And that's apparently the source of the BSODs. They don't occur until you plug in your iPod, which invokes the driver to jump in and help out, and then your system BSODs. Not good.

Leo: Wow. Wow. Now, does GEAR come from Apple, or does GEAR come from somebody else?

Steve: Well, GEAR is from a company called GEAR. They're a German outfit. And in fact I own - GEAR Professional is their writer because I think I mentioned to you in my main media machine I've got four burners. You were chuckling over what do I need four burners for. I said, well, you know, I only have to burn one quarter as many times when I'm doing a little short...

Leo: I don't even know what you're up to, and I don't...

Steve: It's for production.

Leo: You don't burn your own SpinRite disks.

Steve: No, no, no, no, no.

Leo: No, people download that. They burn them, yeah.

Steve: It's just, you know, when I want to share things, like, you know, like for example there was - some friends of mine missed both first and second shots of the first episode of "Fringe." And by the way, I should say that we got a ton of email from people thanking me for aiming them at "Fringe." They very much liked catching the repeat of it last Sunday.

Leo: We're getting a lot of requests to do a Security Now! sci-fi show. And I can't figure out if the requests are because they want us to stop talking about sci-fi on Security Now!, or that they like it so much they want us to do more of it.

Steve: For what it's worth, I do get a lot of feedback from people who want to hear more. I guess the same sort of stuff you're talking about. I mean, there are a lot of people who would not have seen "Fringe," they wrote, had I not mentioned it and said, hey, I think this is worth checking out. And so they were glad they hadn't missed it. So that was cool. I also, since I last talked to you, Leo, actually it was the day after we last spoke, I was joined for coffee at 5:30 in the morning by Stina Ehrensvrd.

Leo: Oh, you're kidding, that's great.

Steve: Yeah, she was down at the DEMO show, which was at the beginning of the prior week, beginning of week before last, or, well, no, last week...

Leo: She's the creator of YubiKey.

Steve: YubiKey at Yubico. And it was really fun. We spent a couple hours, and I got a complete update on what's going on. They're doing fantastically. I had known from email that I shared with her, which I mentioned on the show before, that there was a lot more free, open source stuff being done, which is all available for download at their site, Yubico.com. But also they've lined up some venture capital. So they're going to make the next step forward in going from a generic chip to their own custom chip.

Leo: Oh, that's neat.

Steve: And, well, what's significant is it will dramatically lower their cost, which they intend to pass on to customers. So it's going to bring the cost of the YubiKey down dramatically because they'll be able to bring their own costs substantially down. So that's going to be neat. The other thing that - there were two things that I asked her if I could share with our listeners. The first is that they're getting ready to start growing the company. And she asked me if I knew of any good, like, "suits" sorts of people.

Leo: She's tired of wearing the suit.

Steve: She's just not a suits person.

Leo: No.

Steve: And but she needs some...

Leo: This is why we love her, by the way.

Steve: Yeah. But, you know, to grow forward she needs, like, sales and marketing type people who are familiar with the tech industry. And I said, well, you know, I'm sort of a hermit down here in Southern California, I said, but Leo may know people. And I said, but even more so, our listeners are people. So...

Leo: I figure if you listen to the show, you're probably a good candidate for this job.

Steve: Well, I mean, exactly. You know security. You know the product.

Leo: Obviously you'd have some business experience. They're looking for operating people; right?

Steve: They're looking, yes, for operating and also - not really so much on the tech side.

I think they've got that well covered. But operating and business development sorts of people because there are things that I cannot talk about that are in the works that are very exciting.

Leo: Oh, neat.

Steve: That I'll be able to talk about when Stina says this can be discussed publicly. But I should say that it's just lots of good stuff is going on. It's very clear that the people who see this understand it. She mentioned, in fact, that she ran across the ex-editor-in-chief of PC Mag, and she only remembered his name as Michael. I said, oh, Michael Miller.

Leo: Michael Miller, yeah.

Steve: Of course. And I told her I have a long history with Michael. He was my editor. He edited the TechTalk column for most of the eight years that I was at InfoWorld. And anyway, so he apparently came by where she was sharing a booth with someone. And she was sort of holding it up in the air and saying, do you have an interest in authentication. Anyway, Michael, to his credit, because he is a techie also...

Leo: What's he doing now? Is he...

Steve: I don't know. I guess he's no longer editor-in-chief. But I think he's still writing a column.

Leo: He's paying attention, obviously, because he's...

Steve: Yeah. And he was present for the DEMO conference. So but, you know, again, Michael instantly got and understood what this thing was.

Leo: That's really neat. Of course he would.

Steve: Yeah, so anyway, so things are really happening for them. So I did want to mention, if you are a listener, or you know somebody who's technically savvy and maybe looking around for the right kind of opportunity - up on the peninsula because they are moving, she is moving her family and herself and the company, essentially, to Northern California, just mostly to be in the middle of where all the action is, and all kinds of talent pool. So that's happening.

And, finally, they're going to do - and she hasn't figured out all the details yet. But she's going to host a contest with a number of different categories focused around most innovative applications for the YubiKey. And I have agreed to be a judge on the panel for coolest, neatest ideas for the YubiKey. So that may also be something that our listeners would be interested in, cooking up an idea and entering that. The contest doesn't exist yet. I would imagine like a month from now. And she's considering maybe announcing the winners at next year's RSA conference. Where she will have a booth of her own this

year. As we all remember, she didn't last year. I met her, or I bumped into her, at the top of the escalator when she was looking around for someone who would understand what they had done, so...

Leo: Very cool. Well, that's nice to hear. She seems like a very nice person.

Steve: Yeah, and I just really wish them well. I think it looks like they've got something good that is going to go.

Leo: I might as well mention that we're looking for somebody to - nobody in a suit. But we are looking for somebody who lives in the Petaluma area, the Northern California area, who can commute and come to our office, because we can't do this long-distance, to edit audio for us and work with us in audio and video editing. And if you - you don't have to have any skills in that area. If you're comfortable with computers, just email Dane. It's jobs[at]twit[dot]tv.

Steve: Now, what about Tony? I thought he was the...

Leo: Tony's full-time. We're going - so Tony's going to move more toward the video side because we want to start putting out video. And that's a full-time job, believe it or not, to get video out the door. So Tony will go more to the video side. And then we'll have somebody doing audio, as well. So, yeah, we have to expand a little bit. It's expensive to do all this stuff. But, you know, we've got to jump while the iron's hot. Advertisers are asking us for more products. So we'll give it to them.

Steve: And will this mean more shows? Will you be doing...

Leo: I can't do more shows. No.

Steve: Your schedule is already full; right?

