Listener Feedback #72

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-208.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-208-lq.mp3

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

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

This is Security Now! with Steve Gibson, Episode 208 for August 6, 2009: Your questions, Steve's answers. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show that covers all things secure - securing your operating system, securing your 'Net connection, fighting off bad guys and spyware, protecting your privacy. And here he is, the czar of security, Mr. Steve Gibson. I think I did, in fact, in my cabinet, make you the czar of security.

Steve Gibson: I'm the security czar. Well, I'll tell you, from all of the nonsense I hear about Washington, D.C.'s attempt to find a security czar, no one is applying. They're, like, the gal that's been temporary is stepping down very politely because she wants to put pressure on the administration to find somebody to be the security czar. But the people who are good enough to do that are also smart enough not to, you know, they're smart enough to know better. Because apparently they've got no control over anything, not budget or management or staffing or anything. They're just - and they're split between two different organizations. I mean, it just sounds like a disastrous job, and probably more frustrating than anything. And, like, why would anyone want to hurt themselves and who have, like, the ability to do that?

Leo: A job with all the responsibility and none of the power.

Steve: Yes.

Leo: This doesn't sound good.

Steve: This is just a lose, lose, lose.

Leo: Yeah. It's like being governor of California, another fine job you do not want.

Steve: Although I'm sure you know, you heard, that Clinton, Bill, went over to North Korea and brought back our two prisoners.

Leo: I am so happy about that.

Steve: It was just so cool. It caught me by surprise this morning. First thing I saw is like, hey, very neat.

Leo: We talked about it last night because they worked for Current. Euna Lee was one of the reporters who worked at TechTV. And...

Steve: Oh, you knew her?

Leo: Yeah, well, I don't remember her, but I think I did know her. But I, you know, there were a lot of people at TechTV. I think she was an intern at the time. But, yeah, and she worked at Current with Sarah Lane. And Sarah was on net@night last night, and she said there's reporters on the street, but we don't want to celebrate until we see them get off the plane. Well, they got off the lane. And you know what kind of bugs...

Steve: They were flying into Burbank Airport for some reason, probably just to...

Leo: Kind of odd, yeah.

Steve: Yeah. Well, it was apparently a chartered plane. So maybe that was the right place for it to land.

Leo: Thank goodness, because these two women were convicted of spying and sentenced to hard labor.

Steve: Young women.

Leo: Yeah. Not a good outcome. And so it's a great relief that - and, you know, kudos to President Clinton. I think that's got to be a little scary to fly to North Korea. You don't know what Kim Jong-il is going to do. And so to fly into the lion's den and save those women, I think it's...

Steve: Yeah. Well, apparently he - Madeleine Albright, his Secretary of State, did visit North Korea during his presidency. So there was some sort of a sense of an olive branch. And the presumption was that Kim Jong-il wanted some attention. And so this gave him...

Leo: Exactly.

Steve: He couldn't - to have any of our current administration go over would have been too much.

Leo: Can't do that.

Steve: And so, I don't know, I think it was brilliant, in retrospect. And thank goodness that's resolved.

Leo: Whew. Relief. So today is a Q&A day. That means...

Steve: We have - yes. Because we had to change things around, two weeks ago we did the mega security update. That pushed a Q&A out. I wanted to - there was so much stuff backlogged in the GRC.com/feedback page, our mailbag, that I wanted to spend a couple of those. And this is a big episode for us. Actually this one is, and next one will be. This is 208, which is four times 52. Given that a year has 52 weeks, this is the end, this is the last episode of our fourth year.

Leo: Wow.

Steve: So, yeah.

Leo: And, you know, kudos to you because we know that because you can do the math. There's no other show I think in the world that has done four years' worth of shows, 208 episodes, without break. I mean, that's unheard of. Not one rerun.

Steve: I found one message when I was going through the mail yesterday to prepare and select questions for today. Someone asked me, I think it was a woman, said hey, you know, when Leo's on vacation, you're apparently not. Do you ever take a vacation? And first of all, when you're on vacation, I am, too, technically, because I'm not doing podcasts without you. We do extra ones ahead of time so that we have podcasts to straddle any outage. But I just - I truly love what I do so much that, if I were on

vacation, I'm just annoyed about all the work I'm not getting done. I just - I love computers and technology and, you know, life. And so I'm on vacation all the time. I'm on vacation right now, doing this with you.

Leo: You know, they say that. They say the only difference between a hobby and work is whether you like to do it. There are people, I think Malcolm Gladwell talks about this in his book "Outliers," there are people who pay money to drive trucks and trains, even though that's a job for some people.

Steve: Right.

Leo: For others, it's something they love so much that they'll pay to do it. So I'm not saying I would pay to do this. But I sure, even if I didn't have to, I think we'd be talking once a week one way or the other. Hey, well, let's - so do you have security news and updates?

Steve: We've got news, we've got a little bit of errata, and we've got our Q&A.

Leo: Steve Gibson, what is the latest security news?

Steve: Well, we have a bunch of follow-ups, interestingly enough, from last week. We know, for example, that the iPhone was patched, exactly as we predicted, the day after the formal SMS hack of v3 and prior versions was made public. So Apple finally got off the stick, I mean, I guess they were frantic for, you have to imagine, for a few weeks beforehand, since we knew about this problem a few weeks beforehand. It was patched. So if anybody has not been to iTunes recently, you definitely want to do that in order to update yourself to 3.0.1.

Leo: Yes, and I did it immediately. One point to make is, so far no reports, despite the fact that there was kind of a 24-hour, zero-day opportunity, no reports of exploits at this point. That's good news.

Steve: Yeah. Who knows whether...

Leo: It could have happened because you may not know; right?

Steve: Correct. If you didn't know, if you didn't update your phone - it seems to me that the intersection of reality needed to make this happen is relatively small. Somebody would have to know your phone number, I mean, probably targeting you specifically, who also had the skill or ability to get this thing from the 'Net and perpetrate the hack. So...

Leo: I think going forward we and Microsoft and Apple and everybody should make

the distinction between a completely theoretical attack, an attack that we know how to do but hasn't been in the wild, and then one that is actually out there in the wild. Do they make that distinction?

Steve: Oh, yeah. Normally there will be specifically, well, for example, one of the things we're going to talk about is that BIND has been fixed. We talked about the master server update problem which could crash and potentially take over BIND servers, but it was only known to cause a crash, and that a fix is available. But at the same time, that vulnerability is now being actively exploited on the 'Net to crash BIND servers. So normally there is, certainly in the Microsoft case, they will say that exploits are in the wild and that this is something you really need to patch for that reason.

Leo: Yeah. And Apple doesn't do that. In fact, Apple is very notoriously kind of tight-lipped about what their updates do. I don't think, I don't remember anyway, when the 3.0.1 alerted me, it didn't say you must get this right now, there's a big SMS hack. They just said here's an update.

Steve: Oh, by the way, yeah.

Leo: I think they might - in their tech note I think they said this patch is the SMS vulnerability. The irony is you still have to download the full firmware. It's almost 300MB, even for this one little fix, which could have been a few bytes, I mean, who knows. I wish they would reveal a little bit more about what they fixed.

Steve: Yeah. Of course then the flipside is the more they, I mean, here we are worrying about after-the-patch attacks on people who have not been patched. Even though Apple has said, hey, we fixed it, they're still not disclosing a lot. So clearly they're wanting to keep a lid on this, recognizing that there is still an attack surface among those people who do not update for whatever reason, or until they update, until they next check in with iTunes or the word gets to them somehow. So I guess I can understand that. But it's this double-edged sword we have with security and vulnerability. On one hand we want these companies to be open. But to be open means unless there's a system like Microsoft has that is pushing these patches out, and Microsoft can be, oh, you know, fairly certain that the bulk of their customers are going to be updated because lord knows they don't make it easy not to get updated any longer. it is certainly a tradeoff you have to make.

Leo: Yeah.

Steve: Firefox, my version 3 - I'm not at 3.5 yet, I'm still back at 3.0 - I was at 3.0.12. It updated to 13.

Leo: I noticed that, yeah. Or mine up- oh, I'm sorry, go ahead. Because 3.5 updated, too.

Steve: Well, 3.5 has gone to .1 a couple weeks ago.

Leo: And now it's .2.

Steve: Okay.

Leo: So you were right to hold off.

Steve: Yeah, well, there's an interesting hack which was revealed at the Black Hat conference, which is - I think it's the first question that we've got in our Q&A. So I will cover it more then. But I'm very pleased that Firefox instantly responded. IE hasn't yet and is vulnerable. But Mozilla immediately responded to that. We'll discuss what that is in our first Q&A. They also fixed a heap buffer overflow in their security certificate handling. Firefox 3 had been bringing along sort of a flexible, regular expression-parsing approach to certificates that 3.5 never had. 3.5 used a more traditional sort of standard approach to parsing certificates. It turns out there was a vulnerability in that older, longstanding, sort of inherited from the Netscape days parsing, which they've now fixed.

And there was a really interesting vulnerability that they have fixed that a security researcher, Juan Pablo Lopez Yacubian, reported, where an attacker could use, not surprisingly, JavaScript, to use the window-open JavaScript on an invalid URL, that is, a URL that you didn't mean, which looks similar to a legitimate URL. Then they were able to use the document-write JavaScript to replace the content with what they wanted it to look like, like looking like eBay, for example, appearing to have it come from a spoofed location. And then, if the spoofed document was created by a document with a valid SSL certificate, even though it was not where you thought you were going, the SSL indicators would carry over from the wrong document into the spoofed document. The bottom line of all this was it allowed a typo, a typo that would take you to a site that used JavaScript, to replace the page and spoof the SSL correctness of what you mistyped, making you look like, for example, you were at PayPal, with all the indicators that your security certificate was valid.

Leo: Ooh, ooh.

Steve: So the good news is, that's gone. That's fixed in 3.0.13. And these things were also fixed in 3.5.2 that you mentioned. So Firefox is updated. Anybody using Firefox probably already knows. I found out this morning when I fired things up and logged in and got going. It says, oh, we've got an update for you. It's funny, too, because I depend upon my Firefox session manager remembering all the tabs I have open. It just has sort of become a big database repository for me. But I had two Firefox windows open at that moment. And so I wasn't sure that it would remember them both. So I had to, like, work through the tabs on one, although I could have dragged them all over to the other because you can drag tabs across windows now.

Leo: You still use that sidebar tab extension.

Steve: I'm liking it a lot, yes. But now unfortunately my sidebar is scrolling because I've got so many tabs.

