Listener Feedback #113

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-292.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-292-lq.mp3

Leo Laporte: It's time for Security Now! with Steve Gibson, Episode 292 for March 16th, 2011: Your questions, Steve's answers, #113.

It's time for Security Now!, the show that covers your security and privacy online with the man of the hour, Mr. GRC, Steve Gibson, of Gibson Research Corporation.

Steve Gibson: Or hour and a half, as the case may be.

Leo: Or two, you know, whatever. The man of the next 90 minutes or so. Hey, Steve.

Steve: And we spared our listeners about 40 minutes of you and me yammering about Japan and iPad 2, so...

Leo: And diets. And diets. Which is the thing they least wanted to hear...

Steve: And what is it that makes you fat.

Leo: Yeah. But I think that the earthquake stuff is very interesting. And maybe just a little footnote, you found a very good explanation of how these boiling water reactors, the kind that are in Japan, work. Almost looks like...

Steve: With diagrams.

Leo: Yeah, like how things work. It's on the Nuclear Regulatory Commission website, NRC.gov. They have, I guess, a lot of teaching material, student material.

Steve: I did tweet all this, also. So if anyone wants to get links for all this, you can just put in - go to Twitter.com/SGgrc, which will be my Twitter feed, and you can scroll back a little ways because I tweeted all these links to the stuff that I was finding. The MIT article that you found, that really great blog posting, Leo, and also this diagram.

Leo: Yeah, this is just one last point, which is that those of us who are technically inclined, which I presume is anybody listening to Security Now! for sure, just want to know facts.

Steve: Yes.

Leo: And the problem is there's so much polemic and rhetoric associated with your position, whether pro or anti nuke, and I just want to know the facts.

Steve: And the blondes are nice to watch on the news, but...

Leo: But they're nitwits.

Steve: They're not nuclear scientists.

Leo: Even CNN, nobody has really done a very good job. I saw an explanation of how a nuclear reactor works yesterday that was just wrong. And, look, we were talking, Steve and I were talking, I remember when I first got an Atari there was a great nuclear simulator called SCRAM. And it was very simplified, of course, but you had to be - you were a nuclear operator, nuclear generator operator, and you had to run the rods and scram the rods and so forth. It was so much fun. And I learned a lot on the basics of how a nuclear generator works. I wish that game were still around. I'm going to see if I can find it. Maybe an emulator would have it.

Steve: I was reminded that I tweeted this morning, I found a link to a really neat professor, nuclear professor guy, who's got hair like Einstein.

Leo: Well, that's his credential right there.

Steve: And I tweeted, I said, for your less techie friends, because people who follow me probably are on the techie side, for your less techie friends, you might want to send this link to a kindly nuclear professor explaining...

Leo: A little German accent?

Steve: ...very simply how reactors work. He did a great job talking about the boiling water reactors in Japan, so...

Leo: This was the game. These are screen shots. Chris Crawford did it, who is a very famous simulator designer. And you learn a lot from stuff like this. I wish these kinds of games were still around.

Steve: Simulations actually are very, very powerful for teaching these kinds of concepts. I mean, simulations of anything, physics simulations, for example.

Leo: Yup. I'll see if I can find a - it would be really fun to find an emulator. I know there's good emulators, Atari emulators out there. So I'm sure I can find - if I can find the ROM, I can probably get it working. That'd be kind of fun. Somebody should make an Atari emulator for the iPad. Wouldn't that be fun? Apple would never approve it.

Steve: Yeah, it could run all the classic stuff.

Leo: Yeah. Apple would never approve it unless Atari did it. So let's get to the news. This is a Q&A session; right?

Steve: Yup, #113. But Security Now! #292, so don't let that 113 throw you off.

Leo: Very confusing. We've got two numbers. But we know you can handle numbers. That's why we do it. Steve, what's the latest security news? Speaking of perfect.

Steve: I think you should settle for amazing, Leo. You are amazing.

Leo: Amazing, if not perfect. Imperfectly amazing.

Steve: We'll be happy with amazing. So the good news is nothing happened.

Leo: Yay.

Steve: In terms of updates since the pre-Pwn2Own flurry of updates last week. We're going to cover in detail the consequences of the Pwn2Own competition shortly. But no updates to talk of, to speak of. Although we need some because exactly as I predicted, and shortly after we recorded last week's podcast, I got a little advisory update from

Microsoft. They send email when they revise their existing updates. And I thought, hmm, what is that? So I went to the advisory update. And under "Why was this advisory revised on March 11, 2011?" it says, "Microsoft revised this advisory to announce that Microsoft is aware of public proof-of-concept code being used in limited, targeted attacks."

Leo: Pwn2Own.

Steve: Users that, well, no, not - this is before that. This was the MHTML vulnerability which we commented on them on Tuesday not patching. They fixed other stuff. And...

Leo: Is it in IE9? Because IE9 is now official. Maybe they figured, well, we'll just update IE.

Steve: It's actually not. It's in a library in Windows. So...

Leo: So it's everywhere.

Steve: Exactly. It's accessible through the browser. But it's a Windows DLL that you get to through the browser and you exploit through the browser, so it's very likely that you can get to it through IE9, as well.

Leo: Great.

Steve: Now, again, the moment this happened I tweeted about it. So that's one way you can find the link. There is a Fixit. And so I will say again, as I said last week, when I said last week we're probably going to shortly see exploits of this. Well, now we are. And the Fixit simply disables scripting in the MHTML pseudo protocol. And the MHTML is MIME HTML, which is Microsoft's own format for storing a whole page in a single archive.

Leo: Just like their web archive format.

Steve: It is their web archive format, which is .mht or something.

Leo: Right, right.

Steve: And so that's the file format. So you could argue that we never needed scripting in that anyway. You want to snapshot a page, you wonder why you need to run JavaScript in that. It's a vulnerability there that is the problem. So turn it off. I mean, and leave it off. Even after they fix it you could leave it off because lord knows whether they're actually going to fix it, or let alone when. So we'll probably wait a month for this to get fixed. So there is a Fixit that you can access to just simply disable the scripting for this particular file format, and everyone should do it because it just - no one needs it on.

Leo: Even if you have IE9, even if you've updated, you should do this because it's not...

Steve: Yes. Yes. It's going to be - it's browser agnostic, across all their OSes and all their browsers. Meanwhile, at the beginning of this week, Monday, Adobe confessed to knowing of a new Flash zero-day exploit. Our old friend the authplay.dll is back for more. We keep talking about authplay.dll and various ways that you can access it. In this case, it can be accessed through Flash, and there are exploits in the wild. It's exploited with a Shockwave Flash embedded in a Microsoft Excel file, delivered as an email attachment. So when Windows views this Microsoft Excel file, it allows the Shockwave Flash to run because you've got Flash installed. And that accesses this authplay.dll vulnerability. And it's across everything - Windows, Mac, Linux, Solaris, and even Chrome and Android platforms. So nothing to do about it at this point, unfortunately. Hopefully Adobe will get us a fix shortly. I think they'll do it out of band. Their quarterly update concept isn't really working very well.

Leo: It only works if you only have bugs every three months, you see.

Steve: On their page they said, well, because our 10.x, I think it was, was it Flash 10? I don't - no, it wasn't Flash, it was Reader 10. The Reader 10 sandbox does contain this. We won't be updating that until July. And that's like, okay, wait, March, April, May, June. Okay, well, that's fine. Now they're saying there's containment there, so they're really trying to not update when they don't have to. But they're going to have to update Flash here any day now. So they are working on a fix, so maybe next week we'll be talking about a fix for this. In happy news, Twitter has added always-on HTTPS to their site.

Leo: Yay.

Steve: Much as Facebook has, kind of, as we talked about last week, that they turn it off, Facebook, that is, turns it off if necessary.

Leo: At the drop of a hat.