Leo: It's already full. We're going to do more video. We're doing a lot of video. For instance, we're going to do interviews with Will Wright coming up, Neal Stephenson coming up. I have some very interesting interviews, all that we kind of do ad hoc in the studio with people who show up, like from "Red Dwarf," Bob Llewellyn played Kryten in

"Red Dwarf," he was great. So we want to start putting these out because, if you don't see them live, chances are you're not going to see it at all. So we want to put them out as something you could download. And the only thing holding us back at this point, we've got a bandwidth commitment from the CacheFly folks, which is wonderful. We've got advertiser commitments. But we need an editor so we can put - because, you know, it's hard to put - as you know, video is a little bit more complicated than audio.

Steve: Yup, yup. Well, that's cool. And there's someone who participates over in the newsgroups, at GRC's newsgroups, who captures the stream weekly. And in several instances there have been people who have really wanted to watch the stream.

Leo: I did not think this would be a video show. But seeing you somehow makes it easier to understand what you're saying.

Steve: It's my creative work with my hands.

Leo: It's the hands. So while we always offer the audio, and that really is our primary medium, for those who want to see, say, things like Steve, because we do have video of you thanks to Skype, we'd like to offer that, as well. Just as an alternative way to download it.

Steve: Cool. Well, in my last little blurb before we plow into our questions, a listener - Ki Il Song, I think, is how I would pronounce his name - his subject was "SpinRite Does It Again." And he says, "I'm writing this while listening to the latest episode of Security Now! on my Mac. I'm a loyal listener of Security Now! and most of the TWiT network of netcasts. They're entertaining, informative, and infinitely more enjoyable to listen to on my commute to and from work.

Leo: There you go.

Steve: I don't know if this is a good thing, but there are many nights that I fall asleep listening to one of the many TWiT netcasts. Keep it up, Leo and gang." So he says, "The reason I'm writing this email is because of my recent experience with SpinRite. My 75-year-old uncle became a widower approximately four to five years ago. For almost a year after my aunt passed away, he was lost and depressed after losing his wife of almost 50 years. One day, one of his closest friends told him that he needed to get over it and move on with life. He proceeded to give him a laptop, an Internet connection, email, and a digital camera."

Leo: I think that's a great idea.

Steve: It was really neat. And he says, "Can you believe it? A 70-plus year old learning how to use a computer, digital camera, and email. He became so obsessed with his camera/computer/email that he would never go anywhere without the camera. He would take pictures of everything from flowers, landscapes" - and I love this one - "and pictures of old pictures and events that he attended, and then emailed these to his friends all over the world. He also became the resident photographer for our family. He had over 50 gigs of photos and videos that he had taken over the past several years." Well, you know where this is going.

Leo: Yup.

Steve: He says, "Last week my uncle called me and told me that his laptop was broken. It wouldn't boot up. I went over to his house and saw that the Windows boot screen was in an infinite loop. I tried to see if I could go into safe mode to fix the problem from there, but it wouldn't even get into safe mode. It had the same result as normal mode - infinite loop at boot screen. I told him I would take his laptop home and see if I could fix it. So I took it home, booted into SpinRite, and ran it for several hours. It came up with several errors the first round. Excited, I booted into Windows and, voila, it worked."

Leo: It's kind of fun, but it's true, you are happy to see errors when you run SpinRite because that might explain why you're having problems.

Steve: Exactly, it's fixing things. And he says, "For a safe measure, I ran SpinRite again to see if it would find any more errors. It found no errors the second and third times. At that point I called my uncle and told him that his computer was fixed and his library of photos and videos from the past several years were saved. Thanks, Steve."

Leo: Yay. That's a nice story. I liked it. I like hearing that. Steve, I have in my hand 12 fabulous questions, written by...

Steve: Little do you know. We actually have really good stuff this week. I'm really pleased with these.

Leo: Better than usual?

Steve: Well, there are sort of some themes. There's a strong Wells Fargo theme. There were a lot of people who wrote in about various pros and cons of Wells Fargo.

Leo: Yeah, some people, I have to point out, some people did say that they thought it was okay. But we'll get to that.

Steve: And in fact one of those that you forwarded to me is here also.

Leo: Good.

Steve: And, yeah, it's just some great, really good stuff.

Leo: Let's start with Vic Thompson. He's in Newcastle, Australia. He says he heard our tip just in time: Steve, I'm a retired, as in unpaid, medium-level geek and an avid listener to the "netcast." He says "I say that for Leo." A friend of mind was about to commit his PC to the deep after a major dismemberment of his OS by at that point an unknown event. Even though he managed to get it back to working order, the Sword of Damocles remained hanging over his head, and he still was going to load the PC into his boat, although without concrete overshoes. Then I

caught up with the latest Security Now! episode, and all was explained by your mention of the Trend Micro problem. That's what bit him.

Steve: Yup.

Leo: Wow. There's very little notification anywhere about this, so you were the only light on the hill for us. I am not only a SpinRite owner, but also a SpinRite advocate to all who will listen, and even to those who will not. Thanks for the great pod, oops, netcast. Vic Thompson, Newcastle, Australia.

Steve: Vic was one of a number of people who mentioned that this, like, clicked in their heads. The Trend Micro update, as you'll remember I mentioned last week, caused a bunch of problems for people because it false-positive identified Windows's own OS file as being, due to heuristic pattern matching, as being malicious. And it sequestered them, and then Windows would no longer boot, even in safe mode. And it caused a ton of problems for people. So I did want to - I wanted just to reiterate that, to thank Vic for his note.

Leo: What's the solution?

Steve: It's bad. You need to use somebody else's computer to go to Trend and pursue a solution involving getting those files back out of jail somehow. I didn't pursue it all because it didn't hurt me, and no one that I know or love.

Leo: And presumably Trend has updated their viruses, their antivirus, to not do that anymore.

Steve: Yeah. And in all fairness, actually this is the second time Trend has done this, but it also did happen with Symantec once a few years ago, that they did the same thing. So, I mean, it's risky. It must be that they're checking different language versions. Because it's hard to imagine how they wouldn't be able to check their own Windows system to make sure that it didn't bring it to its knees.

Leo: Well, yeah. And this is why many antiviruses don't do the job they used to do, because, well, any antivirus should be hesitant to quarantine Windows system files; right? I mean, you're killing the baby to save the patient. And...

Steve: Although the problem is, due to the fact that viruses name, malware deliberately names files with overlapping names, it might put in - so it might very well put a malicious code under a different directory with the name of a valid Windows file. So you can't use...

Leo: Or attach itself to an existing Windows file.

Steve: Sure, exactly.

Leo: So this is - but this is what I'm saying. Most antiviruses now will just say, hey, it's a Windows file, I'm not going to touch it, but you've got a problem here. You've got to figure it out. But, see, Trend just said, nah, I don't care. I'm doing to kill the patient.

Steve: Because automatic is just so wonderful. We don't want to have to train our users or have them take any responsibility.

Leo: Opher. Hello, Opher. Our old friend Opher writes to the Daily Giz Wiz frequently.

Steve: Oh, no kidding.