Leo: [Laughing]

Steve: It's like, okay, I'll get around to this one of these days.

Leo: You know, we had Kevin Rose on TWiT a few weeks ago. And he said, okay, quick, tell us how many tabs you've got open. And everybody on the show had, like, 20 tabs open. So this sidebar tab thing is great. But if you've got that scrolling, there's no help for you at all. That must be, like, 60 or 70 tabs open.

Steve: Like I'll get around, I'll get back to that one of these days.

Leo: The name of that, by the way, for people who want to know, is Tree Style Tab.

Steve: Yep, exactly.

Leo: Steve recommended that a few weeks ago.

Steve: So we talked about BIND, which fixes are now available. So anyone who is an admin responsible for their corporate DNS server, it's likely a master. It probably didn't need to receive update messages, but there was a problem that was found, we talked about it last week. I just wanted to let everyone know that patches are available. So you're going to want to update your BIND to the current release and solve this problem. And again, this is being actively exploited by creeps on the Internet. All it really lets them do is crash people's DNS servers. It's like, okay, well, oh, boy. It's annoying, but people are doing it all over the place.

Leo: Really.

Steve: So, yes. You want to get yourself updated to prevent that from happening. And in the Adobe Flash Player news, we talked about their problems last week, which were not fixed, but they had said they would be fixing them soon. I chuckled a little bit because I'm sure our listeners will remember me rolling my eyes, figuratively for those who don't see video, but I was rolling my eyes...

Leo: Literally.

Steve: Yes, when Adobe announced that they were going to be doing their - they were increasing their patching protocol or patching formality, going to be more responsive, and so they were going to do quarterly patches, whereas Microsoft does them monthly. And I remember at the time saying, what? I mean, that makes no sense at all. We'll see how long this lasts. Well, it didn't last even a quarter because they had some bad problems in 9.1, and they needed to update themselves immediately to 9.1.3, I think that's where they are, and v10. Anyway, I wanted to make sure people knew that Flash

Player updates for 9 and 10 are now available. So you'll want to check and make sure you get updated. And I did turn a machine on the other day that said, oh, we got an update for Flash. It's like, okay, good. It's time. And I'd noted, you know, we've been talking about Adobe, like people will probably notice, every week, which is not what you want to be talking about.

Leo: No kidding.

Steve: If you're the target of this conversation on a security podcast. There's an editor of the SANS newsletter - which is an excellent, excellent SANS security newsletter - Stephen Northcutt, who's also the president of SANS Technology Institute; and they sometimes add little - their editors' comments to the bottom of their reports or problems. And I got a kick out of his comment in this most recent newsletter this week. He said, quote, "I think organizations should avoid Adobe if possible. Adobe" - and this is not who you want to have saying this.

Leo: No, SANS is highly respected.

Steve: Yes. It says Adobe - he goes on, saying "Adobe security appears to be out of control."

Leo: Oh, dear.

Steve: "And using their products seems to put your organization at risk. Try to minimize your attack surface. Limit the use of Adobe products whenever you can." And it's like, ouch.

Leo: Wow. Wow.

Steve: Yeah, yeah. Carnegie Mellon did a study which hit the news, which basically stated that in their relatively small survey, it was only about a hundred people, but apparently 55, meaning more than half, of the people that they watched encounter expired security certificates, ignored the expiration...

Leo: I'm surprised it wasn't higher.

Steve: ...and went on anyway.

Leo: Most people would just go, I don't know what this is. Okay, I just want to surf.

Steve: That's exactly the problem is that people were confused by the notices, didn't really read them, just sort of said, uh, okay, whatever, and said what button do I push so that I can continue? And it's funny, too, because, I mean, I saw that, I witnessed it

myself firsthand. You'll remember that GRC's own security certificate expired, to my extreme embarrassment, a few months ago, and I scrambled around. I was set up at Starbucks in the morning when it came to my attention. So I zipped home and had to go through, jump through hoops to get VeriSign to issue me an update, a renewal, as quickly as I could. However, SpinRite sales continued even in the face of that security certificate being expired. Now...

Leo: Now, they're giving you credit card information, too. I mean, it's not just a visit.

Steve: Yes, exactly. It's not just go to Perfect Paper Passwords or Perfect Passwords and pick up a password. It's I want to buy SpinRite, and I'm going to put in my credit card information into this site. We might assume, however, that visitors to GRC are more sophisticated, and they were able to see, oh, look, it says here that Gibson's certificate expired yesterday, so I imagine he's scrambling around right now, as indeed I was, to get it caught up to date. But people did push past that. And there's now discussion about whether it should be possible in a browser to push past that because it's up to the browser's discretion to allow you to either disallow any SSL that has a certificate that is deemed invalid for any reason. You know, certainly mismatching domain names, you never want to get past that.

But, I mean, I've encountered other people with certificates that expired just recently, and I've forgiven them because it's like, okay, I can see how that could happen. I'm sure they're scrambling just as I was. So it was interesting, though, that more than half of people, when they see an expired cert, will say okay, fine, I still want to do what I want to do. So make an exception and move on.

Leo: Never mind, yeah.

Steve: And then my very favorite story of the week comes to us from the Black Hat and DEFCON conferences in Las Vegas.

Leo: Boy, it's been an adventure this week, hasn't it?

Steve: Oh, there was a ton of stuff.

Leo: Oh, man. Not just the iPhone thing.

Steve: What I loved was the fake ATM machine.

Leo: Yeah.

Steve: Which was found during the DEFCON conference.

Leo: Geez.

Steve: People were putting their credit cards, were like swiping their ATM card, putting in their PIN, and nothing was happening. It wasn't giving them cash. And then they thought...

Leo: That's kind of a red flag.

Steve: Exactly. And then the way it was discovered was that some, I mean, here we've got security-aware conference attendees. Someone noticed that the black hole above the screen where normally the video camera would be didn't seem to have any lens reflection coming off of it.

Leo: There's nothing in there.

Steve: So they shined a flashlight in and saw a PC sitting behind, literally sitting behind the screen, pretending to be an ATM. And that was their clue that maybe this was a bogus ATM. And the Secret Service came and took it away.

Leo: Wow. Wow.

Steve: So I got a kick out of that happening...

Leo: How long was it there before they figured it out? Do we know?

Steve: We don't know. We don't know at what point it appeared. It was placed near the security entrance - which, interestingly enough, had no security. It's an area where there was a camera blackout. For whatever reason, there weren't monitoring cameras that covered its location. So someone snuck it in, and it sort of sat there, and no one really noticed it until it began not giving people money back.

Leo: Wow.

Steve: So I have a couple little bits of errata.

Leo: Can I give you one story that just broke?

Steve: Oh, yeah, yeah.

Leo: Critical Windows 7 bug.

Steve: Oh, haven't heard of it.

Leo: It's not a security issue exactly. But it is what they call a "showstopper."

Steve: Uh-oh. Oh, and so RTM is no longer RTM?

Leo: Apparently not. This affects the RTM build, 7600.16385. Enterprise Desktop column. Randall C. Kennedy at InfoWorld says a massive memory leak involving chkdsk, when you run chkdsk against a secondary drive, not the C drive but a secondary drive, using "/r," which means read and verify, in both 32-bit and 64-bit versions of Windows 7, Blue Screen of Death, out of physical memory.

Steve: Ooh.

Leo: Damn.

Steve: Well, and you can't do a "/r" on the primary drive because it'll tell you that it's in use.

Leo: Right, right.

Steve: And it'll ask you if you want to defer the chkdsk for the next time you reboot the machine so that it's able to briefly get exclusive use of the drive before Windows starts opening files and doing everything it does.

Leo: So no idea if, you know, maybe if you do do that reboot and then do a "/r," if it does it on the main drive. But it does do it on the secondary drives.

Steve: Wow.

Leo: So I don't know what Microsoft's response is going to be. But this is - a number of people are reporting this right now.

Steve: You know, I wouldn't be surprised if 7, and I don't know this at all for a fact, you and Paul probably do know because I've - it's going to be a long time before I'm messing with Windows 7 except as a curiosity. But I noted that IE8 now, when you install it, it asks you, may I bring myself current with all security updates before we go any further? And I wouldn't be at all surprised if that's Microsoft's new policy for when you install something, before it even starts it says, okay, hold on a second, I'm going to - who

knows how long it's been since this particular code you've just used to set me up, how old that is. I'm going to go ping Microsoft and see if there's anything I need to do right now before we even start. So it could be that even though this is a problem with the RTM, that they can fix this in patch 00001 of Windows 7, and so no one will see it. It will, immediately upon installing, it'll say, wait a second, we're going to update ourselves. Oh, look, we found something. It's like, okay.

Leo: So, and by the way, I should point out that if you've got a memory leak that can cause that to happen, that often is a - isn't that often a first step in an exploit? Maybe not. It's not a good exploit.

Steve: Well, it's not even clear that that would actually - that doesn't sound to me like a memory leak. That sounds like some allocation error maybe that's been misreported, for example. If you used to try to run Windows 98 on a system with more than a gigabyte of memory - 98 was quite happy with 512MB, you'll remember. And if you actually tried to run it on a system with more memory, it would say that you didn't have enough memory. It would report "out of memory" error rather than "I don't know what to do with all this." So it could just be a fluke of whatever's gone wrong is resulting in this particular problem. It may well not be an out-of-memory error. It just might be saying that it is. So without really looking at it, it's hard to say.

Leo: And I imagine that's an easy thing to fix. I mean, it's not a kernel problem, probably. Although Microsoft's saying it might be a driver issue.

Steve: I'm sure it's easy. In fact, there was news about the - remember we talked last week about the big Microsoft glitch in the ATL, the Active Template Library, that had been part of Visual Studio for a long time, which meant that all of the ActiveX controls which were made with Visual Studio and this ATL, all had a problem. It turns out it was a single ampersand bug. There was an ampersand that was there that shouldn't have been that caused the whole problem. They called it a typo. It's like, okay, well, I guess a lot of bugs are typos. But this Blue Screen of Death from running chkdsk might be something similar. Who knows. Whatever it is, it's obviously wrong.

Leo: Yeah. If you dereference a pointer, that could be a typo, but it also could be a programming error.

Steve: Yeah, exactly. And that's what I'm thinking is going on with an ampersand. So it's like, okay, well, they didn't know what they were - someone isn't happy about the ampersand, but that doesn't mean it's a typo.

Leo: A typo, yeah. So...

Steve: Well, one of our listeners was kind enough to point me to the scifi-az website, where...

Leo: Our good friend...