Steve: Yes. But Twitter has it on. So what that does is it enforces an HTTPS connection at Twitter.com. You normally, if you were to go to Twitter with http://twitter.com, you would be moved to HTTPS for the login, to protect your login credentials; but then, as used to be the case with Gmail, you'd be taken back to nonsecure. Now, on the settings page, the main settings page of Twitter, at the very bottom of the page is a checkbox that just says "Always use HTTPS," which everybody should go and check. Now, the bad news is they haven't extended that over to mobile.twitter.com. So even if you have it checked on your login at Twitter.com, you can log in at mobile.twitter.com, and it won't be secure. But you can manually use HTTPS at mobile.twitter.com, and it will be secure. So you're still responsible for doing that over on the mobile side. And they have said that they're going to work on integrating those two so that the setting, your main settings page at Twitter.com will also have an effect over on mobile.

Leo: Is that because mobile phones tend not to be fast enough for HTTPS, or don't support it, or is there an issue with HTTPS on mobile?

Steve: I can't imagine. Remember that it's only when you initially connect that there's any...

Leo: Overhead.

Steve: Yes, overhead. I just think that they must have server farms that are not integrated. And there isn't, like, separate account settings over at mobile. So they just sort of haven't gotten there yet. I imagine that they'll cross-enforce it as soon as they're able to get around to it. And I did want to note, actually this is thanks to someone tweeting me, Simon Zerafa, who I think is in Wales, made a comment that, while in your settings of Twitter, go over to the connections option page and just scan through all the apps that you have permitted to have access to your Twitter and remove the ones that you're no longer using. I removed five.

Leo: Really good idea.

Steve: Yeah. Because remember that we're authenticating Twitter apps. And then so often we're, like, using different ones, and then we end up stopped using those. I've switched over to TweetDeck. I gave up on Seesmic because it was hosted on that horrible...

Leo: Twitter's down right now, of course, so you can't do that. But when it comes back up.

Steve: For those who are not listening live.

Leo: And Twitter has deprecated these third-party apps because you're not seeing the ads. So they're discourage- they say, don't write any new ones. They're saying, well, if you already have one, okay. But they'd prefer you didn't use those. So I have a feeling in time those old apps will not - you'll be using Twitter.

Steve: I gave up, I was using Seesmic for a while.

Leo: I like Seesmic.

Steve: And they moved it over to Silverlight, which is just a monster. I mean, it makes Flash look good.

Leo: Really.

Steve: It's just horrible.

Leo: Oh, that's interesting.

Steve: It really is. It's big, and it doesn't terminate when you shut things down, and oh, it's just awful. So anyway, it would stop working reliably. And I see everyone's using TweetDeck, so I thought I'd give that a shot, and I'm liking it a lot.

Leo: Now, that's Air, though; right?

Steve: That is on Adobe Air, yes.

Leo: You can't win.

Steve: I know. So the Pwn2Own results from Vancouver...

Leo: Oh, this was exactly as predicted.

Steve: Yes. CanSecWest Security Conference. Safari collapsed in five seconds.

Leo: [Cackling] I'm sorry. That was a cackle. I apologize for cackling.

Steve: And remember that Apple plugged 62 security holes that morning. They should have plugged 63.

Leo: Apparently. Charlie Miller wasn't worried. Actually he didn't do it.

Steve: No, he didn't. He did join up with another guy, Dion Blazakis, I think, Blazakis, and the two of them did an iPhone exploit the night before, working, like, a lot to make that happen. So basically Safari, IE, iPhone, BlackBerry, all collapsed. Significantly, neither Firefox nor Chrome did, although one researcher was a little annoyed because shortly before this he had given Google a heads-up on a cross-site scripting vulnerability which was not previously known, which he could have used to score himself a Chrome exploit for Pwn2Own, and 15 grand. As it is, he only got, what is it, $1,337.

Leo: Well, how dare they fix that exploit before Pwn2Own? How dare they?

Steve: And in fact I think it was Charlie who did make a comment that this was sort of a downside of Pwn2Own because it was tending to cause researchers to hold back their disclosures because it was worth 15 grand, which is nothing to sneeze at.

Leo: Well, and Google added 20 grand on top for Chrome.

Steve: Yes.

Leo: So clearly that was cockiness on Google's part.

Steve: Yeah, but they and Firefox survived Pwn2Own. So it took Safari five seconds to fall, although in fairness this was an exploit that was worked out well in advance so that, essentially, the guy who did it just walked up, plugged his code into Safari, and it collapsed.

Leo: That's how it works. It's not like you sit - I think people think, oh, you sit down at the machine and you try stuff. No. They know exactly what they're going to do. They have a USB key, they plug it in, they go boom.

Steve: Right. Ha ha.

Leo: Ha ha. Give me the money.

Steve: IE8 fell to Stephen Fewer, who's got a small, I think it's a one-man security company, Harmony Security he calls his company. And his exploit was interesting because in order to do it he had to chain three previously unknown, unpatched vulnerabilities, together The first two of then were to allow him to get past IE and Windows ASLR, the Address Space Layout Randomization protection, and DEP, the Data Execution Protection, which we've covered in depth in past episodes. And then the third one, which he said was extremely difficult to exploit, got him out of the sandbox, which protects IE8. He got out of IE8, he busted out of IE8's sandbox and wrote a file to the system, which demonstrates that IE8 sandbox was no longer in control. And Microsoft immediately responded, we're already on the case. And I thought, well, I feel so much better knowing. Oh, joy.

Leo: We'll fix that. Next week. Maybe the week after.

Steve: We're on it.

Leo: Sometime. It'll be fixed.

Steve: Exactly. And then BlackBerry was brought down, the BlackBerry browser, by a multinational team who attacked the Torch and in seconds had it taken down. So, and

RIM said, oh, yeah, we're going to fix that, too. So it's like, okay, fine.

Leo: It's really interesting. Wow.

Steve: I did want to note, as you've mentioned before, that IE9 was released a few days ago, Monday of this week. It's final for download. It's got so much in it that I'm going to give it a deep security review podcast, which we will do maybe next week.

Leo: Oh, great.

Steve: I think it needs that. And I did notice that, at the last minute, a do-not-track header was added, after the RC apparently, which is really good news. I mean, I like that solution. That's of course the one that we've talked about that Firefox has, where every query just says "Please don't track me," essentially. Now, IE9 is already coming under attack for their tracking blocker lists, which I will go - we talked about it before, but as part of my full IE9 security review I'll talk about it in detail. The problem is that users can load multiple lists, which both block and permit sites. And the problem is that the logic that's used is such that, if you load a list which allows, that overrides any other list which blocks, which sort of seems like the wrong thing to do. So I'm going to look into it in more depth, and we will cover it thoroughly. But I did want to acknowledge IE9. I mean, it is a big step forward. I mean, this is a worthwhile browser. You might argue that it's about 10 years too late, but Microsoft has really moved the bar and has created a very nice browser which I think is state of the art now, along with Chrome and Firefox, which I think are the - now we have three state-of-the-art good browsers. I don't know if IE9, I don't think it's going to win me back because it took a lot to pry me away from it.

Leo: Right, right.

Steve: I'm over on Firefox now and very happy. I know that you're over on Chrome and very happy.

Leo: Yeah, I love Chrome. And I guess the results of Pwn2Own kind of justify our support of either of those.

Steve: Yes, yes, good point. Our two browsers did not collapse.

Leo: You have NoScript, which is a really good reason to use Firefox. I don't know if there's a...

Steve: I do, although there is a script manager now for Chrome.

Leo: Oh, there is?

Steve: Yes.

Leo: Oh, good, I'll get it, okay.

Steve: Yes. It's...

Leo: What's it called? Do you know?

Steve: I don't remember the name. It's similar to NoScript in name, but there is one for Chrome.

Leo: I will check it out. I'm sure the chatroom will tell me in just a second.

Steve: And our friends, yes, our friends at...

Leo: It's called NotScript.

Steve: That's it exactly. I knew, I remembered the name was very much like NoScript.

Leo: Chatroom says, "NotScript."