Leo: Yeah. Opher Banarie in Laguna Niguel...

Steve: Oh, right.

Leo: Pardon me?

Steve: I was going to say, he's the guy who also wrote to you, trying to get the note to me.

Leo: He wrote to me first. He says he's got some good news about Wells: First, when I log on and put extra characters at the end of my password, it's rejected. This is contrary to what your listener said last week. Secondly, as reported by others, it is true that neither username or password is case sensitive. But no one has mentioned that, after failing three times to log in, the session is terminated, and the userID is locked out. That happens to me in a lot of sites. It drives me crazy. Because it often takes me four tries. I'm speaking for myself, Leo, now. It often takes me four tries to get the password right. In order to regain access, you need to provide the ATM card number and PIN and answer a security question. Then you need to assign a new password. As a result of this stringent lockout policy, while the lack of case-sensitive username and password is an issue, I think the site's plenty secure, says Opher. If Steve wants to discuss Wells Fargo any further, please ask him to include that lockout feature and any security problems it may expose. I am not an employee of Wells Fargo, just a happy and, I believe, secure customer.

Steve: Well, this is really good news because a lockout policy is super important. And as Opher believes, and he's certainly correct, it shuts down any attempt at doing password guessing, where you're just...

Leo: You can't do a brute force if you only get three chances.

Steve: Right. I mean, just not feasibly. Now, somebody else write, and I didn't have space to include it in today's Q&A, but he had been experimenting with Wells. And apparently it's the first 14 characters of - I don't know if - I'm not sure if it's username or password and/or password. But at least password, the first 14 characters are significant. And after that 14, any additional characters are ignored. So it is still the case that extra characters are ignored, but not until you've got 14 that are not ignored, which we know is a long and fundamentally secure password, yes.

Leo: That's pretty good.

Steve: Or at least potentially secure password. But I did, you know, with all of the bashing we've been giving Wells over the last few weeks, the fact that they do a three-strikes-and-you're-out lockout and then require the user to go through much greater hoops in order to prove that they're really themselves or, well, maybe, Leo, it is the case that that really does mitigate the problem a lot.

Leo: Yeah. Almost all my financial institutions do that. They'll lock you out if you keep guessing. I know that because I almost always have to guess. What I hate is one of them makes me call them. Two of them do what Wells does, which is, okay, well, we're going to have to go through some more hoops for you to reset your password. I don't mind that, if I could stay online. But when I have to call them, that's just a pain. And then, you know, I've been using BofA, and when I turned on - I have quite a few BofA accounts, Bank of America accounts. I hope...

Steve: It'll be Bank of the World.

Leo: Yeah, they own everything now. What's nice is I've set it up, it's not a requirement, but they encourage you to set it up so that each time you log in, it sends a passcode to your cell phone, very much like the football, a one-time log-in passcode, to guarantee that it's really me. That makes me feel so much better when it does that.

Steve: Yeah, in fact we've talked about using a cell phone loop to provide an additional factor in multifactor authentication. I think that it makes tons of sense.

Leo: Yeah, I turned it on in all my accounts. It drives our bookkeeper crazy because she has to call me...

Steve: Well, it actually works both ways, too, because if your phone starts ringing with authentications, and it's not you, then you also have affirmative knowledge that somebody is trying to log into your account.

Leo: That's a very, very good point, yeah. No, I think every high-security application should use some form of, what do you call it, two-layer authentication.

Steve: Yeah, multifactor authentication.

Leo: Yeah, I just think it just really makes a huge - it's just - of course I only know that because I do this show with you. I don't know if everybody knows that. Just makes me feel better. Jon Kuhn in - go ahead.

Steve: Well, and that is directly what Yubico and the YubiKey are doing, too, because if that system were widely deployed, as hopefully at some point it may be, you could just stick it into a USB port and touch the little button, and it would shoot out some characters that absolutely prove it's your YubiKey.

Leo: I like that. Then somebody would have to get me, my YubiKey, my log-in, and my password. Ha ha.

Steve: Yeah, good luck.

Leo: Good luck. Jon Kuhn in Ann Arbor, Michigan has discovered that Wells Fargo is in bad company. Oh, boy. After hearing about Wells Fargo on the Security Now! podcast, I decided to try out all of my GRC Perfect Password-derived passwords, all of them alphanumeric with upper and lower case. I found that Chase, Citibank, Vanguard, and my credit union all have non-case-sensitive passwords. Just thought you might find that interesting.

Steve: So Wells Fargo is sharing the doghouse with these other people. But given that they've got lockout provisions, and I imagine that our listeners may now be curious to poke at their - deliberately log in incorrectly and see what it takes, verify in fact that anyone trying to guess their passwords will be shut down very quickly and then have to go through the extra reauthenticating hoop-jumping in order to get their account reactivated. Which, again, it certainly does mitigate the problem of passwords being non-case sensitive.

Leo: There's got to be a reason they're doing this. Is it possible that some older computers or older...

Steve: Matter of fact, if you keep reading, we will come to the reason.

Leo: Ah. I like it. I like it. Steve is always way ahead of me. Brent McLaren in Ajax, which is near Toronto in Ontario, Canada, brings up a very good point. It's a point about case-insensitive banking passwords.

Steve: Speak of the devil.

Leo: He says: Hi, Steve. Been listening to Security Now! since Episode 1. I really enjoy the show. Me, too. Even though I work in IT and spend my days working with security and networking technology, I've found your insight and ability to explain complex topics very valuable. So I just wanted to pipe in on the topic of case insensitivity for Wells Fargo's online banking log-in. I know that for my bank the password used for online banking is shared with telephone banking. As a result the password has to be limited to alphanumeric passwords with no case sensitivity. It's also limited to six characters. I believe this is one of those tradeoffs between security and usability that is necessary. Having separate passwords for the different channels would be beyond confusing to people. That's a very good point.

Steve: Isn't that a good point? I liked that because you could imagine trying to explain to somebody that you've got, you know, what a circumflex is or...

Leo: I don't think there's a circumflex on my phone. Yeah, you're right.

Steve: Or the pound sign. What? Well, it's that number sign, the thing, you know, I mean, so if passwords were really complex, it could be difficult for them to be used, the same password to be used, essentially repurposed through different venues with the same institution. And so it's like, okay, that makes some sense. You could imagine that trying to explain your password over the phone to somebody could be a problem, much more so than you typing in some strange concoction with shift keys and so forth on your keyboard.

Leo: And I actually remember that I got started in online banking with Bank of America in 1984 or something with phone banking. And so I think that probably it's the same system it's been all along. In fact, and this is what made me ask the question earlier, I remember it was almost a TTY the first time I started doing online banking. A black screen would come up with white letters on it, all uppercase. The menu structure would be, you know, type "1" for this item, type "2." I mean, it was very primitive. And I bet you it's the same back end.

Steve: It may very well be that they just stuck a web server on the front of it.