Steve: ...Michael McCollum publishes his science fiction. He posted a progress report last week, Monday before last, on the status of the third and final book in the Gibraltar series. I love the series. "Gibraltar Earth" was the first one; "Gibraltar Sun" is the second one; "Gibraltar Stars" will be the third one. And he just posted an update to sort of let people know where things stand. He just finished the first draft. The book is...

Leo: See, I'm holding off. I started "Gibraltar Earth," and I thought, I'm going to wait till he finishes the trilogy.

Steve: I don't blame you. I read "Earth." Then when "Sun" came out I reread "Earth" and read "Sun." And I've offered, and he has accepted, to edit the final book for him because when I have read through them, I have found typos. And since I'm reading it, in this case, in a Palm, it's easy for me to mark the section and make a note. So I've sent him, like, little corrections for his eBooks in the past.

Leo: Can you get those on the Kindle? Weren't you trying to help him do that?

Steve: Absolutely. He's got it now in amazing variety of formats. I mean, you can get it on your back molar format.

Leo: I don't want to read it on my back molar.

Steve: Anything you've got, his stuff will read on.

Leo: Oh, good. Oh, good.

Steve: And so he's at 130,000 words. And he's going to go through it now, he's going to reread it. And what he's - the way he phrased it on his site, he said, 15 percent will be removed to, quote, "maintain dynamic tension" or, as he says, "to take out the boring parts." And so he, too, he's going to reread "Earth" and "Sun" to, like, remind himself what they were. Because this has been going on, this series straddles about 10 years. So as he puts it on his site, he wants to remove any small discrepancies that creep in over the better part of a decade of writing a series. So he's just going to make sure everything is consistent. Because of course you know us geeks, we'll read it and go, hey, wait a minute, you said that the Plurion race drank this rather than - it's like, okay, fine.

Leo: I can't imagine doing what he's doing. I mean, and keeping track of all that.

Steve: Well, they're very complex plots. I love his plots because they're - he is a nuclear engineer, literally. And his - I find his books really fun. I mean, they're not literature. They're space opera. But they're really engaging. And he has created, he has set up a

problem for the human race which I've never seen before in all the sci-fi that I've read, which is really interesting. I mentioned before that there's a race called the Broa. And they haven't stumbled on us yet, but they are a huge supremacy. They just absorb any other cultures and alien races that they encounter, getting bigger in the process. And we would immediately be enslaved if they knew about us. And so this is a problem because it's by the merest coincidence of positioning that our radio hasn't - our expanding radiosphere hasn't yet touched them. But and they've got listening posts scattered around because they're looking to acquire new species to take over. So, oh, it's just - it's a spectacular space opera.

Leo: Yeah, yeah. And, well, I will go back to it. I'm glad to know he's working on the third edition, or third volume.

Steve: Yup. I will let you know...

Leo: How do you like - have you been reading "Red Mars"? What do you think of it?

Steve: I've got them all on my Kindle. I just haven't had a chance to start. I've been massively engaged in research elsewhere, which will be the topic for next week's podcast. I also wanted to mention Sony is coming out with a pocket eBook reader at a sub-$200 price. It's got a five-inch screen. It's not very sub-$200, it's one dollar sub-200. It's $199. Supposed to be end of August. And their store is up to about 100,000 books, whereas Amazon is at 330,000 books. So Amazon still has a big lead. Of course, Sony has access to all, to a million public domain books through Google and is also an open eBook format, whereas the Kindle is closed. And finally, Apple is reportedly working on an eBook reader.

Leo: Well, it's tablet. We don't, you know, it's going to be more than an eBook reader.

Steve: Right.

Leo: It's really like a big iPhone, I guess.

Steve: Well, and wouldn't that be...

Leo: We don't know what it is.

Steve: I mean, can you imagine anything better than exactly being an iPhone, but really big format, and being a tablet running the Mac OS? It's like, ooh.

Leo: We may know soon. I mean, there's debate over when it'll be announced. But some say as soon as next month.

Steve: Oh, no kidding.

Leo: Yeah.

Steve: Oh, good good good good. Okay. And one last thing, just this is - this came out of nowhere. This was actually again from - oh, no, it was from Steve Bass. And you know Steve.

Leo: I know Steve, yeah.

Steve: Yes. He's the ex-president of PIBMUG, the Pasadena IBM PC User Group. He has a newsletter that he sends out from time to time. And he often has a section of time wasters. Well, this thing is a piece of - it runs in Flash. And do not put this URL into your browser now, Leo, or I will lose you for the rest of the podcast.

Leo: [Laughing]

Steve: It is just spectacular. It's a toy, puzzle, beautiful thing: www.playauditorium.com.

Leo: This has been around for a while, actually.

Steve: Oh, has it. I hadn't seen it before. Just, oh, just spectacular.

Leo: Yeah. I've wasted a lot of time with it.

Steve: Yeah. I will be, too, because it's exactly the kind of puzzle and toy that intrigues me because you're not in a hurry. There's no time limit. There's no clock counting down. It seemed like there's multiple way to solve these puzzles. As you stumble on and experiment with ways to solve them, you learn more about this. It's just wonderful. So I wanted to turn our listeners onto it: www.playauditorium.com.

Leo: It's kind of amazing what you can do with Flash; you know?

Steve: I'm very impressed with it.

Leo: And it makes beautiful music. I should play, well, you have to do it, you have to solve the problem before it'll make the music. But once you do, it makes great music.

Steve: Yeah.

Leo: Yeah. It's really, really neat.

Steve: And so lastly, a fun SpinRite story provided to us by Juan Guevara Torres. He says, "Hi, Steve. I'm a Mac user, so I do not own a copy of SpinRite. However, the other day I went to a computer store in Houston to get a new device for my network, following the Trust No One policy I've learned from Security Now!. A poor fellow, a PC user and his wife, visibly worried about their data, was in the tech support department. Since this person was ahead of me in line, I was able to overhear the following conversation." He calls it "'The store's pseudotechnician' says, 'I'm sorry, sir, your hard drive has been damaged. You will need to pay $299 for a technician to attempt to recover as much data as possible. This is not a guarantee, but we can try. And that does not include the new drive you will probably need, as well.'"

So the "poor fellow" is quoted as saying, "'But for that price, I can get a new drive, and what about my data? So you're saying I might not recover all of it?' The store's pseudotechnician replies, 'We will try. But once again, it's not a guarantee. Should I start filling out this work order for you?' The wife of the poor fellow says, '$299? I told you not to take your laptop on our trip. Now your pictures are lost, and we'll be out 300 bucks for nothing.' So losing data" - I guess this is now Juan editorializing. "Losing data is bad; losing data and paying $299 is very bad; but there is nothing worse than having an upset wife about losing your data and paying $299. That poor fellow was doomed to hear this story for the rest of his marriage, and maybe for life."

So now Juan says, "Listening to all the praise SpinRite users have been sharing with all of us in the podcast, I approached the couple and the technician. I asked flat out, 'I would imagine the software you use for recovering data is SpinRite; correct?' The pseudotechnician gave me a dirty look. The couple looked at me with a little bit of WTF? The technician answered, 'Yes, we use that software. You know, it's a very complex process.'"

Leo: Oh, yes.

Steve: Juan says, "'I'm sure it is,' I said. Then I turned to the couple - still with the WTF look on their face, I might add - and I said, 'I'm sorry to just cut into the conversation. However, the software the technician is talking about is available on the Internet for less than a hundred dollars. I understand it's a very easy-to-use piece of software, as well. So before paying $299, why don't you go to GRC.com and give it a try? In any case, that's what they are going to do anyway.' The poor fellow, with a slight smile on his face and a huge Texan accent, said, 'Thanks, Bud, I'll try it.'" And then Juan finishes, saying, "'Here is my email. Drop me a line and let me know how it worked,' I said. So then he says, "Yesterday I got an email from the not-so-poor fellow anymore. 'Juan, thanks, Bud. SpinRite did the trick. Those 80-something dollars I paid saved my data, and I'm telling you, man, my marriage.'"

Leo: Now, you don't guarantee that data will be recovered, we should say.

Steve: No. We do guarantee that, if you're not happy with your purchase, we'll refund your money.

Leo: Oh, I didn't know that. That's good.

Steve: Absolutely, 100 percent, satisfaction guarantee. Anybody who tries it and they're not happy, just let us know, we'll put the money back on your card.

Leo: There's all sorts of reasons why your data might be lost that SpinRite - like if you erased it - that SpinRite's not going to find it.

Steve: Well, yeah. Or if the platters have frozen, or the heads have fallen off, or it no longer spins at all. I mean, there are limits to what software can do to repair hardware. SpinRite pretty much pushes that all the way to the limit. And again, if it doesn't work, we'll give your money back.

Leo: And a large, a surprisingly large number, certainly the majority of problems can be fixed by SpinRite. That's kind of the sweet spot of where hard drives have problems.

Steve: It really does work.

Leo: Yeah. All right. We've got questions; Steve's got answers. We're going to get to those questions and answers in just a second. Steve, if you want to take a sip of water?

Steve: I'll sip my coffee.

Leo: Sip your coffee, your triple, what is it, a venti, quad venti you got today?

Steve: It's two shots of espresso in a large - in a venti container.

Leo: Oh, you're a lightweight. You're a lightweight. Alex Lindsay has got me drinking triple talls now, which is the smallest.

Steve: It's an Americano. It's not - it's just hot water.

Leo: Oh, you have an Americano, yeah. Although they say - oh, but they make it with espresso, though.

Steve: They do.

Leo: Because they say that brewed coffee, and I bet we're going to start a whole debate on that, but that brewed coffee has more caffeine...

Steve: Oh, it does. Much more caffeine...

Leo: ...than espresso.

Steve: ...than espresso. The longer you roast the beans, that roasts the caffeine out. And so even though it's a much stronger taste, it's actually less espresso. I'm sorry, less caffeine is what I mean.

Leo: Less caffeine. Not that it doesn't get you going.

Steve: I like it.

Leo: I had my triple tall today, and I'm feeling fine.

Steve: I don't need any more caffeine.

Leo: No, I don't either. Now, Mr. Steve Gibson...

Steve: Well, while you were reading that, Leo, I just bought a PDP-11.

Leo: No.

Steve: Yeah, I just won an auction on eBay.

Leo: [Laughing] I gave him a break, and what does he do? He buys an obsolete mini computer.

Steve: Beautiful, for $225.94.

Leo: Not a simulator, not a - this is the original.