Steve: Yup. NotScript for Chrome.

Leo: Yeah.

Steve: And again, I do recommend, I know you don't like this selective scripting. I'm using the temporarily allow scripting so often that I'm wishing now that NoScript - are you listening to this, Giorgio? - that NoScript could give me the option of a toolbar button.

Leo: Oh, yeah, that's a good idea.

Steve: Instead of doing the right-click and then temporarily, just give me a button that says "temporarily trust this site." Because I don't want to be adding sites all the time to my trusted list that I'm probably never going to go back to again. There are sites like Amazon and eBay and Twitter and lots of sites that I'm using frequently, I would like to have on my permanent trust list. But most of the time I'm just somewhere that I'm probably never going to go, I'm browsing around. And that's where you want script blocked by default. And I look, and I go, okay, looks like it's not come up. So then I - it'd be easy, it'd be nice if it were easier to temporarily add a site to the trust list.

Leo: Sometime we will talk about hashbang, because this is something that Twitter uses, a lot of sites are starting to use this as a way of making an AJAX-y page. And when you go to Twitter.com, I don't know if you've noticed this because you have to allow scripting or you can't even load Twitter because instead of getting any HTML at all, you get a big lump of JavaScript, which then renders the page after the hashbang. And this is being used more and more widely. Gawker's using it on their sites. And it really breaks the Internet in some very interesting ways and absolutely requires JavaScript. You don't get anything. There's no graceful degradation. You get nothing.

Steve: And that's so dumb because all you have to do is put, I mean, put something in NoScript tags, and then you see that...

Leo: Well, the reason they don't is they want these dynamic pages that, you know, if you go to Twitter it's rolling and scrolling and things are updating and all of these chunks are all loaded as AJAX chunks instead of HTML rendered. So it would remove considerable amount of functionality. But I think they have - I don't, well, this is a big debate going on in the...

Steve: So I guess what you're saying is that they have gotten themselves so committed to scripting that the site isn't at all usable with JavaScript disabled.

Leo: And I think probably that's going to happen, Facebook and everybody else, because they want these - it's web apps. They want their page to be not a page as we understand a web page, but to be an app.

Steve: I'm a JavaScript programmer now.

Leo: You have to be.

Steve: No, I mean, in the last few weeks I started, pretty much from cold, and I have a JavaScript page running on GRC, a capabilities and compatibility test page which I'll be making public...

Leo: Well, you can see how powerful it is. I mean, it's incredible.

Steve: It's a very useful system. And you're right, when you add this HTTP query facility, which we've had since IE5, that allows JavaScript to query back to the server and get other things, you're right that instead of this notion of going from, like, clicking links to go from page to page, the state-of-the-art approach now is that you go to a site which is an application, very much like Flash-enabled sites used to be, where you sort of stay on the same page and just browse around within that one page using Flash to take you to different things and do different things. Now that same capability with JavaScript and the Document Object Model and DHTML and all that, has come so far that it's possible now to do that without using Flash, just using scripting. So, yes, unfortunately, I think scripting

is clearly the way sites in the future are going to be written and built.

Leo: You should look at jQuery, which is of course a client-side library; and then Node.js, which is a server-side library. That's what these sites are using. Mostly Node.js. It's very popular, gives you great functionality, really cool web pages that totally suck. By the way, just an update. Tim O'Reilly just tweeted - Twitter's back, but it just got back - has tweeted that the Mark 1 nuclear reactor design used at the Fukushima plant caused GE scientists to quit in protest at the time. This is from ABC News, so, fascinating. Story still coming out. And I don't know, again, but there's a lot of information, and we've got to sift through it. We're going to try to get some intelligent people on to discuss this at some point.

Steve: So our friends from San Diego and the University of Washington, whom we discussed last year hacking a car by hooking their laptop into the car's network, are back.

Leo: Oh, boy.

Steve: They gave a presentation recently where they demonstrated three new means of hacking into existing cars. They used an undisclosed model of a 2009 auto which they sort of deliberately used because it was an older car that was presumably less vulnerable than newer cars. They were able to take the car over by playing music. Now, this shouldn't surprise anyone...

Leo: Oh, boy.

Steve: ...because all this means is there was a vulnerability in the...

Leo: Player, yeah.

Steve: ...CD player software, a buffer vulnerability that we're used to dealing with all the time on our PCs. And so a specially crafted MP3 file was able to load a trojan into the car's operating system, rewriting the firmware, in order to give them control. They were also able to get into the car by Bluetooth and by cell phone.

Leo: Whoa, boy. That's not good.

Steve: So this is not good. I mean, again, it ought to surprise nobody. No one who's listening to this podcast ought to be surprised. I mean, these are rolling computers. And unfortunately it's important, just like nuclear reactors, to have safety systems that function correctly. It's important that our rolling high-speed multi-ton computers on wheels be secure. And it's incredibly difficult, if not well-nigh impossible, to achieve that. And these guys have shown that it's possible.

Now, I did want to back off from this a little bit and say that they had made a specific

comment which I thought was important to understand, that these attacks are extremely car specific. That is, no attack that they designed would work on any other car. So it's not like Windows, where we're all using IE8 or we're using Windows 7, and we have a massive code base which is almost universal. In this case, it would only work on a given make, model, and year of car with a specific version of firmware. So they specifically found vulnerabilities in an instance of a car, rather than something much more weaponized.

But the other thing we know is that, over time, these things get easier. I mean, these attacks mature. If you want an example of maturity, just look at Stuxnet, which we covered last week. So this is something that we'll certainly be keeping an eye on. Many people wrote to me and tweeted about this music taking over a car. It's like, uh-huh, well, who would be surprised by that?

Leo: Amazing.

Steve: They're computers, and they're going to have buffer overruns, and that allows code to get injected, and that's what happens.

Leo: Well, the only surprise is you'd think that the car computer would be isolated completely from the music player.

Steve: It's more expensive to do that.

Leo: Well, they will in the future, I hope.

Steve: Yeah, I mean, you're right. You would hope that. And in fact, in the photo, they showed the instrumentation, "pwned" was the word showing in the instrumentation of the car. And remember that they were able to stop and brake and literally really control the car.

Leo: That's so horrible.

Steve: Control its functioning. So I think we really are going to need, well, there's a commercial on TV now where Dad's talking to his teenage daughter, and he says, hold on a second, you can borrow the car, let me start it for you. And he presses a button, and the car starts. I just think, oh ho ho ho ho ho, help us.

Leo: Why not just use Bluetooth. You know Bluetooth's secure. There is no problem there.

Steve: Oh, god. Well, finally, in the news, the U.S. Pacific Command - I thought this was interesting, a little unrelated story but interesting - requested 13 high-profile sites be blocked across the Department of Defense's .MIL network in Japan to conserve bandwidth.

Leo: YouTube?

Steve: YouTube, Google Video, Amazon, ESPN, eBay, DoubleClick, EyeWonder, Pandora, StreamTheWorld, MTV, iFilm, MySpace, and Metacafe.

Leo: I love it.

Steve: It's like, okay, now, wait a minute.

Leo: That's all the fun stuff.

Steve: Exactly.

Leo: But really, it is a military network.

Steve: This is a .MIL network, and they're streaming Pandora? It's like...

Leo: They're having fun. Well, hey, look, they're at an office. They want some music.

Steve: They need some tunes.

Leo: I'm glad they didn't block TWiT, you can keep listening to TWiT until they discover us.

Steve: And Facebook. They didn't block Facebook. It's not on the list.

Leo: Well, it's probably, you know, most of those are rich media sites. They're video and/or music sites. So those are the ones that use a lot of bandwidth. Facebook probably isn't as bad.

Steve: Yeah, well, yeah, YouTube, Google Video.

Leo: Pandora.

Steve: Amazon now has video streaming that they're offering. Wow. So anyway, sorry, guys, you're going to have to work over there in Japan.

Leo: I think the generals use Facebook, so they didn't want to block it. That's how the generals stay in touch.