Leo: Yeah. It's looking better than it used to, I have to say. But for a long time online banking, for me, was that. It was like a TTY. David Townsend in Wimbledon, U.K., worries about his employer: Hi, Steve. I live in the U.K., work for a large blue-chip computer consultancy. We have a timesheet and expense system that is used globally by the company over the Internet, feeds directly into our central billing system. The site, not SSL. And to make matters worse, there's no password expiration, no lockouts after X attempts, and the passwords are not case sensitive. I've written to my company formally two times, but my concerns have fallen on deaf ears. The company believes that, because it has not been hacked yet, they are completely safe with HTTP, and my concerns are just scaremongering. I feel ashamed to actually be working for this company with such a lax attitude to security,

especially since the company is involved with IT development. Do you think my concerns are real threats here? What are the risks the company's exposing themselves to? Could the HTTP traffic be sniffed? Are there other concerns they'd need to be aware of? I'm hoping, if you answer this, that I'll have some real evidence to go back to the company with and get this changed before we are attacked.

Steve: Well, our listeners, any listeners who've been listening for 162, or 161 previous weeks, know a lot about this. And of course David, who is a listener, knows...

Leo: He knows.

Steve: ...that he has absolute cause for being concerned. And clearly he does. The question I think is, in order to sufficiently understand the threat model of the system, we have to know how is the system really being used. That is, if you assume that somebody unauthorized is going to have access to this, what is the consequence of that? He's saying that it's their timesheet and expense system that's directly tied into central billing. So the question would be, if somebody maliciously had access to this, what does it mean? The response he seems to be getting from the company's IT people are that there's not a problem. To quote him, he says they are completely safe because they've never been hacked. Well, the world is full of people who are, well, they're not safe because they've never been hacked, but they have a false sense of security because they have never been hacked. And it takes a company losing millions of employee confidential information or credit card information that's sold on the Internet or one of these horrific events to realize that its reputation has been damaged, and to say ouch.

He actually, in his letter, provided me some additional information that he asked me to keep confidential about the system that they're using. I did some research, and it's a third-party tool, not the company's own tool, which apparently provides this level of insecurity. So it's not just this one company that's using this. This is a tool that is globally used widely. And so all the companies that are using this particular Internet-based timesheet and expense system are exposed. Which to me, given the fact that the security at the log-in - this is a freely available public server.

I went to this website and looked at the front end. It was from there that I figured out what the package was that was running behind it. And I then went to that company and explored them a little bit to see who this was and how pervasive this was. So, and it's a well-known, successful company that has incredibly insecure log-in policies. I mean, it's irresponsible. Like I would say first of all the company that David works for has got their head buried in the sand. But more importantly, this is a commercial product being offered by a company, certainly at some expense to their clients, that has zero log-in security. So it's definitely a bad idea.

Leo: You know, the temptation, I think, for employees like David is to prove it by logging in insecurely and demonstrating how easy it is to hack. And I've got to warn people about that.

Steve: I was just going to say.

Leo: This happened again, that a guy who got so frustrated with his company's security policies that he hacked in and got some password information and then sent it to the president and said, look, I've been telling you about this. Look, see what I got? And of course he's going - he went to jail. In fact, our good friend Randal Schwartz did the same thing at Intel some years ago and was arrested and tried for hacking. Companies don't take well to having their nose rubbed in it, let's say. So be careful about how far you go to prove the point.

Steve: So just to answer his question, that site, and the same log-in page for everyone else using this company's timesheet and expense system software - and, you know, I don't have it in front of me. I ought to tell everyone the name of that company because they deserve to be in the doghouse. Although I guess that would expose anyone who had access to them to - we'd be making it obvious that these people are really attackable. So it would be better to send them a private email and say, look, this is just not okay. They are exposing all of their clients. The fact that this does not require SSL definitely means that this can be sniffed. If in any situation there was wireless, then anyone with a wireless system could be logging all the traffic, seeing people log into this timesheet and expense system, capture their log-in, and then do, I mean, the only thing we don't know is what level of mischief someone could get themselves up to.

So in summary, this is the question I would ask David to pose to his company's management. And that is to say, it's very much like the analogy I draw with WiFi. When I try to explain why wireless is so dangerous, I say, okay, plug a wire into your wired hub and run it out the front door to the lawn, and then stick a stake in the lawn with a sign that says "Free Internet Access."

Leo: That's good.

Steve: I mean, they're doing the same thing with wireless. So do you want any random stranger, 24/7, to be able to plug into your hub in your home and see what's going on? So similarly, David ought to pose the question, okay, here's the worse case. Is there anyone that you would really be unhappy giving free and unfettered access to the timesheet and expense system? I mean anyone. Because essentially, depending upon the exposure that people logging into the system have - and he says this is used globally by the company over the Internet, which means random people of this large blue-chip computer consultancy are sitting in Starbucks and random WiFi hotspots, logging into the timesheet and expense system. There's no question then that that log-in is sniffable and open and is compromisable. So this company needs to ask itself, what damage could somebody do who has access to the system, because that's what they're making possible.

Leo: Yeah, wow. Very scary. Moving on to our next call here. Or it's not a call, it's a question from Anonymous - he says I don't want this to be public, but I like to use the PPP, Perfect Paper Password system. But I'd like to generate passwords that follow certain rules. For instance, I want to say must be mixed case, must contain at least one digit. Is that possible with the web application or with the EXE application? That's sometimes a requirement of some systems. I run into that all the time where it says, well, I like your password, but you've got to put a digit in it.

Steve: Well, I loved the question. The reason I made it anonymous, I actually know who this is. But he sent it to GRC, to Greg, our tech support guy, which Greg forwarded to me. So he didn't intend me - I don't know that he intended me to make this public and to read it. But I wrote him a lengthy reply because I thought it was sort of an interesting question for our listeners, from a theoretical security standpoint. So here we've got the Perfect Paper Password system. Now, as it was designed, that's a one-time-only system. So the individual tokens are short. And certainly they're not correct, they're not appropriate for long-term static password use. But in the final evolution, I think it was the third major revamp of the Perfect Paper Password system, which we remember was Even More Perfect Paper Passwords, we allowed them to be any length. So you absolutely can use both the online, web-based version or the EXE, with the appropriate command line options, to make really good, really random, really long passwords. You can make them as long as you want, basically use it as a random password-generating - or string generator.

So then the idea of saying, oh, but they have to - what if they have to have mixed case? Then can that be enforced? Or what if they have to have some digits? And, okay, well, frankly, that lowers the security. I mean, it actually does. And that's the point. That's the reason I wanted to add this to this week's Q&A, is the reason that those sorts of requirements, like mixed case, must have several uppercase characters or lowercase characters, must contain at least one digit, those are enforced on passwords generated by people because people don't generate high-quality random passwords. They use all lowercase because it's easier for them, deliberately, or they won't use any digits so their passwords tend to be in dictionaries or would be prone to brute-force attack; whereas salting them with a couple digits, forcing some digits in, breaks brute force attack possibility.