Steve: It's a PDP-11, 1123, full height stand. The description says "One complete digital DEC micro PDP-1123 system. Amazingly, this unit was still being used in an office environment and was fully operational when shut down. Everything inside the case is intact and untouched. Dual front floppy drives and hard drive. Maintenance log is included. Rare find."

Leo: Aren't you amazing.

Steve: $225.94. So I scored on that one.

Leo: How many do you have now?

Steve: About 15.

Leo: What are you going to do? Are you making a cluster? What are you...

Steve: No, I'm just, you know, they might die. I might, you know, you know how many Palm Pilots I have.

Leo: Do you have them in the freezer?

Steve: Yeah.

Leo: Well, it'd be kind of cool to line them up all on the wall, you know, and you could...

Steve: Well, they're all various types, makes, and models. And someday I'm going to program them.

Leo: Great. I love it.

Steve: In the meantime, we're actually going to do a Q&A.

Leo: A Q&A, yeah, now that you've scored. Brian Mooney - Question 1, Mr. G. - in Springdale, Arkansas, brings news of a new SSL problem: Steve, It looks like they've found another method to work around SSL. And here I am saying how secure SSL is. This isn't based on the faults in the encryption, but on faults in how browsers handle null characters. And he's quoting an article in Mac World magazine from July saying the only "safe" browser is Firefox 3.5.

"Frylock" also raises the issue, are SSL certs completely broken and useless? He says: Huge fan of the show since Episode 1, ran across this on Hackaday.com. Does this not render SSL certificates useless? Please, what's the story?

Steve: Oh, this is so wonderful, Leo. This surfaced during the Black Hat conference in Las Vegas. It turns out that a null character, that is, a zero, is - to give a little bit of background about how computers process strings for our listeners, a string, like "Now is

the time for all good men to come to the aid of their country," a string in some languages, like you may remember Pascal, you had a byte for the length, it was the first character, that is, the first byte of the string was the length, and then you just had the characters that followed.

Leo: Does anybody still do it that way?

Steve: No.

Leo: They're all zero-terminated now, null-terminated.

Steve: Yes, because the problem with that was that you could not, in Pascal, the original UCSD Pascal, you could never have a string longer than 255 characters.

Leo: Oh, because you only had a byte length to represent it.

Steve: Because you had a byte. And so, you know, those designers back then said, well, that's plenty.

Leo: No one will ever need more than that.

Steve: Exactly. Now, what that allowed you to do was to have zeroes in the string because the zeroes didn't have any special meaning.

Leo: Right.

Steve: Contemporary languages, like most notably C, there are so-called null-terminated strings, meaning that it's - a string is any collection of characters going on as long as it wants to until a zero byte, a so-called null character. So strings are null-terminated, meaning that you read them until, you know, you follow the string character by character until you hit a zero, telling you, ah, I just hit the end of the string. And in fact that characteristic is indirectly responsible for many of the security vulnerabilities we have because it turns out that it's one of the ways you're able to get exploits to, for example, copy code from one place to another and do your bidding is fancy uses of this null termination. Well, it turns out that browsers, all browsers except at this point now Firefox 3 has been fixed, 3.5 was, and NSS, which is the Mozilla package that handles secure socket technology. They fixed that, too. But other browsers are stopping the parsing of the domain name in a security certificate at a null. It's not very surprising. That's sort of what you'd expect. The problem is that the security certificate issuers are not looking at nulls in the domains that you apply for. So here's the scenario. This is wonderful. You apply for a certificate for www.paypal.com[null].mymalicioussite.com. So what that looks like to your certificate authority is you're asking for a subdomain certificate of mymalicioussite.com. Much like, for example, I might - I did get, like, a certificate www.grc.com. So it's GRC.com is the root domain; www is a subdomain, as we know, of GRC.com. But in this case the subdomain is www.paypal.com[null], then

mymaliciousdomain.com. So since you control mymaliciousdomain.com, the certificate authority says, make sure that you want a certificate for this subdomain. You say, yes, I would like one very much, please. So they issue it to you. Now you have a valid certificate for this funky domain.

The problem is that browsers, not knowing any better, stop at the first null they encounter. Technically the second null in this case is the actual end of the domain name. But the browser really can't even be faulted for not knowing that. So now the one thing that you could normally not do with an SSL connection is a man-in-the-middle attack because there is no way for you, if you were able to use, for example, ARP spoofing or just splice yourself into a connection somehow, there's no way for you in the middle to pretend to have the valid certificate for PayPal.com because only PayPal has it, as long as certificate authorities do their job.

But now you can now do a man-in-the-middle attack. So if you can arrange to intercept traffic, then as soon as you see somebody attempting to go to PayPal.com, you splice into that connection, and you return your certificate with the www.paypal.com[null] subdomain. Since it was a valid certificate issued by a certificate authority, your browser checks their certificate, sees that it's valid. Now it does a comparison of the domain you entered in the URL to the name on the certificate. It stops at the first null, www.paypal.com matches, and it says yes. You are connected to PayPal.com. So it is a functioning, valid, SSL certificate-spoofing technique that is currently unpatched on any but Firefox browsers.

Leo: Wow.

Steve: Really cool. I mean, this is just a beautiful hack.

Leo: Interesting.

Steve: You know, hats off for the guys who discovered this one.

Leo: So how would you be bit? You would go - you'd have to go to a malicious site to begin with that was posing as PayPal; right?

Steve: No. This requires traffic interception.

Leo: Oh, it's a man in the middle, yes, yes, yes.

Steve: So I don't want to - now having talked about how cool this is, I want to back the terror level off from all of our listeners because this isn't going to a malicious site. This isn't - they're like, in order to do this, this is a man-in-the-middle attack. So it's only somebody who can be filtering your traffic, who can be - now, for example open WiFi. Open WiFi is prone to man in the middle because there's no encryption on your connection. So this is a perfect example of something that ARP spoofing, which for example in a hotel that uses hubs instead of routers that we've talked about years ago, or in an open WiFi situation, you can imagine a toolkit where that could be developed.

I'm sure they're in the works right now. It may well already be that Metasploit supports this because it doesn't take them long to do, to update their Metasploit framework for these kinds of things.

And this got everybody intrigued. But it means that you have to have your traffic intercepted. So absent that, there's no way that somebody could use this funky certificate. You can imagine all the certificate authorities who also know about this are going to get on the ball and be careful not to issue domain names with null characters in them, and that very quickly all the browsers will be updated in order to be smarter about this. So I think this will close fast. But it's open at the moment, except for Firefox.

Leo: And you probably don't have anything to worry about.

Steve: And you probably don't have anything to worry about. I mean, it would really require someone have access to your traffic. I would say, in the habits that most people have, nonsecured WiFi is the really - is the only obvious place where this could happen. And frankly there it's trivial.

Leo: Sparky is saying, what about a blended threat using a DNS spoof, perhaps?

Steve: That's a very good point. That's another way of somebody getting you to go to the wrong site. So if you - because normally the DNS spoof would take you to the wrong IP for what you thought you had entered. Oh, wait, no, that wouldn't work because you would - your browser would think it was going - let me think. Would that work or not? The certificate - oh, yeah, that would work, absolutely. Your browser thinks it's going to PayPal.com. It goes to the wrong IP.

Leo: But gets the certificate.

Steve: Yes. The server there returns its valid certificate that's got PayPal.com on the front and mymaliciouswebsite.com on the back, and your browser would be completely happy with it. So, yes, that's another - DNS spoofing does allow and support a man-in-the-middle attack. But again, you know, that's still less common than anybody using open WiFi. Which, I mean, I'm, in Southern California I'm surrounded by it.

Leo: Oh, everybody, yeah.

Steve: Exactly. People are annoyed that Starbucks makes you log on. Of course, once you do it's still unencrypted. So it might as well be open. So, yeah, anyway, this is just very cool. And I imagine we will see immediate updates for the SSL back-end components of all of the browsers just as quickly as they can deal with it. And of course we'll let our listeners know.

Leo: Question 2, Andrew H. in Texas says Microsoft Security Essentials not free for all: Hey guys, sorry to be the bearer of bad news. I think we said it was free.

Microsoft's Security Essentials is not free for commercial use. According to the website, it says "for your home PC," and it will not run on Windows Server. Also David Horwitz in Denver, Colorado says the same thing: I really learn and enjoy your weekly podcast, Steve. I'm using Microsoft Security Essentials beta, very happy with the usability of the product. What is your ability, I'm sorry, your opinion of the product, and when will it be available without the beta label? Thanks for all the good information. David. So, yeah. It's not for commercial use.

Steve: Essentially what happens is Microsoft has taken their high-end corporate IT Microsoft Forefront product - that's where this came from. That's Microsoft's big iron sort of formal corporate level. They've been able to test it and round it out and make it work, develop all the signatures and patterns and really nail this thing down. Then what they're doing is they're peeling off a sort of like a junior version of it, which will be available for home PC users. They're deliberately crippling that, that is, the Security Essentials, so that it senses whether it's running on a - someone's attempting to run it on a server platform. And it will not run on their Server versions of Windows. Which Microsoft has done similar things like this before.

So I remain bullish on Security Essentials, to answer also David's question. I am so excited that Microsoft is going to get into this. The people, security researchers who have been looking at it, are very impressed...

Leo: Good.

Steve: ...with its zero false-positive track record so far.

Leo: Okay. That's good. But does it also - how accurate is it in finding viruses?

Steve: It's deadly accurate.

Leo: Oh, that's excellent.

Steve: I mean, I think this puts everybody else in real trouble. So, I mean, I'm not shedding a tear because I know, you know, I've got so many people who are just not that computer savvy. And they'll be much happier, I mean, these are the people I can't drag away kicking and screaming from IE. So it's like, okay, fine, stay there. But just tell Microsoft you want Security Essentials. And as far as I know it's going to be later this year. So later in '09 it's supposed to be happening, out of beta.

Leo: We've been talking about it on Windows Weekly. And I just don't remember off the top of my head what the official date is. But anyway, yeah, soon.

Steve: Good news, and we'll certainly let everyone know. And it's the first AV I will use. I just, you know, I've gotten along without one being careful. But I'd like the idea of it being - the problem is, so many of these are just glommed onto Windows and cause

more trouble than the virus, especially if you never get any.

Leo: Right. And, you know, I'm just saying - beta tests started June 23rd...

Steve: And immediately shut down because they offered 75,000, and it just sold out in less than a day.

Leo: And all they say is by the end of calendar 2009, as you said.

Steve: Right.