Steve: And one little bit of errata that I wanted to mention. When I logged into Google Docs this morning in order to prepare the document that you and I are looking at right now, Leo, and which you'll post...

Leo: Yeah, already have.

Steve: ...I got a little reminder screen that said, imagine how it would feel if you weren't just able to log on.

Leo: Oh, yeah, good. Good for them.

Steve: That wouldn't be good, would it. And I said to myself, no.

Leo: It wouldn't.

Steve: And they said, here's the information that we have for you, which is used for access recovery. Is it still correct?

Leo: Good. Brilliant.

Steve: And I thought, wow.

Leo: Brilliant. Love them.

Steve: Very, very cool that they were proactive in, like, saying every so often, is this information still correct?

Leo: That's just good sysadmining. I mean, that's what, in a business, your sysadmin will go around and say every three months, change your password, we're going to lock you out unless you do. Google has some really - the problem with recovering your password with Google if you don't set up things like an SMS number is it's really tough. So they're proactively saying, make sure you have a phone number that we can SMS, and make sure it's up to date. And this is advice to everybody, if you don't have that secondary means of notification, besides your email. Because if somebody hacks your account, unless they get your phone, that SMS - I guess they could change the SMS. But that's why you want to check it regularly.

Steve: Yeah. I was very impressed that Google proactively reminded me.

Leo: That's great.

Steve: We'd like to see more of that.

Leo: I think they can't change the SMS unless they send you a text message saying, do you have this phone, is this a new phone. I think they - I hope they would do that. Very important.

Steve: And speaking of support, I got a nice note, a different twist on SpinRite from a listener, Anthony Ungerman. He said, "Hi, Steve. I purchased your software about two years ago in support of Security Now!. I had no immediate need for SpinRite, so I soon forgot about it."

Leo: That's fine.

Steve: "Well, this Friday I had a few drives that needed some SpinRiting, but I could not find my download codes anywhere. I sent your support alias a 'Help!!!'" - with three exclamation points - "email at 7:15 p.m. on a Friday night. By 7:26 I had received a reply containing the codes I needed. The download took a second, and the system created a bootable CD a few minutes later. I had SpinRite up and grinding away by 7:45 p.m., and I made the 8:00 p.m. date with my family for a Friday night movie. Do me a favor and call Dell, Linksys, et cetera..."

Leo: And let them know.

Steve: "...and teach them how to do support. It would more than likely have taken three phone calls and a lot of waiting to get the same level of service."

Leo: Absolutely.

Steve: "Thank you very much. Anthony."

Leo: Isn't that great.

Steve: Thanks for sharing that, Anthony.

Leo: Now, is that automated, or do you have a tech guy sitting there?

Steve: No, that's Greg, who checked his email.

Leo: Awesome.

Steve: And probably sent it over to Sue, and she checked hers, and she looked him up in our database and said, oh, yeah, here he is. And then we sent him email containing his download information.

Leo: Isn't it great when you have a great team that is just there and works hard.

Steve: They're the best.

Leo: Love it. Steve Gibson, I have got questions, if you have answers.

Steve: You have to look at this professor. Can you real quickly go to...

Leo: Yeah, what is his URL?

Steve: Go to Twitter.com/SGgrc.

Leo: Okay, that's your Twitter handle, all right.

Steve: To get my feed. And it's the most recent link.

Leo: All right. You have to, I think you have to type https: now to get - oh, it's down again. Thank you, Twitter.

Steve: .

Leo: You see, by the way, that hashbang in there? So if you type SGgrc, it adds that hashbang to render the page. And so that's what we were talking about. It basically is a lump of JavaScript you'll see that comes in, and then the page is rendered. So you enter SGgrc, but it - so apparently the servers are enough up to give me the hashbang, but not the data.

Steve: I just put in twitter.com/sggrc.

Leo: Yeah. Maybe it's just me. That's what I put in.

Steve: Oh, and it comes right up.

Leo: Is it coming up for you? No. Maybe it's just our network. Twitter doesn't like me. I'll get it before the end of the show, I'll get...

Steve: It's a little - and I would give you the link, but it's a YouTube shortcut, and I couldn't even begin to...

Leo: I will get that for you. I will put it in the show notes, too.

Steve: Oh, the guy is just wonderful.

Leo: I hope they have the good German accent.

Steve: He's got the best hair. In fact, somebody said, he said, somebody sent back to me, said, well, that guy explains things as clearly as you do, but he sure has a lot more hair than you do. Like, yeah.

Leo: Maybe you should grow your hair out there. You should grow it out. And maybe have a German accent. That would be very...

Steve: I don't think he's ever cut his hair, that crazy Einstein guy. Anyways, well, it's a really nice presentation.

Leo: I love it. I love it. It's not Cliff Stoll, is it? We used to have him on Call For Help. He wrote a book called "The Cuckoo's Egg," where he talked about tracking down the...

Steve: Okay, if you go to YouTube and put in...

Leo: I got the link from our chatroom.

Steve: Oh, good.

Leo: The chatroom is - chatroom, you rock.

Steve: He's just wonderful.

Leo: Chatroom rocks. Nuclear reactors in Japan. Oh, my god, look at his hair. That's great. Oh, my god. That's fantastic.

Steve: He does a great - and in fact his desktop, you can see it toward the beginning, the screen blanker kicks on after a while, but his desktop looks a bit like mine, you know, basically covered with icons.

Leo: This is great. And you liked his description of how reactors work and all that stuff.

Steve: Oh, he does a beautiful job and really covers the whole thing in about eight minutes.

Leo: Fantastic.

[Clip] I have quite a personal interest in this because I went to Sendai six years ago...

Leo: This is great. All right. We'll put the link to that in our show notes. And you could just search for it. Let me just see what you would search for. You go to YouTube.com and search for "nuclear reactors in Japan."

Steve: That would probably bring it up.

Leo: It's from Periodic Videos is the YouTube channel, Periodic Videos. This is actually kind of neat. The periodic table of videos from the University of Nottingham.

Steve: And he's got a - his tie, at one point we're looking down at the table because he's got some balls, and he's showing how neutrons split atoms. And you can see his tie is the periodic table. I mean...

Leo: Oh, this is - that's my kind of guy. Look at these guys. So, yeah, in fact, if you go to PeriodicVideos.com, all the videos are here. And the very first one is Nuclear Japan. So this is the University of Nottingham in England, which is a great engineering school, very well-known engineering school. So, good. PeriodicVideos.com. Fantastic. I can't wait to watch that. Maybe, you know what we'll do, for those of you watching the live stream, right after this show, in between this show and This Week in Google, we'll run that video because it's only eight minutes long. Are you ready for questions, Steve?

Steve: Let's go.

Leo: Question #1 from Chicago, Illinois, Jeff says: I wonder about reverse DNS. Steve and all, I recently found the podcasts of Security Now!, am enjoying them, learning a lot. Thank you, we appreciate that, Jeff. I did have one question about the reverse DNS message under the ShieldsUP! proceed page. It was "The text below

might uniquely identify you on the Internet." One time it showed me no listing, and it was rated as a good thing. Then, after an hour or so, my DSL or ISP listing was on that page. His own IP address, I presume. Which I guess is bad? Someone could track your descriptors? What would keep this IP/DSL listing from showing up to begin with? And why would it later show up when I did a ShieldsUP! scan? I did switch to a dual boot with Linux/WinXP, maybe that has something to do with it. Keep up the good work, and thanks. Jeff in Illinois. I've seen this before. So you do a reverse DNS lookup on his IP address.

Steve: Yeah, sort of as part of what ShieldsUP! does, sort of as a privacy heads-up, I check the reverse DNS of everyone connecting and just show them what theirs is. In some cases, it's nothing but their IP address, like with the digits reversed and then a suffix of their ISP or something else. But in some cases it looks more like an account name, which is, even though their IP address might be changing, their reverse DNS doesn't change. That is, it does actually uniquely identify them. And so...