But taking a system which is generating highly random, I mean, really, really, really high-quality random passwords, and then imposing on it some such rules, reduces the strength because an attacker who knew which rules were being imposed would then reject passwords that broke those rules. And essentially you are, by imposing those rules against a system which is already generating really high-quality passwords, ends up lowering the security of the system because you're discarding a large subset of passwords, forcing a smaller rule set on them.

So I just thought - that's essentially what I told the person who wrote. And he actually replied, and he says, I understand what you said, thank you for the explanation, but I wanted to use these in systems that enforce those rules. And it's like, well, okay. So put something, manually change the case. And if it happens you get a long password without a digit in it, then put some in. You can, with the Perfect Paper Password system, you're also able to specify the alphabet. So you could specify an alphabet with upper and lowercase alpha. And also, if you wanted to make sure you had numbers, you could put in 0-9, 0-9, 0-9, that is, if you specified those three times you'll get - then digits are three times more likely to occur than they otherwise would. And essentially what that means is that you'll tend to have, in a sufficiently long password, it'll be extremely rare that you get one that doesn't have digits in it. On the other hand, the Perfect Paper Password system also generates them endlessly. So you could just cross out the ones that don't obey the rules that you need and keep the ones that do. Which is probably the right solution.

Leo: Very good. Let's see here. Carl Schweitzer in Hilbert, Wisconsin says, why is it all just 0s and 1s? Why aren't there any 2s in there? Dear Steve and Leo, this is a topic that's been brewing in my head for some time, and I'd like for you to help

answer some nagging questions for me. It all started many episodes ago, when the two of you were talking about the ability for someone to scan the residual information on a hard drive and detect the original bits that were overwritten by new data. Regarding this first part, I was wondering what type of equipment would you have to use to detect the residual magnetic field on a hard drive? Specifically, is it small enough to be contained in a standard hard drive case?

Outside of this thought process, I've been trying to adapt a bug into a feature. Well, if the answer to the first question allows it to be possible, could you manufacture a hard drive to write over data and still detect it, essentially doubling the capacity of a drive? Also, if current hard drive heads can detect these fields effectively enough, could some smart programmer create new drivers to double the capacity of existing drives? Thanks a lot for the great show. It really gets one thinking.

So let me explain what Carl is saying. Since you can theoretically read erased data, why don't we just record double the data on a hard drive and use that technique to read both?

Steve: Well...

Leo: Can you use baby words?

Steve: It's not as crazy as it sounds.

Leo: Really?

Steve: Well, there are, and we mentioned this before, there are multilevel flash RAM storage. There are, because flash storage is trying to grow in density, one of the tricks that's being used in flash storage is to store analog values in the individual cells so that, rather than just having an individual bit cell be either fully discharged or fully charged, they're deliberately storing multiple levels of charge in the cell and essentially storing more than one bit per bit in the cell. Now, it works there because the tolerances are sufficient that you are reliably able to determine what the charge is in the cell, essentially by dumping the charge out of the cell. You transfer the charge out of the cell. In the process of doing so you're able to see how much charge there was. And with sufficient resolution you're able to create a multilevel charge per bit cell in nonvolatile memory.

The problem with hard drives are many. Mostly this is an extremely unreliable process, more than anything else. It's more than theoretically possible to determine what data was on the drive before. But it is far from reliable enough that you could count on that happening. The only way that that would be feasible would be if you really cranked up the error correction technology such that large chunks of areas and individual bits that couldn't be determined could be corrected across.

The problem with doing that is that error correct technology essentially works by correcting bursts of errors, that is, groups of bits that you cannot determine, because that tends to be the way errors occur. There's a physical defect on the hard drive. That physical defect is larger than many bits. So many bits are swallowed by that. Therefore you need an error correction system that's able to straddle across the entire dead zone

created by the physical defect on the drive.

Leo: I think your physical defects just - my microphone just fell over. Sorry about that. Clonk.

Steve: So the nature of trying to recover individual bits from underneath, essentially that have been deliberately overwritten by super strong bits, is that you would scatter your inability to recover across the drive. Error correction, burst-style error correction wouldn't be feasible. And you end up with so much overhead trying to correct that, that it's better just not to try. So bottom line is, I mean, you could theoretically do it.

One of the other problems would be the technology would radically slow down your storage. You'd read off the most recently recorded data. Then you'd have to switch into a mode where you're struggling really hard over a great period of time to subtract that massively strong signal from the signal you're reading in order to ascertain what was there before. I mean, it's just - it's not practical or feasible for any number of reasons. It makes sense in the narrow case of forensic analysis where some agency on a governmental scale desperately needs to know what was underneath the most recently written data. But it's just not practical on a daily basis. Besides, just wait a week, and the drives will double in size all by themselves.

Leo: Well, they are doing tricks that involve kind of layers and so forth. So it's not so crazy as all that, really.

Steve: Yeah.

Leo: Yeah. Carl Schweitzer - oh, no, that was him. Blake in Minnesota wants to get a better handle on Windows security: Hey, Steve and Leo. I was just listening to a Security Now! episode from a couple of weeks ago. And I wanted to inquire further about what you said about Vista/XP security. That was last week. You mentioned other OSes being more secure than Windows. In fact, it seems to be conventional wisdom and seemingly a "fact," according to most people. I seem to think that while Windows sees by far the most action concerning security vulnerabilities, it is also under the most frequent attack by far. Actually I disagree, but I'll explain why in a second. Just thought I would ask to know what you thought about this, seeing as security to me means more than just how many vulnerabilities are found per week when comparing two software products. I think the ratio of bad guys attacking Windows is so large compared to other OSes, comparing the security of them is much more complex than most think. Am I way off base on this one? Sorry this got a little long. Thanks for all you guys do. Signed Blake.

Steve: So what do you think, Leo?

Leo: Well, I have to say that what you're overlooking is, yes, of course there are far more Windows, what is it, almost a billion installations of Windows out there. But don't you think web servers get attacked an awful lot, too? And they're running Linux. I mean, they're the ones, they're actually the ones in many cases, Linux or

BSD or some other UNIX form, they're the kind of presenting face of a lot of computers to the outside world. Many Windows machines, most Windows machines are probably sitting behind routers. So if you want just the face of attack, I think a lot of it is going against UNIX variants. Do you agree?

Steve: Yeah, although in that particular instance it's not the OS itself that's being attacked, not the core OS. Typically it's an insecure...

Leo: Server, yeah.