Leo: Question 3, Phil in Los Angeles wonders about cellular broadband security. This is a good question: Steve, I've recently started tethering my G1 phone to my laptop to get Internet when I'm not near a wireless connection. I was wondering what are the security implications for doing this? By tethering, or using something like the MiFi, which is the $60 a month EVDO solution...

Steve: I'll have one by the end of the day, Leo.

Leo: I love it. I love it. Is the connection as unsafe as hardwiring my laptop to the Internet without a router? If so, what should I be doing to keep my computer as safe as possible while tethering? In the event you answer this question, please keep the response as simple and pedestrian as possible. I'd like to understand the answer. Me, too, Phil.

Steve: Okay, Phil. There's many different areas of broadband security. One is the idea of cracking the relatively - even more than relatively - the very weak encryption of the connection. There are cracking devices around. They're not common. They're expensive. But they exist, meaning that the "encryption," unquote, that is being used for our digital cellular connections today is not near the grade of encryption that is available everywhere.

Leo: Really. Oh, I didn't know that.

Steve: Yeah, they used - remember the problem is that these standards were put in place when phones had calculator watch chips in them, you know, really low power technology is when these standards were put in place. So now we're all carrying computers around in our pocket that decompress highly compressed MPEG-4 video at 30 frames per second. I mean, these things have computing power just falling out of themselves. But that wasn't the case back when these standards were built.

So, for example, there are multiple shift registers with prime numbers of bits which rotate in a circle, and the outputs are XORed in order to create a pseudorandom bit stream which is XORed with the digital data. We know that if that pseudorandom bit stream was really high quality, really random, and could not be guessed, that XORing

your digital data with that makes virtually uncrackable encryption. I mean, it's very good encryption. The problem is, if you just use some shift registers that everyone knows about - I mean, this is in the spec, it's in the standard. They tried to keep it secret, which of course is the first bad sign. They didn't want anyone to know. But inevitably this information got loose.

And so they also used frequency hopping so that it's not - you don't just put up an antenna and suck this stuff in. You need to be clever about tracking the frequency jumps that the digital signals make. But that's all been done, too. So there's that aspect of it. But when he specifically asks relative to hardwiring an external router on his computer, that makes me think that he's talking in terms of, like, the attack, external attacks within the channel, which is itself not as secure as we would like, as I was just saying. And I just realized I completely blew him out of the water because he wanted a simple and pedestrian answer, and I don't...

Leo: I wasn't going to - I was going to let you finish, and then I was going to say, okay, now tell me the answer [laughter].

Steve: Okay.

Leo: No, keep going with the technical one. I think that that's important.

Steve: Okay, so...

Leo: But then we'll get the bottom line after that.

Steve: So there's the one problem of someone actually cracking the wirelessness of your connection. And that exists, but it's very, very slim. Then there's the problem of you being on the Internet. And so in that sense it doesn't matter how you're on the Internet. In this case he's on the Internet using broadband cellular.

Now, there's two possibilities. And we actually discussed these a little bit last week. Remember there was a - someone wrote in and asked why do I sometimes have this IP, and it was like 142.something or other, meaning a public IP, and why do I sometimes have 10.something, which is a private IP? So if you had a public IP, then it's very likely that any traffic out on the Internet can come to you.

If you are behind - if you have a private IP, like 10.something, then that means that someone somewhere, no doubt your ISP, your cellular broadband provider, has a NAT router, which is a NAT just like you might have. It's not quite the same as yours because it's possible that other people on the cellular network could have access to you. They also have a 10-dot IP. So do you. So there might be some visibility from one phone connection to the next, so it's not as private. But at least you're protected from the public Internet behind a NAT router that doesn't know how to send traffic to you unless you've got a connection established to that external location.

So again, the problem is this isn't a simple, easy answer to - or easy question to answer, if you're going to broadly look at the implications of cellular broadband security.

Leo: I guess the question is should I - are there any precautions I should take? Should I stay away from banking? What should I not do?

Steve: Okay. If he talks about as unsafe as hardwiring his laptop to the Internet without a router...

Leo: It's not that unsafe.

Steve: Then really the only thing a router is providing you is essentially a hardware firewall. So you've got a software firewall in any computer you're now using. The Macs have them, Windows has them, Linux machines have them. So if you're behind your software firewall, since you're not concerned about malware in your machine messing with it, you're concerned about external threats getting in, you're safe.

Leo: Okay. But don't assume that every transaction is encrypted. Or safely encrypted.

Steve: That's very much the case. Well, you've got encryption on your broadband.

Leo: Just weak encryption.

Steve: It's not state-of-the-art powerful. It's not AES, SSL-style, or triple DES even. I mean, it's weak encryption. But it's way good enough so that it's very unlikely that anyone is going to be able to hack in and track your spectrum frequency jumping cellular phone all around.

Leo: And they'd have to be going after you particularly?

Steve: There's now equipment which is very good about cracking this kind of stuff. But it's very expensive. It's not stuff that hobbyists have.

Leo: Okay. So I guess the pedestrian answer is you probably don't need to worry about it. Theoretically it's a possibility. But it would have to - it's a pretty high-end thing to do.

Steve: And wherever possible use SSL. If you've got an SSL connection, then irrespective of everything else, even if they could hack into your frequency spectrum-hopping, pseudorandom stream-encrypted connection, then they hit real industry-strength encryption, and they don't go any further.

Leo: I always, you know, of course your banking and all your purchases are

probably SSL anyway. But I try to - the one thing that really is a vulnerability it seems to me is your email. If you're not sending that password encrypted, if you're not reading the email encrypted, you should. And most email providers will let you do that.

Steve: Yup.

Leo: John Jones in Wirral, U.K. is seeing red in Firefox: Hi, Steve. After having problems with some sites that I need to visit responding very sluggishly, I finally complained to the admin of one of those sites. He said, "Well, you're using IE7. That could be the problem." He says his site was not meant to be used by such an old browser. It's not that old.

Steve: No.

Leo: Whilst I balked at the thought of IE7 being old, I thought, oh, well, what the heck. I got the latest version of Firefox and have been forcing myself to use it after hearing that you are now exclusively, except for updates, doing the same.

Steve: Yup.

Leo: The good news is all my sites are indeed much snappier now. However, I have noticed something in Gmail that is bugging me. I have my account settings to always use HTTPS. This is exactly what we were just saying, which is he's using SSL when he logs in and reads his email in Gmail. And when I initially log into my account, it shows HTTPS and the rest of the URL in green text as one would expect. I'm safe. But after a few minutes of maintaining my emails, I've noticed the text in the URL has gone to red. It still says HTTPS, but now it's red. If I right-click and view the page info it says, "Connection Partially Encrypted." This is - I get this message a lot from IE, as well. Well, this page is only partially encrypted. You want to continue? Doesn't tell you what part.

If I further click on Details it says, "Parts of the page you are viewing were not encrypted before being transmitted over the Internet. Information sent over the Internet without encryption can be seen by other people while it's in transit. The URL text never goes back to green until the next time I log in, but never stays green. What's going on? Are my transmissions encrypted or not?

Steve: Well, people who used to use IE may be familiar with the little popup that IE generates. It says, "This page contains mixed content."

Leo: Mixed content, yeah.

Steve: That's what they used to say. And I can't diagnose what's going on with Gmail, but I can explain what this means. It's probably not something to concern yourself with.

But my guess is there's a little glitch in Gmail somewhere.

Leo: Well, I think I can answer. I mean, I think some of the text that's sent by Gmail, perhaps the Google ads, they're not encrypting. But I'm pretty certain your email is encrypted.

Steve: And that's why I'm suggesting that it's really not something to worry about. Now, remember that the way a web page is built is that there's the main body of the page, which is the text typically that you get from the URL. It says HTTPS, which is your assurance that that portion that is the original sort of text content is encrypted. The problem is that when the browser receives that, it contains requests, other URLs to other stuff, for example, images and other components of the page. They all, if they don't specify any HTTP://, that is, if it's a so-called relative URL, where for example it'll just say the URL is /images.google.com and then the name of the image, what the browser does is, it just says, oh, this is relative to the current page, meaning that whatever encryption the current page is using, that fetch for that asset, that image will also use. So there you sort of automatically get all of the assets of the page fetched over the same encryption or not as the main page.

But if, as Leo suggests, for example, ads may be explicitly saying http:// and then the rest of the URL, that's telling the browser explicitly use nonsecured fetch for this particular asset, that is, it overrides the default for the page which is established by the URL of the page. And that's where the red comes from in the page.

Now, the reason I'm hesitant to draw any really firm conclusions is that there's probably nowhere on Earth you find JavaScript so heavily used as at Google. And lord only knows what, I mean, basically you're downloading a program when you are using Gmail which is getting more sophisticated by the month. So, again, it's just impossible to know what this JavaScript is doing as you click around among pages and things. It feels to me like it loses synchronization or something gets lost where it was trying to hold onto initially, at least from John's explanation. He says, after a while of maintaining my mail something goes red.

Leo: I think UrbanWarsNet in our chatroom has actually hit the answer. Some of the email you're getting probably is HTML and has relative links within it to unencrypted content.

Steve: Ah, that's exact- that would perfectly do it.

Leo: Yeah. Because if it were the Google ads, well, it would immediately go red.

Steve: Precisely.

Leo: But if it's tied to various mail you're looking at, it might not go red until that kind of - you view that kind of mail. And then all of a sudden, oh, yeah, well, part of this page is unencrypted.

Steve: Now, John, who asked the question, does say that once this happens, it never stops happening until he logs out. So again, I think the idea from the guy in the chatroom, I mean, that makes sense.

Leo: That makes sense, yeah.

Steve: But again, so much is going on with something like Gmail, which is just script land, that it's difficult. My original explanation here sort of applies mostly to a generic typical web page. These things are so automated now, it's difficult to know. My guess is it's a bug. That is, if you log out, and you log back in, and you're green again for a while, then something times out or something fetches something or refreshes or who knows what's going on. But that's at least what the red means.

And again, I couldn't definitively say whether the textual content is safe or not. One thing you could do if you were really curious and had the ability would be to monitor your packets. I mean, put a packet monitor on and see what content it is as you move around from one mail to the next which is going over the wire in the clear.

Leo: Yeah. That's the problem is they don't tell - they browser doesn't - it says some of this is unencrypted. They don't say which. They don't say what.

Steve: I mean, with Gmail or anything on Google it's become a program. I mean, it's a client-side program you're running. It's not just a browser anymore.

Leo: And UrbanWars said it would make sense that if it was the message it would stay red because now that that session has been - some of it's unencrypted, it's not going to go green again.

Steve: Well, but if you went to a different - if you went, like, back to where you were before and looked at...