Leo: So it's a machine name, in effect.

Steve: Well, really it's whatever the ISP wants it to be because the DNS provider determines when a reverse query is made, what they'll say, what they'll send back. So some ISPs actually do send back your account name, I mean, something that's like a serial number, not your IP address, with the octets reversed. So because of that, I show that on ShieldsUP!. Well, this question came up because something happened to GRC's DNS server. We got a bad update, like a week ago, from the root servers, and reverse DNS failed at GRC.

Leo: Oh, that's interesting.

Steve: And so I just wanted to bring it up in case anyone else had seen this. It was a problem at our end which I tracked down and fixed quickly, which is why it was coming and going and may or may not have worked for him or seemed to change. It wasn't anything he did. It was just...

Leo: It was a coincidence that he hit you when you were...

Steve: Exactly, down and then not down, and we're no longer down. I've locked that so that it can't happen again. So it was just a - it was a one-off thing at our end. But I wanted to also...

Leo: It is, in my case, it's my IP address preceded by netblock and ended by dslextreme.com. So...

Steve: Yes.

Leo: And that's probably fairly typical.

Steve: That's more common. Although in some cases I do have people who sometimes send me what theirs is, and it's definitely, like, it's not their last name or anything, but it's something that, if they go and change their IP address, it stayed the same.

Leo: Yeah, interesting.

Steve: Which means that anybody could lock onto that as something more persistent than an IP address. You know, we're talking about tracking and identity and stuff, and this is just a sort of an obscure but still present means that in some cases some ISPs are not changing the way they should.

Leo: We should point out, and I think this is a common area of concern that doesn't need to be, we should point out that every website you go to knows your public IP address. That's just automatic.

Steve: At that moment.

Leo: Yeah, at that moment. And all websites could do what you do, which is a reverse DNS, a query saying, well, who is this? So the issue is really your Internet service provider because all sites can do what you've done.

Steve: Although actually...

Leo: And many do. Our chatroom, we do that all the time. If we want to block somebody, we can immediately right-click on somebody's name and see what their reverse DNS is.

Steve: Except if they're running through a proxy, a transparent proxy from an ISP.

Leo: Don't tell them how to do that.

Steve: Oh, no, I mean, only if you're secure, only if you're secure with an SSL connection are you sure to bypass a transparent proxy that your ISP may have. I always think of Cox for some reason in our neighborhood because when I was developing ShieldsUP!, I had my employees testing it. And it's before we were using HTTPS, in the very, I mean, the early days before this thing went public. And I realized, oops, I'm not testing them, I'm testing Cox Network's transparent proxy. So of course ever since this was released we were smart enough to get around that. But it does mean that you may be seeing a proxy's IP rather than the user's IP, unless they're establishing a secure connection.

Leo: We won't tell our trolls that.

Steve: And for what it's worth, anybody listening who wants to check their reverse IP, just go to ShieldsUP!, and the first page you get will show you a page, because I do reverse DNS on the actual...

Leo: I just showed that page for people watching on the video.

Steve: Ah, cool.

Leo: And by the way, our IRC server, we are so locked down on our IRC. We have such a great team of IRC people, including some really good programmers. And apparently, I'm being told now by our mods that our IRC server checks for proxies and does in fact block them.

Steve: Nice.

Leo: Yeah. For that reason. It's not that we - it's just that sometimes we get attacked. And so we need to make sure that we can protect ourselves. Chris B. in Northern California wonders about Aegis Padlock hardware encryption and SpinRite. Well, well, well. He says: Good afternoon, Mr. Steve Gibson. I've been a fan and devoted follower of Security Now! since the very beginning. I've used ShieldsUP! more times than I can shake a stick at. Well, I'm curious about the security of hardware-based encryption, primarily related to Apricorn, that's the Aegis Padlock software. Actually hardware. They have USB and eSATA drives.

Steve: Right.

Leo: Also being a SpinRite owner I'm curious if hardware encryption will have any impact on SpinRite's operation. A short shout-out to SpinRite's awesomeness. I've used SpinRite to fix an Archos-605, that's the little tablet PC, prior to vacation. I used it to store pics from my vacation in Central America. And I can tell you the drive was so handy and convenient, it's worked flawlessly. Oh, I guess the Archos is - maybe it's one of those photo wallet things. And the value of SpinRite has just become priceless, in my honest opinion. Thanks so much, and keep up the excellent work. So hardware-encrypted - and there's lots of different kinds of hardware encryption. In fact, even ATA drives have a built-in encryption mechanism. Does that impact SpinRite?

Steve: Well, some ATA drives have built-in encryption. And I would, I guess, maybe more recent ATA drives do. But that's - we need to make sure we separate that from just a password. So...

Leo: Right. All ATI supports passwording.

Steve: Yes. Passwords have been available on IDE/ATA drives for many years. And what that is, is a low-level lock on access to the rest of the drive, which has to be provided. That, however, can be bypassed by the manufacturer, and even by the end-user. If you forgot your drive password, and you had locked the password, or for example sometimes if you had a password-protected hard drive in a laptop and moved it to a different laptop or even to a desktop machine, that drive would still be locked, and you would be unable to unlock it. So if you format the drive and wipe out the contents, that will clear the password from one of those drives, allowing you to access it again - although, of course, you've lost access to the data that you had there before.

But manufacturers and, presumably, the three-letter agencies are able to remove a simple password protection and get at all of the data on the drive behind it. So what you really want is encryption of the drive, which is driven by a password and, you know, by a key that the drive has, which you're able to eradicate if you needed to, and that would make all of the drive's contents incomprehensible. So, I mean, that's the way to do it right is to, before you ever put any important data on the drive, you get a drive which has encryption at its interface, assign it a password, and at that point you're good to go because all the data that's written on the drive passes through this cipher on the way in. Well, this is what this Apricorn.com, this Aegis Padlock for USB and eSATA drives does. It's an external case which adds that in hardware to a drive that doesn't already have it.

Leo: Oh, I get it. I get it.

Steve: So, yeah. So you're able to take any drive, a USB or I guess a USB or eSATA interface, and I'm not sure what kind of drive it takes internally. It might be IDE or eSATA, for example, internally. And it performs hardware encryption on the fly in both directions. Apparently there's some overhead in doing so because they have a pro version which is way faster than their non-pro version. So it looks like theirs is not quite as transparent as you'd like. You'd like to have this happening on the fly, at full speed, so that you're not suffering any performance overhead in doing this. But the benefit of that is that, when you remove that drive, it never had plaintext stored on it, so you don't have to worry about all the scrubbing and recovery and emergency procedures and all that that people are worrying about more and more, about leaving unencrypted data on the drive.

Leo: Okay.

Steve: Oh, and as for SpinRite, SpinRite runs right through it.

Leo: It doesn't operate at that level.

Steve: It doesn't operate at that level. It sees the sectors. It will recover them. That's why, for example, SpinRite is usable on a TrueCrypted drive, too, one that has been encrypted. SpinRite doesn't care about the fact that it can or cannot see the data. So you could run SpinRite either on the outside of it or even on the encrypted inside, which

actually might be better because there you really do care about performance, and it'll take much longer, if there's this hardware overhead that there seems to be on this particular brand, SpinRite would run a lot slower through that drive's encryption than if you just plugged the drive temporarily onto a motherboard and let SpinRite have at it.

Leo: Right. That's important. I think people don't know sometimes the different drive recovery or data recovery levels. I mean, you operate at the sector level, at the hardware level. So encryption doesn't matter to you.

Steve: Correct.

Leo: Then you can operate at the file system level or the actual data level. Encryption would affect those, of course, because...

Steve: And that's why, for example, we're able to fix TiVos and iPods and things.

Leo: Right. You don't care.

Steve: Don't care what it is.

Leo: It could be HFS, yeah.

Steve: If it spins, we'll fix it.

Leo: If there's a sector, we can examine it. Question #3, Dick Nelson in Melbourne, Florida wonders about uncovering spoken phrases in encrypted voice-over-IP conversations.