Steve: Well, it's an insecure application like PHP. And so it's code. It's like it's higher level code running on a web-exposed surface of the server. One of the problems, I think, that Windows has is that it's never staying the same. That is, it's inherently evolving. Microsoft is continuing to mess with it and add new features and services. Now we have the whole new .NET thing, a whole new API that was added after we already had an existing Windows API because they said, oh, no, we're going to make it better in a whole number of new ways. Well, they still have the old API. They still have support for the 16-bit API and for DOS. And now we have .NET, and who knows what's going to come next. I mean, now we're looking at an increase of Java applications and JavaScript being run by clients on Windows, like the example we talked about with Chrome last week, Leo, where you're running Google Mail in a Chrome application window. So I wanted to bring this question up because it is something that comes up a lot. And the question is, what's more secure? I would argue that the thing that is targeted least is probably more secure effectively.

Leo: Effectively, right.

Steve: Yes, effectively. Now, I mean, one of the benefits of Windows is that it's being pounded on all the time. Problems are being found all the time, and they're being fixed all the time. The problem is, though, then, that it's constantly changing. Microsoft is also introducing new problems all the time.

Leo: Every patch has the potential to introduce a flaw.

Steve: Well, and Leo, look, just try running Windows Update. You have to reboot and run Windows Update when you install XP because the security patches have security patches. And then once you get them patched, they've got patches. So, I mean, it just proves the fact that Microsoft's updates are buggy and are introducing new problems that then need to be fixed. So, I don't know, I mean...

Leo: I think it's often said that FreeBSD is the most secure, only because it was designed to be secure from the ground up. Windows...

Steve: Do you mean FreeBSD or OpenBSD or Net...

Leo: Oh, now I'm confused. There's Free, Open, and Net, and I can't remember which one is the considered...

Steve: Open is generally...

Leo: Is it Open?

Steve: Yeah, I think Open is generally considered to be massively secure.

Leo: Written intentionally to be secure.

Steve: Yes.

Leo: So I think when you - see, Windows was not because security wasn't an issue when - let's say we're running on the NT code base. We're not running Windows 98, obviously. But even when NT was designed it wasn't really the issue.

Steve: Well, and frankly, there was security, I mean, NT was designed with security in mind from the beginning. And the original architecture of NT was much more secure than what Microsoft has devolved it into.

Leo: That's right.

Steve: Remember that NT had a strong client-server model. There was the kernel, and then there were the user EXEs, remember that User32 DLL kernel and GDI were all operating in user space. But that wasn't high enough performance. Microsoft wanted more performance. Well, there was, I mean, deliberately not high enough performance in the beginning because the original architects wanted to separate the kernel from applications running in user space. Microsoft said, oh, look, if we just move GDI down into the kernel, we'll have many fewer kernel/user space transitions, and we'll get a performance boost because, you know, we want the system to be snappy.

Well, what did we hear last week? GDI+ that was added to XP was a source of a huge number of vulnerabilities. And those vulnerabilities were much more serious after Microsoft moved that code into the kernel than they would have been had it stayed outside. So you could argue that Microsoft is, in this case, is their own worse enemy. Whereas decisions are being made, for example in the case of OpenBSD UNIX, I mean, where security is first, they're doing nothing to lessen it, Microsoft just can't help themselves because they keep believing that the next thing they do is going to be secure even though nothing they've done so far ever has been.

Leo: Well, they also live in a different world. They have to work with businesses. They have to, you know, it's a different environment. I'm looking at the OpenBSD

site. It says only two remote holes in the default install in more than 10 years. I'd have to say that's a pretty good record.

Steve: That's phenomenal.

Leo: Yeah. So I guess we'll give them props for that. But it's a different environment. You can, you know, you're not customer driven. You're security driven. So you only do those things that make sense from a security point of view, and customers be damned because...

Steve: Well, but there's also - I've always given Microsoft the benefit of the doubt when it comes to bugs. Anyone can have bugs.

Leo: Yes, of course, yes, yes.

Steve: I mean, we wish there were fewer of them. My big complaint with Microsoft is over policy. Because, for example, for so many years it was their policy to run services by default. And even today I'll install XP in a system that has never seen a wireless card, has no WiFi at all, yet wireless zero configuration service is running by default. Why?

Leo: Yeah, yeah. No reason for that, yeah.

Steve: I mean, it's nuts. And similarly, remember we were talking about kill bits. I've been thinking about this some more. This notion that VMware in their update last week flipped the kill bits, that is, enabled the kill bits of their ActiveX controls, that was such a great policy from a security standpoint. All ActiveX controls ought to be marked as not executable by IE unless they are explicitly known to be IE required, rather than the other way around. As it is now, it's called a "kill bit" rather than a "live bit." It ought to be the "live bit" instead of the "kill bit," and it ought to be off normally and only turned on if you know that this is something that Internet Explorer could be expected to use. Instead, we've given IE access to all the ActiveX controls in Windows. I mean, that's just dumb. I mean, that's clearly, on its face, that's, like, wrong. But that's not the way Microsoft thinks.

Leo: Right. But I'll defend them because they have a different imperative. And their imperative is much more complex. They don't want to piss people off. They've got to make the vendors happy, the independent software vendors happy. They've got to make business happy. And that's...

Steve: Yeah, hence we end up with things like UAC that bug people to death so much that they just - they abandon Vista, go back to XP.

Leo: They turn it off, yeah. But it's a difficult situation. I mean, I think that they

have a very difficult issue that they have to face. And it's, you know, it's nontrivial, their issues.

Steve: Well, and complexity is the enemy of security, as we've often said. And once upon a time DOS was three files. Now no one knows how many files.

Leo: That's a lot. Thomas Paulsen in Nordland, Norway shares his clever security and usage restriction solution involving OpenDNS: Hi, Steve. I'm a proud owner of SpinRite, longtime listener of Security Now!. My Top 10 list of favorite netcasts consists of all Leo's publications - thank you, Thomas - with Security Now! in a definite No. 1 position. My jaw dropped to the floor as you detailed the recent DNS spoofing attacks. I was amazed at the creative solution to adding entropy to DNS requests by using capital letters. Well, mixed case; right? The jaw again dropped as I heard the SEAL team get out of a real tight spot using SpinRite. The show you produce is, in my humble opinion, entertainment at its finest. Thank you. Thank you, Thomas. So here's his OpenDNS story:

I work as a senior consultant in IT, and one of my clients is a private high school. They run a network for their students on a separate ADSL line, and they're using a Cisco Pix 501 for security. We've got to get them moved to Astaro since the Pix is being phased out.

Steve: Yup. I thought the same thing when I read that.

Leo: The network is all wireless, with somewhere around 10 Linksys APs - access points - providing network access on campus. They have a policy for students that only "normal" Internet access is permitted. But budget restraints and lack of IT knowledge has kept them from enforcing the policy. Students take advantage of this, of course, and use the network for heavy downloading and peer-to-peer filesharing, rendering the network mostly unusable for the rest of the student body wanting to surf the web or download email. Aware of services like Websense, which the Cisco unit supports, they've been unable to afford any subscription services - oh, we've got to get them Astaro - and their limited knowledge of the firewall has kept them from blocking traffic selectively. Anyway, many peer-to-peer clients use the HTTP port or dynamic ports, so blocking them on the protocol level would be an exercise in futility. Or they use encryption now and all sorts of stuff.