Leo: The whole page is SSL.

Steve: Yeah, if you went to mail that didn't have any of those problems, you'd expect it to say, oh, look, now it's all encrypted again. We just don't know.

Leo: I don't think it's that smart.

Steve: But that's what it means. It's not really - we don't know that it's really bad. I think it's just a bug.

Leo: Ryan in New York, two questions and a comment. He says: Hi, Steve. I have two questions for you. You've talked a lot about wireless encryption on your show.

Because of it I've always stayed on top of the latest wireless security measures for my home router. Recently I bought a new router to upgrade to Wireless 802.11n. After hooking up the router and making sure I can get online, the next thing I did was go to the wireless settings page, turning on WPA2 encryption. That's when I noticed something I'd never seen or heard about before: WPA-PSK [TKIP] + WPA2-PSK [AES]. I am not sure exactly what that means. Does it use both forms of WPA to encrypt the signal? It's got a plus. And if so, how does that work, and why would I want to or not want to do that?

Second question, a quickie. My parents are fairly well-connected. My mom just recently bought a laptop. I've noticed that their passwords for email and other sites just make me cringe. I have tried to explain to them why they should use better passwords, but they seem to either not care or don't want to bother with the hassle of - and I bet you this is it - remembering more complex passwords. I'm not sure what to do. I'm afraid that they use similar

passwords on their bank accounts. Is there any easy way to get them using passwords at least better than things like "qwerty" - I see a lot of people use passwords "asdf," which is the first four letters on the second row, I mean, it's like, come on - short of me writing a program that can manage their passwords for them?

Thanks so much for the show, you have no idea how much help you have been for me in understanding computer science concepts before I actually learn them in class. Many times you go more in depth and explain things much more clearly than some of my computer science teachers. Please keep

up the good work. This show is more of a never-ending computer science and crypto course for me than a podcast. You really should write a textbook or ten. Signed Ryan in New York.

Steve: So, okay. There are some routers which are offering sort of an either one of the above encryption. So you could choose WPA-PSK using TKIP, or you can choose WPA2-PSK using AES, or you can choose both. And the idea is that it would allow you, it would allow the router to accept connections from clients using either. Now, if PSK, if the TKIP encryption were a lot weaker than AES, I would say you definitely don't want to choose that. You would want to just use WPA2-PSK with AES. But there's really nothing wrong with WPA-PSK with TKIP encryption. It's lighter weight, requires less processing. So it's really not a bad thing.

On the other hand, if you know that your devices you're going to want to use all support the latest generation, the so-called WPA2-PSK using AES encryption, then it's a tiny bit more secure to tell your router only allow connections with the best possible encryption. I mean, in general security best practices that's certainly the case. You only want to allow the most secure things. You don't want to allow less secure fall backs. Although in this case TKIP is fine as long as it's WPA and not WEP, which was the bad stuff. So that's what that option is. It lets the router accept connections using either of the encryptions, not forcing it to choose one or the other. It lets the connecting device specify which it wants to use. And again, if you know that the things you're connecting support AES encryption, I would choose it on the router, too. It just makes more sense. As for your folks, I don't know what to tell them.

Leo: Make them listen to this show over and over and over.

Steve: Yeah, I just, you know, I can - this is the problem, is they could very well go about their whole lives using bad passwords and never have a problem. We know that many people using bad passwords get hacked. As a percentage, I don't know what percentage of people get hacked having bad passwords. But for those of us who follow security and care about security and recognize that bad things really do happen to good people, using complex passwords makes us feel better and makes us more secure. There's no doubt about it. Whether your parents have enough security, it's just impossible for me to judge. And I don't know, I mean, I don't have any magic elixir for suddenly getting them to care more.

Leo: It really is the issue of making it easier to remember. And that's why people use bad passwords because they can remember them. And it's certainly no better to put post-it notes down the side of your screen with those hard-to-remember passwords.

Steve: You know what I would get? I guess what I would suggest is, those of us who are really security conscious are good about not reusing the same password. What I would - a compromise would be to come up with one really good password, that is, upper/lowercase, a few special symbols, maybe tie it into something in their lives like mix their date of births in with the alternating letters of their dog or something, something where you could say here's how I came up with this. Just if you guys can memorize this, change everything that's qwerty right now over to this. So maybe...

Leo: Better than nothing.

Steve: Exactly. So it's a compromise. You tell them, just one unbreakable password. You really ought to have different unbreakable passwords. But that's - I really understand that's going too far. So a good compromise is just one really good password that they would just memorize once. You could quiz them over dinner. Say okay, Mom, what is it? And get them to switch over to it. I think that's probably the best you can do. And frankly, that's pretty good.

Leo: You know what I use, and this might be simple enough for Mom and Dad to get using with it, I have a master password which, as you described, is that one password that's not a dictionary password. It's easy to remember for me because it's an acronym for a long sentence. And then I mix cases, and I put punctuation and stuff like that. And then I use that master password with a website called SuperGenPass. Have you ever seen this? It does a hash between the master password and the top-level domain.

Steve: Right.

Leo: So when I go to PayPal.com, I press - I have a bookmark on the top of my

page that generates this password. It'll ask me for the master password and then hash the master password, which is always the same...

Steve: And give you some gobbledygook.

Leo: And it gives me really, really gobbledygook. And that gobbledygook is the unique password for that page. It's only used on that page.

Steve: Or for that domain.

Leo: I'm sorry, that domain.

Steve: Right.

Leo: But I can always regenerate it as long as I remember my master password. And the bookmark does it for you automatically. Then that way, when they go to a page, they press the button, it fills in the password for them. You can even have it remember the password, which is probably not the most secure thing to do. But so you always have unique passwords that are really good, strong passwords. And all you have to remember is one password. This is how I do it. I mean, it's worked for me. Doesn't work everywhere because some - and it has your favorite thing, JavaScript, running in the background.

Steve: It really - that ought to be just an add-on. I mean, it's a perfect little thing.

Leo: I think so, yeah.

Steve: Instead of having to go to - I don't like the idea of going to a third-party site and having them do that for me.

Leo: Well, you don't. You can download the JavaScript.

Steve: Oh, okay.

Leo: Actually the JavaScript in my case - it depends on your browser. IE won't do this, but Firefox will put the JavaScript in the bookmark. So the JavaScript's running from the bookmark.

Steve: Okay.

Leo: It's not a very complicated, I mean, you can look at the code. And it can embed it in the bookmark. So the bookmark just says what's the TLD, hash it with the master password, what's the master password, hash it, spit it out, and it actually fills in the password field automatically. That's SuperGenPass.com. And I think it's a good way to go; you know? Anyway, that's my suggestion. That's kind of in between what you were suggesting and true security, which would be using a 64-byte Perfect Password every time.

Steve: A nightmare.

Leo: A different one every time.

Steve: And then a database to keep track of all that.

Leo: Yeah. Somebody's correcting me, yes, it's a "bookmarklet," not a bookmark.

Steve: Bookmarklet.

Leo: Bookmarklet. And it uses JavaScript. Let's see here. David Johnston in Sydney, Australia says thank you for talking about W3C validators. He says thanks for bringing up - wait a minute, no no no, let's go back a little bit actually, speaking of W3C. Kevin Ghadyani in Overland Park, Kansas was the guy who sent us in the message about the errors.

Steve: Exactly.

Leo: He says: Thanks so much for reading my question. I've been listening since 2005 - which is I think when we started.

Steve: I think so.

Leo: ...back when I was in college, and was extremely surprised to hear my question read on the air. Thanks for discussing it. I will cover GRC on BadMarkup.com. Oh, it's his site.

Steve: Yup.

Leo: But also explain your reasoning. Fortunately for me, you have well-written show notes for referencing purposes. Yes. That's one thing Steve does really well. Here's some personal bits. While I'm not adept enough to program an entire blogging system myself just yet - as you have, Steve - my business's website and

any future one I've been programming using PHP and Notepad++. Had I not used PHP, I could understand how difficult making a site like GRC is. I actually use PHP to change the CSS files I send to browsers, even changing the DOCTYPE and meta tags for older browsers

like IE, which is why my site is even IE4 compliant, haha. Other than Google Analytics, I run no JavaScript on my site and have a good policy to make it work on all browsers including mobile and Pocket PC devices.

I love what you've done with GRC. Because of that, you're the main person I think of when I do web design. I always tell people, "If Steve can do it without JavaScript, so can I." Much with the way you program in Assembler, I try as hard as possible to use the most efficient methods in any sort of design I do because I know there's someone else out there who does them, too. Thank you for such a great show.

Steve: Well, I liked that as a lead-in to - and remember, this guy was critical of the 13,000-some-odd errors on the Security Now! page. And I said, yeah, okay, that's true. I don't care.

Leo: Because it's hand coded, baby.

Steve: Well, and, yes, and I'm not doing per-browser customization. That's just not the approach I took. I certainly could have used the User-Agent header in the request to determine what browser was pulling the page and then customized the page per browser. But for me the pages are there, they do their job, and I'm fine with it.

Leo: Yeah. And that really is only practical, I think, if you're using JavaScript because you have to do if-thens and stuff like that. It's hard to do in plain HTML. So that segues to David's question...

Steve: Exactly.

Leo: ...from Sydney, Australia, "Thanks for talking about W3C validators!" Dear Steve, thank you for bringing up the topic of W3C. W3C is the World Wide Web Consortium, by the way. They're the ones who make the HTML standard. It's run by Tim Berners-Lee, the guy who invented HTML. Although I am an idealist and wish that every browser and site used compliant code, this just isn't the world we live in. I, too, have been hand-coding sites for many years, pride myself on having sites that work on a very large range of browsers. I'm so tired of having to defend my work in the face of W3C validators and those with just enough knowledge to run them. So thank you for making me feel a little bit better. That's nice.

Steve: And I thank David for making me feel a little bit better. All of those of us who are out on the edge saying, eh, I don't validate, well, we're all together.

Leo: You know, most sites don't validate. Most don't have 13,000 errors, but most sites do not validate.

Steve: Per page.

Leo: Per page. That's quite a lot. But most sites. And very few sites will validate fully.

Kendall Bailey in Des Moines, Iowa uses Buy.com - we were talking about that. In fact, I'm so glad, I wanted to thank you again for coming on the radio show this weekend.

Steve: Oh, yeah, it was perfect. And you were right that it's a big issue. We had - we got a bunch of email from people sharing their stories.

Leo: This is that issue with some etailers like Buy, Orbitz, Flowers.com...

Steve: Fandango...