Steve: Oh, so cool.

Leo: I haven't seen this, but he points to an article at the Association for Computing Machinery, ACM.org.

[http://portal.acm.org/citation.cfm?doid=1880022.1880029]

Steve: Okay. So...

Leo: On VoIP-encrypted calls. What is going on there?

Steve: Okay. So a number of people sent me tweets. I'm going to read the abstract of the article. This was published in the ACM, the Association for Computer...

Leo: Computing Machinery.

Steve: Machinery, that's right. Okay, their abstract says: "Although Voice over IP (VoIP) is rapidly being adopted, its security implications are not yet fully understood. Since VoIP calls may traverse untrusted networks, packets should be encrypted to ensure confidentiality." Okay, so we're talking about encrypted VoIP. No biggie so far. "However, we show that it is possible to identify the phrases spoken within encrypted VoIP calls when the audio is encoded using variable bit rate codecs."

Leo: Oh, interesting.

Steve: Think about that. That's all - when I read that, it's like oooh, yes. Because the rate, the amount of compression you get...

Leo: Varies.

Steve: ...is a function of the audio.

Leo: Right. Oooh, clever.

Steve: So, oh, my god...

Leo: So you could basically - you'll get a frequency.

Steve: Well, you'll get a - the amount of compression is a function of the audio. So that means that the density of the VoIP varies with what is spoken. So they go on to say: "To do so, we train a hidden Markov model using only knowledge of the phonetic pronunciations of words...."

Leo: So they're going to get something that maybe would sound like [garbled speech].

Steve: Well, so we...

Leo: To get a waveform; right?

Steve: "We train a hidden Markov model using only knowledge of the phonetic pronunciations of words, such as those provided by a dictionary, and search packet sequences for instances of specified phrases. Our approach does not require examples of the speaker's voice, or even example recordings of the words that make up the target phrase. We evaluate our techniques on a standard speech recognition corpus containing

over 2,000 phonetically rich phrases spoken by 630 distinct speakers from across the continental United States. Our results indicate that we can identify phrases within encrypted calls with an average accuracy of 50 percent, and with accuracy greater than 90 percent for some phrases. Clearly, such an attack calls into question the efficacy of current VoIP encryption standards. In addition, we examine the impact of various features of the underlying audio on our performance and discuss methods for mitigation."

Okay. So what this means is that, I mean, this is just a brilliant side channel attack on crypto because - so what this says is that, if you're using a variable bit rate codec, the compression ratio is a function of what you say. That would be obvious. So what they did was they were able, they took a spoken language corpus and basically trained a pattern recognizer to map from what was spoken to the equivalent compression of what was spoken. And since encryption does not compress, the fact that it was encrypted didn't change its compression. So they took the encrypted data and looked at the compression that it had experienced, and they were able to map it back to what must have been spoken if it had that much encryption. It's brilliant, and just incredibly clever.

So we know that the amount of compression you're going to get is going to change with what you say. So it's possible to build a pattern recognizer, which is what this so-called "hidden Markov model" - a Markov model is one means for doing probabilistic state analysis of something like speech, for example. It's been applied to speech recognition. So basically they're doing compression recognition. They're looking at the amount, like the way compression varies with time, and which encryption doesn't change because you compress, then you encrypt. So they're able to look at the rate at which compression occurred and develop - and their pattern recognizer is encryption blind. It doesn't care about that. It just sees how much compression you got. And so with 50 percent accuracy and up to in some cases as much as 90 percent, it is able to figure out what you're saying. It's like, it's just brilliant. It's fantastic.

Leo: Yeah. And actually, in hindsight, kind of obvious.

Steve: Exactly. Again, it's like one of those things that's like, oh, yes, that's just perfect.

Leo: Now, presumably you could have VBR encryption that would pad it or something, make it somehow not - but the key would be to turn off VBR. I guess, though, that that's not typically built into, you know, any of the control panels.

Steve: You want VBR because it's what you...

Leo: It's more effective.

Steve: Yeah, you get so much better bandwidth use. Unfortunately, that gives away what you're saying.

Leo: I presume - we're using Skype. I would bet you it's using VBR. I don't know...

Steve: Oh, it is a variable bit rate encoder, absolutely.

Leo: So there. I bet you the NSA's known about that for a while. In fact, they're probably a little peeved that this information got out.

Steve: Somebody else figured it out, yup.

Leo: Dagnab it.

Steve: And imagine, if you then had this, you'd feed encrypted VoIP into this. And even if it only got 50 percent right, you could be reading, and like most of it's wrong, but you'd get lots of snippets that would get you a lot of information. Half of the conversation contains a huge amount of data because most of what we're saying, especially on this podcast, is nonsense.

Leo: Right.

Steve: So - no, not really.

Leo: I'm sure it would sound like the teacher in Peanuts [muffled speech].

Steve: There's a huge amount of redundancy in normal, natural language.

Leo: Of course there is.

Steve: And so you could get away with missing a lot of it and still pick up the content. Wow.

Leo: Unbelievable. Just fascinating.

Steve: Very cool.

Leo: Yeah. This is, you know, understand why Steve's excited about this. It's kind of a cool insight. It's not that he thinks it's a great thing that it can happen. It's a very cool insight. And once you understand it, you go, oh, of course you could do that.

Steve: A brilliant hack.

Leo: It's a brilliant hack. Question #4 from Hendrik in Utrecht, The Netherlands. He's been playing with something called PLCs.

Steve: Our PLCs that Stuxnet programs, yeah.

Leo: Oh. Greetings from Holland, Steve and Leo. As an intern I have been doing research into security-related applications of PLCs. I can't tell you much more than that, I'm afraid. I was therefore greatly interested in your Security Now! episode on Stuxnet. As usual, I learned a lot. Steve, you're amazing. I mean, even somebody who this is their field. One thing I noticed was you mentioned that PLCs have their own network. What does PLC stand for, just to remind me?

Steve: Programmable Object Controllers.

Leo: Okay. Those are the things in the Siemens controllers, for instance.

Steve: Yes, those are the things that run all the plants everywhere.

Leo: Right.

Steve: And the nuclear plants.

Leo: Right. Because PLCs have their own network, a Windows machine is needed to infect them. In my research I've come across various PLC models, most of which supported many connection types to create a network. One of these connection types is Ethernet. In other words, a standard network cable. In my security research report I mentioned there's a reasonable risk of someone misconfiguring a network by accident, not intentionally, or accidentally plugging PLC into another network, say, one connected to the Internet? This is one of the reasons the company I was doing research for chose only to use models using different connections in Ethernet, he says, RS-485 in this case. I can imagine other companies finding the ease of Ethernet too attractive not to use. Does seem like that opens up a big hole.

Another thought was that some system administrators might find it useful to connect the entire system to the Internet anyway so they could fix things without getting out of bed. Now, I don't like being a pessimist, though it seems second nature in the security field. But I'm sure there are plenty of PLCs, SCADA systems and other such networks that are in some way connected to the public Internet. This combined with the frightening malware advances you've told us about in last week's show does not make me feel so great about the whole thing.

Anyway, just wanted to share my thoughts on the subject and thank you, Steve and Leo and all the other folks that make Security Now! happen, and there's a big bunch of people, for a great podcast. Regards, Hendrik. He is Malachy on the TWiT IRC, by the way, if you want to say hi to him. None of the PLCs I've worked with have any form of encryption while communicating over Ethernet. So usernames, passwords, et cetera are sent in the clear over that network.

Steve: And they're typically all default, too, because...

Leo: Right, because why change it?

Steve: ...the presumption is, well, no one can get to our network, so we don't want to have to bother with figuring out what our username and password is.

Leo: We're here inside the uranium enriching plant. Who could get in here?

Steve: What could go wrong?