So as I was driving down to see them I was listening to Security Now!, and OpenDNS was mentioned. I had, of course, heard about it previously and was using it on my home network. I then started wondering, hey, maybe OpenDNS would be usable for what my client needed. I got so excited I had to stop my car and jot down a quick plan. As I later tried to explain this to my client, I got that glazed look you often get when the level you're explaining something is 10 notches higher than the recipient is able to process. So I assured him this would save them some serious bandwidth, and I got the go for setting things up.

I created an account with OpenDNS for the high school and set up the official static IP address of the school as the network in the OpenDNS dashboard. This is, by the way, a really nice feature of OpenDNS they introduced not too long ago that lets you

configure your machines by IP address. I then configured some other options, blocking categories of sites like peer-to-peer, anonymous proxies, a few others. I then went to work on the firewall and configured it with just three simple access rules: 1. Allow UDP port 53 to only the OpenDNS DNS servers. Is 53 DNS?

Steve: Yup.

Leo: Okay. So in other words you couldn't use another DNS server.

Steve: Right.

Leo: Allow http, https, smtp, pop3, imap, ftp, ftpdata to any network. Otherwise, drop all other packets. By the way, that is pretty much the way I would configure any router; you know? This setup would make sure that the only DNS servers allowed were the OpenDNS, should some students try to mess with the IP configuration of his or her computer, which they would inevitably.

Steve: Of course.

Leo: Yeah, first thing I'd try. Also, the only port protocols that would be usable were the approved major Internet ports. The results were immediate and dramatic. The hit count on blocked networks was ticking away feverishly, and bandwidth usage came down dramatically. Oh, those students must have been really miffed. Oh, man. The stats that OpenDNS give you are an additional boon. This is really a nice feature, by the way. And this is all free, which I love. You can quickly see if there are false positives among the domains being blocked and tune them accordingly. I realize this isn't a foolproof situation, but it really gives the high school a great layer of control over the students' Internet usage, all for the great price of free. Again, thanks for a great netcast. And thanks for a great solution. That is really awesome. I think that's a very clever solution.

Steve: Well, I wanted to share this with our listeners because I could just imagine how many other listeners might have applications for this sort of solution. The configuration of the firewall is very simple. You allow UDP port 53 only to the OpenDNS servers.

Leo: The only place it can go.

Steve: So as you mentioned, Leo, what that prevents is it prevents any students from configuring a different, explicitly configuring a different DNS server for their machines. So what that means, of course, is that they have to use OpenDNS. Then by using the DNS dashboard, which is configured based on the source IP of incoming requests, that is, he configured the dashboard to the school's public IP address, so that tells OpenDNS who is asking, which allows OpenDNS to apply restriction rules on which types of sites by major classification, like peer-to-peer, transparent proxies and so forth, which ones it will respond to. So suddenly many of the games that the students were playing are shut

down completely. We know, sure, you could use an explicit IP if you knew it. But we've talked about the problems of doing that. Because as soon as you go to a site that, even by IP, more often than not you're bounced around, and you're back into domain names. And again, if it's something that OpenDNS won't be willing to look up for you, then there's nothing you can do. And then finally he simply allowed just port 80 and 443 and 25 and 110 and...

Leo: The obvious canonical report-through ports.

Steve: Yes, basically web, email, and FTP, to allow the students to surf the 'Net to sites that are fine, and to transfer files, and to do email. So, and this is what the school's policy always was. But of course the students weren't abiding by it because they're, you know, they're students. That's what they're going to do. So I thought this was - and as he said, it's simple to establish the firewall, the OpenDNS service that is part of the filtering solution works beautifully, and it's simple to configure and free.

Leo: It's just really excellent. I have to say I've been using this for some time. I have a home configuration and an office configuration, which is by IP address. You can totally control what you're doing, blocks domains and so forth. I have to say this is - OpenDNS is providing a very valuable free service to users. And you combine that, I mean, you need the firewall to make sure people are forced to use it.

Steve: Precisely.

Leo: Yeah. But I just think this is an excellent choice. So good, yeah, thank you for sharing that with us. That's very, very cool. Let's move on to our next call here. Ben Jaques in Des Moines, Iowa, wants to know what "fixed" means. In the last Security Now! you said that Google had "fixed" the EULA, but what does this mean? Repaired. Could you please explain in the next Security Now!? Thanks.

Steve: They had a broken EULA.

Leo: A broken EULA.

Steve: Got their EULA fixed.

Leo: Yeah, it does sound like an operation of some kind, doesn't it.

Steve: Your uvula.

Leo: Yeah. This is the Chrome - we were talking about the Chrome EULA, which - now, I haven't looked to see what they've changed. But they immediately apologized. They said, our bad, we used boilerplate language, and we will fix it.

Steve: In fact, one of the main Google guys who was blogging, I guess he was initially sort of snide, and I think sort of snotty in his first responses. And he later apologized, which I thought was very nice. And he said, I should have understood that we were really wrong, and I want to apologize for the nature of my initial reactions upon having people being upset with the way we were behaving. You'll remember that when we first talked about it two weeks ago, when Chrome first appeared, their standard boilerplate EULA, the End User License Agreement, EULA, it stated that they owned the rights to anything you did with your browser. Like, I mean, any data that you posted anywhere using the browser as the interface to Web 2.0-style sites. And my reaction was, well, okay, so no one is ever going to use this browser. I mean, it was ridiculous. It was ludicrous. And immediately they said, whoops.

And it may well have been an oversight, despite the fact that this browser has been in the works for two years. They said, our bad, what we meant to say was that you retain the copyrights to anything you already had the rights to. So you're giving us nothing that is yours. Any copyrights you have, you retain. And so it's like, oh. Which is why last week we began to entertain the idea that maybe Chrome had a future.

Leo: Huh. Which that idea will quickly be - you will be disabused of in moments.

Steve: Oh, yes.

Leo: Yeah, they just took that paragraph out. It didn't say we assert copyright. It just said you keep the copyright, but we get to do anything we want. We get a non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display, and distribute any content that you create with the browser. But that, you know, I have to say in their defense, that's exactly the kind of boilerplate you see. It was in, if you've ever - you've signed it a few times, the TechTV release form basically says that. We reserve the right to use your likeness and anything you do on here in perpetuity, in all media ever conceived of in any time and any place in the future.

Steve: Wait, wait, wait. Did I...

Leo: You signed it.

Steve: I signed that?

Leo: Several times. Yeah. It was kind of surprisingly broad. And a couple of people said, whoa. But that's pretty typical. And all it's saying is, look, we're going to do an interview with you. We want to be able to use this. And we may, some day there may be some virtual cube presentation we'd like to do that we never heard of, so we'd like to be able to do that. And by the way, they still retain those rights. And G4 Comcast now has them. I don't know what they're going to do with it. But I don't, you know, none of us have any rights to anything we did on TechTV.