Leo: Fandango, kind of colluding with these web - they call them web loyalty programs, but really it has nothing to do with loyalty, it has to do with money extraction, giving them your credit card and letting them very easily charge you without...

Steve: Well, selling them your credit card.

Leo: Oh, yes. They don't give it away for free. Selling them your credit card because they say, well, you agreed to do it. That's personal information.

Steve: It's in our fine print. Don't you read the fine print?

Leo: And these companies really kind of racking up charges without your knowledge because the fine print allowed them to just say, well, just give us an email address, and we'll charge you. So I've been - I've used Buy.com exclusively with Google Checkout, says Kendall. See, that's the solution because they don't have your credit card; right?

Steve: Mm-hmm.

Leo: Never had any problem or coupon offers. Thanks for mentioning the issue. I'll be sure to watch out. I use a Discover card secure online account number with

Google Checkout. Basically it's a single-vendor account number as opposed to a single-use number. Now, we've talked about that. PayPal offers that, as well. Since all charges go through Google, it works for multiple Google Checkout sites. So this is clever. He's using one credit card. That goes to Google. Google then does the transaction with these other sites without giving up even that credit card. and these other sites couldn't use the credit card.

Steve: They have nothing to sell.

Leo: They've got nothing. Since all charges go through Google, it works for multiple Google Checkout accounts. Buy.com is by far my most used etailer, but they don't have my email address or credit card, only my Google Checkout data. And Google doesn't even have my full Discover account number. So I hope I've covered myself as much as reasonable. Have I?

Steve: Yeah, I think he has. And the reason I wanted to bring this up was that you and I on the radio show after the podcast talked about this notion of using PayPal or Google Checkout. I don't know if there's - are there any other third-party suppliers...

Leo: There are a lot of them. But those are the big two.

Steve: Yeah. And I don't encounter others very often. I'm happy to see more and more Google Checkout. I like Google.

Leo: I'd like to use Google. I would. I'd love to use Google all the time.

Steve: Yes. And so I just wanted...

Leo: Amazon is the third one. It's very common.

Steve: Amazon as a - no kidding.

Leo: Yeah.

Steve: So you go to a site that's not selling books or anything, and you can use Amazon in order to...

Leo: I think so, yeah.

Steve: ...pursue your transaction. Okay, I hadn't seen that. But anyway, the idea being that the beauty of that is you're keeping your credit card information confidential from

the site from which you're buying. They've got a relationship with PayPal and Google Checkout, maybe with Amazon or whatever third party you're using to provide the assurance of payment. And there's nothing for them to sell. So they can be as loyal to the web as they want to be, and unfortunately get nothing but the purchase price, no money for selling your credit information to some third party.

Leo: Matt Ridley in Appleton, Wisconsin wants to scold us. He says: Love the podcasts since I found them around Episode 150 or so. Oh, you've got a lot to listen to, Matt. In fact, I have to say that while we do cover topical stuff at the beginning of every show, most of what's in these shows is timeless.

Steve: Yes.

Leo: If we're not talking about specific security flaws, a lot of what we're talking about is fundamentals that, you know, you can listen to Episode 1 and learn something that's useful today, even though it was four years ago. However, I think I'm missing something. After listening to the massive security update - that was 206, couple of episodes back - you and Leo commented at the end of the show you don't understand why we can't be proactive and take these bad computer clusters down. We were talking about botnets, I guess. You didn't reprimand the BBC - or didn't you reprimand the BBC just a month or two earlier for buying a botnet and, after researching it, notifying the users that they were part of a botnet, as being a violation of privacy? What's the difference? I completely agree we need to have something that can scout and clean these botnets - although the term "Skynet" seems to come to mind - but I fear the same privacy rage as being a result. Or am I missing what was being said about the proposed solution in the original story? Yeah, I think he misunderstood us.

Steve: Yeah, he did. We were not saying that we wish that it was...

Leo: We didn't advocate taking these botnets down.

Steve: Exactly. What we were saying was, we were talking about, in the future, we imagine that the laws will change. There's pressure to get the laws to change because the bad guys have such an advantage over the white hats because the white hats, who know how to counterattack, how to disinfect, how to commandeer a botnet and shut it down, are unable to do so because even in the best interests of the Internet, the world, the people whose computers have been hacked, even though we're trying to help people, it's against the law. We can't break the law. The bad guys already are breaking the law.

So the problem is we need the law to change. So our reprimanding the BBC for doing what they did was that they presented a notice on people's computers telling them that their machine was infected, and here's where you need to go in order to fix it. While that was in the best interests of everyone, and I don't disagree with that at all, it was not legal. And they got not just us, but many people were upset that that's what the BBC - and actually they did it through an affiliate security company and so brought some good, needed attention to this, but technically broke the law, at least what is U.S. law, in the process.

So what I'm bemoaning is that there's no level playing field at the moment between the bad guys and the good guys. I mean, there almost never is. But from a technology standpoint our hands are tied at the moment, the good guys' hands are tied, while the bad guys run around in circles and do whatever they want to.

Leo: Well, and maybe appropriately tied. I don't really think it's a great idea - that's vigilante justice, and I think it's probably not the ideal way to solve this problem.

Steve: Yes.

Leo: I wanted to mention, and we forgot to mention this in the news update, and maybe next week we can talk about it. One of the things demonstrated at Black Hat was something called a bootkit, which is a combination of a rootkit and a modification of the master boot record that allowed you to bypass TrueCrypt's full disk encryption.

Steve: Yup. I know about it. I looked at it, and it actually doesn't do that.

Leo: Oh, good, okay.

Steve: Yes. What it does is it installs some hooks into the system such that if you're using whole disk encryption, it's able to be a trojan even though you've got whole disk encryption.

Leo: Oh, okay. It doesn't unencrypt.

Steve: No.

Leo: It launches itself before the encryption takes place.

Steve: Precisely. It's able to hook - it only runs on BIOS, not EFI BIOSes, traditional BIOSes. It hooks Interrupt 13, which is the disk BIOS interrupt. And so the idea is it's malware you can get on your machine which gets on even though you're using TrueCrypt to protect your drive. So but it's not bypassing TrueCrypt encryption at all. It's just riding along and sneaking in and then staying alive after you've provided your password and decrypted your drive.

Leo: Well, thank you for that update. I'm glad I asked. Question 10, we're going to talk about Fandango. Justin Lowmaster in Oregon says: I ordered some Fandango tickets before - Fandango lets you buy movie tickets - and likely never again now. And yes, I had one of those coupon offers, the loyalty system, pop up. I think there was an incentive, a "free" - huge quotation marks - movie ticket. Oh, dear. That's a lousy incentive. Nine bucks, thank you. I looked all over the page, found nothing

mentioning a charge or a fee. I signed up and, yes, I got a free ticket code, intending to cancel the service if I didn't want it. Some time later I found an odd charge on my account.

Steve: Whoops.

Leo: I looked up the company and found a number and called them. I got the service canceled. I got the money refunded. There was no hassle. They know. And nobody ever does this, so they can afford to be generous.

Steve: Exactly.

Leo: It was indeed the offer I had signed up for at Fandango. I had assumed I just missed the fact that I would be charged until I heard your Episode 207. Thanks for letting me know I didn't miss a notice, it wasn't there. While Fandango is a useful service, I think I'll take my chances at the box office instead of buying tickets online. P.S.: I just got SpinRite. No miracle stories yet, but maybe someday. No, maybe not. Maybe you won't. Maybe you don't need a miracle. I'm just glad to have it at hand.

Steve: Well, if you run it from time to time, you won't need a miracle, exactly.

Leo: It's a miracle avoidance system. Think of it that way. How do you like that? By the way, another intermezzo, Apple has just released an update for Leopard, 10.5.8. They don't mention any security fixes, but I am sure they're in there. They do say it enhances stability, compatibility, and security of your Mac, so...

Steve: And that's always good.

Leo: We don't know what, we don't know what...

Steve: But it does something. So I just wanted to toss in Justin's comment. Here was a listener who actually fell into the net of the web loyalty, had an authorized charge occurring on his card. He didn't know it, but it apparently would have been periodic, that is, he subscribed to something. So it may not have been a one-time charge. But he jumped on it and got it reversed. And as you said, Leo, they'll certainly not fight you on that.

Leo: Would hope not. I mean, geez.

Steve: Yeah. And so this stuff really did - it does happen, and it did happen to a listener.

Leo: Do you review your credit card statements every month carefully with a fine-tooth comb?

Steve: Sue actually does. My bookkeeper does. And so, and she asks me, she says, Steve, I need your receipts, because I pile them up in my wallet as I'm doing things, and also I'm printing them out when I buy things on the web. And she matches up everything. And there have been times when she's said, okay, I didn't get a receipt for this, and what's this charge, do you recognize this? I go, oh, yeah, I know what that is. So, yeah, I've got her watching. And it's, you know, it comes in handy.

Leo: I've got to start doing that. Dan in Walpole, Massachusetts reports that his parents' computer got trojaned - again. Dear Steve, my parents' computer has gotten infected by a trojan twice in the last six months. First time they got Antivirus 2009. That bit an awful lot of people.

Steve: Yeah, we talked about that. 35 million people.

Leo: Was that the final count? Holy-moly.

Steve: Yeah.

Leo: I had them back up their data and restore from Dell's hidden restore partition. I'm not sure how they got "owned" this time. But they were getting pop-ups from "Home Antivirus 2010."

Steve: Well, it's nice that they updated the year. They're staying ahead.

Leo: He's done some research, he says that's usually installed by a trojan. Maybe Malwarebytes can fix this - Malwarebytes.org is the place to go. That does get rid of some of these versions. And most - better probably yet is the Microsoft Malicious Software Removal Tool, MSRT.

Steve: Yep.

Leo: But I suspect another backup and restore is in their future, he says. They have antivirus software. They have Windows Automatic Updates turned on. I've explained to them they shouldn't click links or attachments in email. I've installed Firefox. I think they're still using IE, he says. What else can I do to harden them against malware so they don't have to do a full restore every six months? SandboxIE is going to be too hard for them. So is a VM. You know, you can't harden people against...

Steve: Bad habits.

Leo: Yeah. There, thank you. I was going to say stupidity. That's much nicer.

Steve: Yeah. The only thing, I mean, the only thing I would think is he didn't mention what their email client is. It sounds like if he's unable to pry them away from IE, they're almost certainly using some flavor of Outlook.

Leo: Yeah, yeah.