Leo: What could possibly go wrong. Wow. Question #5, Steven Gibson, from Robert Osthelder in Fond du Lac, Wisconsin. He wonders how to switch from Windows to Mac without losing all his security tools. Oh, that's an interesting question. Never heard that one before, actually. I've been a longtime Windows user, go-to guy for IT support for my family's Windows machines. I've been considering purchasing a new laptop since mine is getting very old and clunky. Doing some shopping around online, I'm very interested in the new MacBook Air. Which I give two thumbs up for. I know you don't have...

Steve: Me, too. It's beautiful.

Leo: Oh, you have one.

Steve: I do, and it's a beautiful machine.

Leo: Elegant machine. Which runs Windows, by the way. You don't have to - you could put Windows on it. I know people have been thrilled with it. The big reasons for being so interested in the Air are the size, weight, build quality. Yeah, the build quality in the Air is pretty spectacular. Right now, though, my concern about switching to Mac is figuring out where to get started when it comes to securing and protecting a device running the Mac OS. For example, on my Windows machine I'm running Malwarebytes, Spybot, Comodo Firewall, and AVG antivirus. The problem is I don't have a clue if those types of programs exist or whether or not they're needed on a Mac or in what combination. Would you mind giving me a quick rundown of how to get started keeping a Mac OS squeaky clean? Thank you for all the time and work you and Leo do on the Security Now! podcast. I've been a regular listener for the past couple of years and a proud owner of SpinRite since shortly after I started listening, which I have used to recover several drives. Best regards, Robert. Steve?

Steve: So this is a combined answer from you and me, Leo.

Leo: Okay.

Steve: Not being a big Mac person, I don't have an answer on the details of third-party

software for the Mac. I would say, however, immediately switch to Firefox or Chrome as...

Leo: I think we know that now.

Steve: ...opposed to Safari. And that the Mac's got a nice firewall built in that prevents external stuff from getting in. So beyond that, what do you think?

Leo: Yeah, I mean, the advice for all operating systems, of course, is keep it up to date. And Apple, right under the Apple, has a software update which will check. It will do it automatically, as well, to make sure you've got all the patches. Immediately after Pwn2Own, another bunch of patches came in, obviously to patch Charlie Miller - no, it wasn't Charlie, the attack on Safari. Nevertheless, we know that there are holes in Apple's OS. I agree with you, use Firefox or Chrome. I like Chrome on the Apple. I think it does a great job.

There is, in the system preference pane, that's the Apple equivalent of the control panel, a security button which gives you some useful security things. For instance, I always make sure that I require a password after sleep or screensaver. I disable automatic login. I use secure virtual memory. A lot of people don't realize that the virtual memory on your system, the pagefiles, will contain unencrypted data. So this is built in. Apple also has built-in secure deletion in its trash can. You might want to use that, as well.

FileVault secures the entire drive. It's whole-drive encryption. You may or may not want to use that. I don't use it. You might want to prefer to use TrueCrypt or something like that. And you're right, turn the firewall on. You see it's not on here. But turn the firewall on. And when you do turn on the firewall - let me just log in. This I like, by the way. Apple, kind of like user access control on Windows, requires administrator login to do anything of importance, including - and you can set it this way, and I do - including the system preference panes, require a password to unlock each system preference pane. That keeps kids and others with access to your computer from doing stuff. But you're right, I think the firewall is quite good.

And you see immediately, by the way, as soon as I turn on the firewall, do you want the application Axia DVD to accept incoming network connections? It's immediately notified me that there is a request for network access. I do know what that is. That's our audio software, so I'm going to allow it. But you'll get those periodically. I think that's great. I always keep the firewall on. And you can even have it block all incoming connections except those required for basic Internet services - DHCP, Bonjour, and IPSec. At that point your browser works, other stuff works, but all incoming connections are blocked. That's super secure. I don't know if you need to turn that on. You see, I've allowed two connections. It will list these connections. You can add more manually, or it'll do it automatically.

This is another checkbox you may or may not want to have checked: Automatically allow signed software to receive incoming connections. Probably want to uncheck that so that you have explicit approval. And this you would like, Steve: Enable stealth mode. Which means don't respond or acknowledge attempts to access this computer, including ICMP packets, that's ping.

Steve: Yup. I'm responsible for them using that word, too.

Leo: That's right. Stealth mode is a Steve Gibson trademark. Well, I don't know about that.

Steve: I invented that for ShieldsUP!.

Leo: So I always turn that on when I'm in public. We're on a protected network in here, so I don't have it on in here. But actually I'm going to turn it on. There's no - it doesn't seem to have any performance hit.

Steve: No.

Leo: It really is a good firewall. It's based on the BSD firewall, so it's - I don't know if it's ipchains or which firewall, but it's a very strong firewall. That's probably the most important thing you can do. There is security software for the Mac. ESET makes a program called Cybersecurity for the Mac. It's an antivirus, antispyware. And there are other commercial programs like that. But there are also some free Mac antiviruses, as well, that you could take a look at. I personally don't run one. I don't feel it's needed. The Pwn2Own, I don't know what to say about that except that I use Chrome. But no guarantee that that's secure, either. Most important thing to do on any OS is just update it as often as needed.

Steve: And in this day and age the entry vector for problems is going to questionable, sketchy sites with a browser that is either not updated or has zero-day vulnerabilities that no one knows about. That's how they get you. And in every instance it involves JavaScript. So I just - if you have JavaScript disabled normally, and you enable it selectively, you're really very safe these days.

Leo: Yeah. So that's a big addition, NotScript, I guess. I'm going to have to find that for Chrome and put that on there. I hate doing that because it really slows me down in my surfing. But on the other hand...

Steve: I know.

Leo: ...it is the single most important thing you can do to protect yourself.

Steve: It really is.

Leo: Chrome extension gallery, NotScripts, that's cool. I didn't know about this. I'm so glad to have found this. That's great. And they liken it to NoScript. So that's fantastic. I'm installing it now. Thank you. Question #6 from Greg in Brisbane, Australia. He wonders about IPv6 and ShieldsUP!: I'm currently trialing IPv6 on my

home connection with my ISP in Australia, Internode. That's neat, that Internode offers that. Curiously, there appear to be no testing sites such as ShieldsUP! that support testing an IPv6 firewall. Do you plan to do that?

Steve: I do. I've got a call in to Level 3, the guys who provide bandwidth to GRC, to say, hey, guys, I'm liking all my IPv4s; I'm going to need some provisioning of IPv6. And I have not heard yet back from them. But I'm sure they must have this, I mean, they probably have to just push a button somewhere, and I get a bunch of IPv6 IPs. And when I do, I think it's definitely a priority for me to make ShieldsUP! run over IPv6.

Leo: Yay.

Steve: So no - I don't have a date yet, but it's definitely going to happen.

Leo: And you can of course go to Hurricane Electric in the U.S., and they're offering IPv6 tunneling. If you want to play with IPv6, they have free tunnels. Randal Schwartz was telling me he's got, like, five IPv6 addresses for free. Actually, no, wait a minute he has, like, a Class B block because there's so many IPv6 addresses, I think he has 65,000 of them. I can't remember. Some huge number.

Steve: Yup, that would be a B class.

Leo: Yeah. Because there's so many, you can have as many as you want.

Steve: How many do you like? How many do you want?

Leo: Take 20,000, they're free.

Steve: Yeah.

Leo: Question #7 - is it a lot of work, by the way, for you to make IPv6 compatibility in ShieldsUP!? Or is that something not too...

Steve: Oh, no, it's just sort of, like, I just have to refocus myself. It'll be fun.

Leo: Steve, you have way too many things on your punch list now.

Steve: I've got a big one that I haven't talked about yet, but maybe next...

Leo: Oh, dear. Okay, good. Look forward to it. Question #7, Anthony Woodall in Santa Rosa, California, just up the road apiece, comments about the IE6 Countdown. We talked about that web page where Microsoft's urging people to dump IE6. I just thought I'd mention that some businesses are using IE6 internally, Internet Explorer v6, and are probably not included in the IE6 Countdown website. This is true within the company that I work for. Yeah, I suppose if you have an Intranet that is written to IE6, which is not uncommon. He says: We're using a heavily customized-with-code IE6 for all of the web-style internal network resources. There you go. Also I remember you mentioned that a specific government in Europe has refused to move from IE6 because they have so much custom code.