Steve: Right.

Leo: That's pretty typical. And I think that that just leaked in because they just - they were too lazy to write a new one. Or maybe, as some people think, they thought they could sneak it by, and then...

Steve: No, I don't - I can't even imagine that. It was so bad. I mean, it said so clearly, we own everything you do. It's like, uh, yeah.

Leo: So it's fixed. They took that paragraph out. Corby in Reno, Nevada shares his different view of Google's Chrome browser. "Browser" in quotes, I might add. Hi, Steve. Not for a second do I think Google is trying to compete in the browser market. How could anyone compete with Mozilla? Rather, Google is making a new platform to deliver their web-based apps. I think that's basically what I've been saying. I'm sure they're finding that the current browsers are too limited for what they want to do. They don't need to be concerned about all the issues about Chrome that you mentioned in your recent episode. We'll have the Firefox browser running side by side with Chrome as a Google app machine. It might look like a browser. That's just a side effect. Soon their apps will have APIs that only Chrome will know, and only Chrome will be able to run them. I disagree with that. I don't think they're going to do that. That would be crazy. And if we thought Microsoft once had a monopoly, just wait till Google controls the apps and the data. Call me paranoid. We've seen this cycle before. But it's going to be coming at us faster and bigger than ever. You think that's going to happen?

Steve: I don't think it's going to happen. But, I mean, I wanted to share Corby's view. I think the problem is that it is a browser rather than being a simple app machine. And so it does need to offer the features that contemporary browsers have.

Leo: Because people will use it that way.

Steve: Well, they will. I mean, and they'll get bitten by its lack of security and privacy features unless they're very careful. I mean, I think it's very clear that - and by the way, Chrome's share has continued to fall.

Leo: Oh, interesting.

Steve: As people have uninstalled it. And, well, for what good that does, and we'll cover that in the next question. But it's unfortunate that, in my opinion, that it's not, as is, a highly useful browser. You know, everything that they were doing in terms of the work they've done with the security model profiles it as wanting to be a mainstream web browser. So, I mean, certainly there is a problem if their apps won't run in non-Chrome browsers. I can see that Google wanted their own, wanted to own a platform that their future apps are going to run in. I don't understand how it forces other browsers to follow if their apps run in the other browsers without any modification. So, I mean, it is sort of a - it's a strange animal, in my opinion.

Leo: Yeah. I'm looking to see if it's changed, the browser usage has changed. You say - you're seeing a drop-off, huh?

Steve: Yup, I did see below 0.9.

Leo: Let me - I have to select, let's see, just this week, let's try.

Steve: Oh, I see, your own TWiT browser usage.

Leo: Yeah, because of course our audience is really sophisticated. So I would imagine that they would be very quick to try it, but that it would drop off. Yeah, it's now 7 percent. Which is down a little bit, but that's still a fairly large percentage. 8,000 people still using it. Firefox 56 percent, Internet Explorer 18 percent, Safari 13.9 percent, Chrome 7 percent. So it's down a little bit. But not, you know, oddly enough, not as much as it is globally. So I think our audience, they like this stuff. They like to use the latest greatest, don't they.

Steve: Yeah, just wait.

Leo: Steverino, are you ready? The "Bad Chrome-Osome," from Richard Chao of Fullerton, California. Steve, when I installed Chrome, it apparently also installed some plug-ins into my Firefox 3. What?

Steve: Uh-huh.

Leo: Then, after I uninstalled Chrome, the plug-in and files remained in the Mozilla Firefox directory. I was able to disable the plug-in, but when I went into the Mozilla Firefox program files in the C directory to remove the folder called Chrome, it broke my copy of Firefox. This is not good. Firefox was easy to remove and reinstall, but I'm worried about IE. Have you heard anything about whether Chrome installs files in IE or not?

Steve: Yup.

Leo: This is another reason to avoid Chrome. I was never asked by Google if I wanted a Chrome plug-in, it just did it. Wow. This is the first I've heard of this. What's the story, Steve?

Steve: It's bad.

Leo: That's terrible.

Steve: I remember you - I was thinking how you chuckled when I told you I had just created a VMware container.

Leo: Yeah, you were right.

Steve: Well, I'm glad. Get this. When you install Chrome, with no notification at all, it installs plug-ins for Firefox 3 and IE. It instantiates a browser helper object, an ActiveX control for IE, an add-on under Plug-ins called Google Update. It also runs a Google Update service in your system and deliberately leaves all of that in place after you remove it.

[LEO: Hi, this is Leo. I'm going to interrupt here because - this is somewhat after the show was recorded. After the show was recorded, Steve did a little more research and was able to verify that Google Update does remove itself from the PC, not immediately, but some time after Chrome has been removed. In fact, Google says this in their own Help documents at the Google site. So he's going to test this more extensively. But perhaps it's not as bad as it seems. Also want to let you know that we found out, thanks to our chatroom, that the Chrome folder that our correspondent removed in fact isn't Google Chrome, but Firefox Chrome. It's a critical part of the Firefox user interface. So removing that Chrome folder from Firefox will, yeah, it'll disable Firefox because it is part of Firefox. And even if you haven't installed Chrome, you'll have that folder. In any event, I wanted to let you know that it may not be as bad as it seems. But Steve is going to take this next week to do some research. And we will get you the update on what Google is doing with Chrome, what Update is doing after it installs itself. And frankly, I asked him to also maybe take a look at some other applications, like Apple Safari, that may in fact have exactly the same behavior. All right. We now return you to our show, which is already in progress.]

Leo: Well, we're going to do more research on this and get back to you next week with more about exactly what this is doing.

Steve: Yes.

Leo: All right. Hey, thank you, Steve Gibson. Fascinating stuff. Go to GRC.com to find out more about what is going on in your world when it comes to security. GRC.com, you've got the show notes there. You've got the 16KB version of the show. Of course you've also got all of Steve's cool stuff like ShieldsUP!, his many free security programs and utilities, too, like Wizmo. And let's not forget, of course, the crown jewel in the operation, SpinRite, the world's finest disk maintenance and recovery utility. It's all there at GRC.com. And I want to take a look at what exactly is going on. Apparently Google's Updater is installed by a lot of other Google applications, as well. This is something that's kind of part of a Google package that you automatically get. And again, this is, by the way, what Aureate said is, well, we can't uninstall Aureate. It might be installed by other applications.

Steve: Yeah.

Leo: So their Chrome probably says, well, we don't know if you've got Google Earth installed, or Google Toolbar; so we can't uninstall these updates because you might have other things. I have to say, if you're using Google at this point, you might want to reassess your association with Google. I certainly am. Thank you, Steve.

Steve: Talk to you next week, my friend.