Steve: Which uses the IE display control by default. The only thing I could suggest, I mean, would be moving them to a non-Microsoft email client, maybe to Gmail through Firefox. I wonder how they're using IE? If he's installed Firefox, I would imagine it's now the default URL handler. So when they click on links it's going to open Firefox. Unless they're still using Outlook, in which case they're technically still using IE because it's what's viewing their mail.

So I would say to Dan, get them away from Outlook. Outlook has traditionally and historically been probably the number one problem. You could argue now that browsers are more of the target than mail. But from the history that he's talking about it sounds like they just can't not click on things in email. So to make that safer would be the thing, would be the next target of opportunity that I would try to go about changing. Just switch them to something other than Outlook. And maybe hide IE from them so that they're not able to get to it. Put Firefox's icon where IE is and just say, no, folks, you really need to do this. The other problem is it sounds like Dan's cleaning up their problems, and so it's really not a problem for them. They may just be...

Leo: They're not incented to do anything.

Steve: Exactly. They're just casual computer users. And it's like, "Oh, son, we've got a problem again. Come over for dinner and fix our computer." So Dan does. Doesn't seem like it's causing them a huge problem.

Leo: Nope.

Steve: But I'm sure glad he's on top of it because it could cause them a huge problem.

Leo: You bet. I guess, you know, the thing is we used to say don't click on links in email. But now really anytime you get a popup that says "download something" or "fix this," that sounds like what's biting them. They should, you know, think twice before you say, oh, thank you.

Steve: Well, yes. In fact in both of those cases, both the Antivirus 2009 and Home Antivirus 2010, what happens is you go to a site, and it says, oh, scanning your computer for malware. And it shows you the progress bar, and it says malware has been detected. Click here to take care of it. I mean, again, it sounds like there's an education problem. His parents don't know any better. So they're, oh, no, and they don't want to

bother their son Dan. And so they think they can handle this themselves. Unfortunately, they've just gone down the wrong path.

Leo: Maybe Dan sent it to us. Thank you, Dan. Antivirus 2010 is here.

Steve: Yay.

Leo: What's maddening, and maybe they need a better antivirus, is that their antivirus isn't catching this. Shouldn't it stop this behavior? Seems like if it's got good heuristics it would notice this. Anyway...

Steve: Yeah. The problem, of course, is that's always a moving target. They're always lagging behind.

Leo: This is what I say on the radio show, that your software, your antivirus, your firewall, that's a second line of defense. You are the real line of defense, and your behavior.

Steve: Right, right.

Leo: David Stephens in Bloomington, Indiana wonders whether a VPN can be used to transport a virus. Steve, I've been listening since Episode 1 of Security Now!. I've learned so much from you and Leo in these four years. I can't begin to thank you both enough for helping me learn so much about protecting myself and friends and family online.

Here's my question: I was talking with my boss today, and we were wondering if a virus can travel through a VPN and infect a PC on the other end. Her son recently had a very nasty virus infection on his PC that we think he got through a file he downloaded in Limewire. Yeah, that sounds right. I know, that was the first mistake. My boss asked me today, if a virus from her son's PC was able to make the leap to her PC, would it be able to go through the VPN she's set up, back to her office, and then infect PCs there? I thought that was a good question. I don't know the answer. I knew you would, though. If this is a possibility, would simply putting an additional router in her home and segmenting off her PC do the trick? Thanks for your help, Steve. It's always appreciated.

Steve: Well, that's a great question. And unfortunately the news is all bad. It is certainly the case that a VPN would transport a virus, that is, it's not what it's designed to prevent. It is essentially, like, providing a secure link between Mom's machine - which is sometimes on the home network. But when the VPN is established, now the machine is on the corporate network and probably insulated from the home network. So the threat model here is that when the VPN is not on, and Mom's machine is on the same LAN as her son's machine, there certainly are viruses that are LAN aware. We've talked about them not long ago on this podcast, where there are things that propagate through Windows shares, that use the fact that they're behind the router and look for other machines on the network and jump over to them. So that would allow an infection to

jump within the LAN from one machine to the other. And that is a frequent occurrence these days. It's one of the ways that malware is propagating itself better because it knows that it's frequently going to have other machines that are there.

Then, when the VPN comes up, that machine which is now infected, it's essentially on the corporate LAN. And so the same scenario recurs. And what's worse, now we've got malware that we know is LAN-aware because that's how it infected this machine, Mom's machine, because it was LAN-aware. So now it's on a huge LAN with all kinds of potential targets.

Leo: Ooh, goody, goody, gum.

Steve: Exactly, it's just found nirvana. So it uses its VPN connection, which is essentially it's protecting bad guys from getting in. But once you're in, once you're on the corporate LAN, all the goodies are there and available. So it's certainly the case that a corporation needs to protect itself - and this is a common occurrence - protect itself from infected traveling machines that connect by VPN into the LAN. So this is a well-understood problem.

It's certainly the case that protecting Mom's computer when it's not LAN-linked into the corporate network is a good thing. And we've talked about using multiple routers to segment a LAN so that machines can't see each other, so that you have an insecure and a secure LAN area. And that's - we've done some podcasts on that. So I would recommend that Dave takes a look back in time. As you said, Leo, all of these things we've talked about are still surprisingly relevant. You can almost wish they weren't so relevant any longer, but things have not gotten any better in the last four years. And so that would probably solve the problem.

Leo: Yeah, yeah. Yeah, VPN just means it's the network. You're just - you're expanding the network, that's all.

Steve: Exactly.

Leo: All right. So that's 12 questions. But we do have one more side note. And I thought we'd throw this one in at the end. Dave Schuh in Maple Grove, Minnesota. His subject is "Vitamin D - a great tangent." I've been, by the way, yesterday intentionally did my rowing out on the deck at the gym so I'd get full sun. And I even took my glasses off so the light would get in my eyes because you need Vitamin D in your eyeballs, too. But we'll - I don't know if this makes a difference. But let's find out.

I've listened since the beginning, and I hope you never stop doing the show, Steve. Also a SpinRite owner. I was very pleased to hear your take on Vitamin D, having been in the science field and following it for many years. I'm a white male about your age, also starting to track my blood level, specifically summer versus winter. I live in Minnesota, and for exercise I like to run. So about six months of the year I can get my exposure without supplements. And I agree with you that supplement amounts are very low. So it will be interesting to see what level I can maintain during the frozen tundra months when I can't get outside. The tangents you and

Leo, by the way, go on are very enjoyable, like sci-fi. I would love to hear occasional updates on your Vitamin D research. Thanks for the great show and all your hard work. Dave. Thank you, Dave. So? So? I want to know. What's the deal?

Steve: We're going to talk about it next week.

Leo: Really?

Steve: The first episode of our fifth year.

Leo: So why don't you tell folks, recap what you've been talking about.

Steve: What I have to say is that we've had a lot of people who've written in and said, love to hear about security. It's called Security Now! for a reason, and certainly that will always be our focus. From time to time things come up which are important. I've been researching Vitamin D as a health hobbyist. We all know I'm not a medical professional. Packets are my passion, and Internet and security and coding. But health is also a passion that I've only talked about glancingly from time to time. But when I get into something I generally get in with both feet. And I've read, oh, maybe 50 to 60 scientific journal articles now, and I am full to the brim with a bunch of information which has begun to sort of take form and is coherent and I think is really important. I would argue that next week's podcast will be the most important podcast we've ever produced.

Leo: Really.

Steve: I really think so.

Leo: Having nothing to do with security.

Steve: Having, for once, I mean, we're going to wander off the reservation. But don't worry, we'll be back the week after. But we're all human. We all have bodies. It is the case that from everything I've read, and I have - I'm putting together a page that'll be up next week. with links and PDFs for full documentation of everything that I've learned so people can go to the same source. But it's very clear to me that the lag our medical system has is a problem in this instance. This has come together in a way that I can also tell a story about how we evolved and where Caucasians came from and why. And I believe that our listeners...

Leo: Oh, this is good. I'm going to tease this. Next week: Where Caucasians came from.

Steve: And why.

Leo: And why.

Steve: Yes. I mean, there's a story here. There's an amazing amount of epidemiological research, which is only beginning to happen in the last few years. And again, I'm not kidding when I say that for our listeners I think this will be the most important episode we've ever produced.

Leo: Wow. I can't wait to listen. I'm very excited.

Steve: And I will spend more time producing this next episode than I have ever spent on any podcast before. I just - I really sincerely believe it's important. And I know our listeners care about us. We care about them. And believe me, I mean, I believe that one of the things people enjoy about the podcast, as we've read from time to time, that people appreciate the fact that I can explain complicated things in a way that they understand. I may have let down our one listener earlier today who asked for a simple explanation of cellular broadband security.

Leo: Okay.

Steve: But I understand pretty much the whole picture now, although I'm not a biologist or a trained medical professional. I understand the whole picture of Vitamin D metabolism. I'm going to explain it because it turns out to be important. And I think our listeners will find it really fascinating. Which is why they tune in.

Leo: I'm sure they will. We will. And I should say upfront, and we'll say it again next week, you're not a - you're a scientist. You're not a junk science - Steve is the least superstitious person I know. So this is not going to be some airy fairy thing. This is going to be based on research.

Steve: No, I mean, it's the Mayo Clinic, lots of references from the American Journal of Clinical Nutrition and the Journal of Nutrition and, I mean, serious science which has been done, which has just not come to light. And the good news is dealing with the consequences of what I will describe is incredibly simple and inexpensive.

Leo: And what we'll do, by the way, we'll still have the security news at the beginning and the errata at the beginning. So you'll get that security fix. And if you're not interested in the Vitamin D, although I think you will be, move along. That's the beauty of a podcast. You don't have to listen.

Steve: I would, yes, I will urge our listeners, I'll hook them in the first 10 minutes, I promise. And I don't do fluff. This will not be fluff. This is important.

Leo: Great. I look forward to it. Steve, thanks, as always. A wonderful show, a great

episode. Thanks to all our correspondents. If you have questions for Steve, GRC.com/feedback is the place to go, and we answer questions every other episode, every even episode, at least at the moment. And of course at GRC.com you'll find the 16KB versions of the show for quick download, if you're bandwidth impaired. There's a transcript. It's very easy to download, read, and search, one of the reasons Steve does that. Show notes are excellent there, too. And of course all of Steve's great software, most of which is free - programs like ShieldsUP!, Shoot The Messenger, DCOMbobulator, Perfect Passwords. And there's one paid program out of all of that, that you must have there, and that's SpinRite, the world's finest, the only hard drive maintenance utility you will ever need. GRC.com. Steve, we'll see you next week.

Steve: Talk to you then, Leo.