Steve: Yeah, we did talk about that a while ago. And this is the - I guess it's a conundrum that Microsoft is in because 6 happened and was, in its day, very good and very dominant. And Firefox, or I guess back then Mozilla probably, or Netscape, they were still struggling. There really wasn't any strong competition. But Microsoft also was not following standards. They were just adamantly saying we're going to go do these things our way. I've been fighting that for the last two weeks because I'm now writing JavaScript code that needs to be platform agnostic. And half of my code is dealing with the fact that Microsoft handles events that happen on the web page completely differently from everyone else. I believe that they finally got with the plan with IE9.

But, look, here we're trying to kill off IE6, which is a decade old, not to mention 7 and 8 since then. So no code is going to be able to not take Internet Explorer into account until, not only 6, but then 7 and 8 also stop being used. And that's never going to happen. So, yeah. So it certainly is the case, I mean, Microsoft is guilty of really defying standards, even after they existed. Well, because at the time they thought maybe they would win. I mean...

Leo: Thought they'd be the standard, yeah.

Steve: Yeah. I mean, they were using Visual Basic for scripting, VBScript.

Leo: Oooh.

Steve: Yeah. You're not going to see that anymore. That one lost big-time. But it certainly is the case that people can't give up IE6 without investing a huge amount in reengineering. And the question is, why would they? Their system's working now. Of course what's going to happen is that IE6 support will disappear, and they'll end with a browser with lots of vulnerabilities.

Leo: Well, but is that a problem if it's only on the Intranet?

Steve: If they kept it, as long as they didn't use it to go outside, then you're right, that could just be a separate application. Although the problem is IE has never lived along other instances of IE very happily. Whenever you install - and that's the whole Microsoft, oh, no, it's part of the operating system nonsense from the trust, the antitrust suits, where they were saying, oh, no, you can't - notice I have no problem with Opera and

Netscape and Firefox and everything else, and Safari and Chrome, all loaded in my OS at the same time. Except, oh, no, I can't have two versions of IE. So it's like, okay, fine.

Leo: Curious. I'm thinking, if it would be possible to make network policies that said you could use IE internally only. Yeah, they could lock it down and then give you Chrome or something, or Firefox.

Steve: Yeah, or maybe...

Leo: People are going to want to use one browser, though. I know I look at my office staff, and they've got - they're all using IE. They just, well, it's the browser, it's on Windows.

Steve: The one that's there.

Leo: It's what I got.

Steve: Yeah.

Leo: So it kind of would be very difficult, very challenging for IT to say, okay, IE6 for our Intranet, but the minute you want to go outside the Intranet you've got to launch Chrome.

Steve: Ah, good point. You wouldn't switch to IE9 because it would conflict with IE. You would switch to...

Leo: Firefox or something.

Steve: Yes, exactly.

Leo: But you'd have to somehow enforce the policy and...

Steve: Yeah, you might be able to get IE to refuse to go out.

Leo: Yeah. Oh, you'd lock it down. You'd just lock it down with the security and say you could only use Intranets. That's easy. But then what happens is your user calls you and says, my browser doesn't work. I'm trying to go to Amazon. And you say, remember I told you you have to use Firefox to go to - what's Firefox? I just, I don't, what's Internet Explorer? I just, my, the Internet is broken. That's the problem. And I love users, by the way, and that's not you. I'm not talking about you. It's that other person next to you.

Steve: Any of our listeners.

Leo: Nobody who listens to this show. The Internet is broken. Help me. See, they don't want that call. Final question from Kevin York who's in our IRC. He is wickedproxy. That sounds dangerous. He's in Harrisburg, Illinois in the real world. He says malware hides in strange places. He was looking at an article on Al Jazeera with a disturbing sentence that, if true, could be a game changer in computer security. By the way, I just want to point out, Al Jazeera is a highly respected and excellent news source. Even during this earthquake they've been great. So it's not just Middle East coverage. And they are not owned or run by terrorists, as some seem to think.

Steve: Right.

Leo: They're great. And so this is an article on Al Jazeera English about - it's an opinion article about, well, it says: "Even next-generation rootkits were explored - to remain active despite the removal of a hard drive, to persist on a machine in the video card memory." It's been the case to the best of my knowledge that if you wipe or replace the hard drive and put in a fresh install of the OS, you should have a clean machine. That's the advice I always give our listeners on the radio show.

Steve: Rational.

Leo: Yeah. I mean, what are you going to do if it's sitting in the CMOS or on memory in a video card or some other firmware? He says: If things can live on your video card, what are you going to do? This is at the least troublesome and scary to think what would happen if this were to get in the wrong hands. It's in the wrong hands, I'm sure. But who is to say whose hands are the right ones, he points out.

Steve: Yeah, a number of people picked up on this and said, hey, Steve, can malware live in video cards? And the answer is, unfortunately, yes. Think about how powerful our video cards have become. I mean...

Leo: They're computers in themselves.

Steve: Yes. They are more, there is more processing power now in the video chips in the video cards than there is on the motherboard. I mean, no matter how many cores you've got on your Intel processor, notice when we were talking about Bitcoin, it's the guys who were minting the bitcoins are using the GPUs, the graphics processing units on their video cards, that are getting 140,000 hashes per second, where I'm getting 5,000 hashes per second, and I've got the state-of-the-art i7 quad core. So the video card technology has gone crazy. And they've all got Flash-updatable firmware now. Well, that's how the viruses are living. There is malware that is able to live in a video card. And that's just another area that the bad guys have explored.

Leo: Unbelievable. Wow.

Steve: So it's not good. It's a side effect of the complexity. We always get this when we get complexity.

Leo: So format your video card. You can't just unplug it; right? The video card, it's static RAM or whatever it is. It's firmware.

Steve: Yeah. So you would need to reflash the firmware BIOS, the BIOS of the video card, from the manufacturer's clean copy, in order to make sure that nothing was living in there, if you thought and were suspicious of something having crawled into your video card. Unfortunately, it's now possible.

Leo: Wow. I just - sometimes I despair.

Steve: Leo, we're getting old.

Leo: I just despair.

Steve: If we can hang in here for another couple decades, we can just say, okay, we're done with all this stuff, turn it over to the young whippersnappers.

Leo: Next week - that was our Q&A session.

Steve: Yup.

Leo: Have you decided what you're going to cover next week?

Steve: If I can, I'd like to give a thorough look at IE9, really cover it from stem to stern, what's new, what they've done, what the security is, what the implications are. And also the privacy factors, which I think are a big addition to IE9.

Leo: Can't wait. IE9, time permitting. If you have questions for our next Q&A episode, which will be a couple of episodes hence, you can go to GRC.com/feedback, leave those questions there. While you're at GRC, get SpinRite, the world's best hard drive maintenance and recovery utility. You'll find 16KB versions of these shows as well as the full audio fidelity versions. Those are for people who don't want to spend the bandwidth, or they've got bandwidth caps. And they sound pretty good. They're not, you know, they're a little crunchy, but they sound pretty good.

You can read the transcripts. That's the smallest version, thanks to Steve, who pays

Elaine to make those transcripts available. I really appreciate that. That's at GRC.com. And a lot of freebies, including ShieldsUP!. It's all there, Gibson Research Corporation. You should follow Steve on Twitter if you're not. I think we're going to see some more interesting tweets from him about this nuclear situation. SGgrc is his official Twitter handle, SGgrc. And we record this show live every Wednesday around 11:00 a.m. Pacific, 2:00 p.m. Eastern time at live.twit.tv, so do tune in for that. Steve, I thank you for a great show. Fascinating show.

Steve: Thanks, Leo. Great, as always.

Leo: See you next time on Security Now!.