Listener Feedback #90

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-244.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-244-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 244 for April 15, 2010: Your questions, Steve's answers #90.

It's time for Security Now!, the show that covers everything you need to know about keeping yourself safe online. And here he is, our safety guru, the man in charge at GRC.com, the Gibson Research Corporation, creator of SpinRite, the world's finest hard drive maintenance utility, and an expert on all of this stuff: Steve Gibson. Hey, Steve.

Steve Gibson: Hey, Leo. It's great to be with you again. That was a little more of a melodic opening than you normally give [indiscernible] quite enough...

Leo: I started to sing. You know why? You probably don't watch this because there's no spaceships in it. But I watch this show called "Glee," and it debuted last night. And I've been singing my little heart out ever since.

Steve: I've seen commercials for it. And something, some guy was, like, doing an "L," I guess, for G-L-E-E or something with his hand, but...

Leo: Yeah. Because they're the - the Glee Club is the losers in the school, and all the attention goes to the cheerleaders and the jocks. And the head of the cheerleaders is the evil villain in this show. But the only real reason I watch it is because they burst into song fairly frequently, and I love that.

Steve: Are you familiar with, oh, I'm forgetting the name of it, on HBO, where they do the same thing. Two crazy guys...

Leo: Oh, the "Flight of the Conchords."

Steve: "Flight of the Conchords."

Leo: Love, love, love "Flight of the Conchords." I just adore them. Yeah.

Steve: Okay. Well...

Leo: Anyway, [singing] that's why I'm singing, I'm in the mood for song. Now, today we have a Q&A. You may ask...

Steve: #90.

Leo: ...why is Leo singing? Because I love Q&As.

Steve: And not because it's tax day today in the United States, April 15.

Leo: Ugh. Nothing to sing about there, I'm afraid. Although you and I both have finished our taxes long ago. Because...

Steve: Thanks to having elves.

Leo: We have people. Thank god. 51 years of my life I did my own taxes. And finally I have people. People who do it all year. That's the key; right? It's not like you're going to H&R Block. It's somebody who's collating the stuff all year.

Steve: And that's, yes, exactly. You want to do it incrementally. So, I mean, I'm sending receipts to Sue throughout the year. And so she's presumably, it's not some horrible thing at the deadline. She pretty much has our stuff done and ready, you know, early in the year. So that's good.

Leo: Oh, thank you, thank you.

Steve: So we've got a bunch of interesting stuff. Great questions, a mix of stuff, people talking about our subject from last week, of course, which was the SSL security certificate problems with state-sponsored spying and so forth.

Leo: SSL should stand for state-sponsored something. Lawlessness, I don't know.

Steve: It's bad.

Leo: Yeah.

Steve: But we've got a bunch of that and other stuff I think people are going to find interesting. This is, here we are on the 15th, puts us just past the second Tuesday of the month. So as always, we've got the Microsoft second Tuesday of the month security event as just behind us.

Leo: Yes.

Steve: There were 11 bulletins issued, which addressed upwards of 25 different problems which Microsoft had flagged as both critical and important. Some remote code execution, some privilege elevation problems. They were in Windows and Office and also some Server components. And pretty much most of the things we've talked about that were pending were fixed. That longstanding SMB, the Server Message Blocks problem, has been resolved. You may remember that that was the problem where somebody - you could go to a malicious site that would cause your system to establish a filesharing connection to a remote malicious server, which could then take advantage of a vulnerability that had been discovered to execute code on your machine. So that's happily fixed. We also had, we've talked about before, the Windows Help file problem, where you could get a Help dialogue that would pop up. With a little bit of social engineering you would convince the user to press F1. And in doing so, that allowed a bad guy to run code on your machine. That's been fixed.

Leo: Yay.

Steve: Yay. Also MP3 files had a problem, which was not publicly known. It was privately reported. But there was a way that someone had discovered and then informed Microsoft that just going to a site and clicking on an MP3 link, causing your system to attempt to play a file, there was a way of formatting that file maliciously so that, once again, it would run code in your machine.

Leo: Now, that's a big deal because usually we say, oh, you're safe with documents. It's only programs that can install or infect your machine. Which is still true, but it takes - but if the program is mal- what is the program that - the player that's not working?

Steve: It's Windows Media Player. So it was a problem there. And, you know, we have seen, for example, malicious images.

Leo: Oh, yeah. And we've seen malicious MP3s through Winamp. There was a flaw in Winamp. This isn't the first time. It's just that those are rare compared to the other modes of infection. Because people are always saying, well, Leo, I want to save my data. Is it safe to save my data? And the answer is yes. But data can still cause a problem. Actually it's not strictly speaking yes because there's macro viruses, too.

Steve: Yeah. I would say that, unfortunately, what is - the domain of what is safe is rapidly shrinking. And it really doesn't seem to be getting any better. We're seeing, I think, just a - we're seeing continual development of code. And as we've said, it's so difficult to be perfect. And to be secure requires perfection. You could argue we're not ever going to get there. So, you know, we're not ever going to run out of things to talk about on the Security Now! podcast.

Leo: I guess there's a blessing there.

Steve: So, and I'm sure you heard that the U.S. Federal Appeals Court dealt a blow to 'Net Neutrality.

Leo: Yeah.

Steve: What happened was, some time ago the FCC sanctioned Comcast for specific handling of BitTorrent traffic. And we talked about this a long time ago. Comcast was looking at their customers' traffic and dropping BitTorrent connections, which a lot of people got up in arms about, feeling that that was, you know, really not playing fair. The FCC sanctioned Comcast. Comcast sued the FCC, saying you don't have the authority to regulate this aspect of our business. And it turns out that initially that lawsuit failed, and then they appealed it, and the U.S. Court of Appeals agreed with Comcast that the FCC lacked the authority to enforce what it was trying to do. They were relying on some congressional sort of broad, sweeping, the FCC's rule is to make the Internet a better place and happier for all people or [laughing].

Leo: You know, I got into - I've gotten into an interesting email exchange on this with a person who is not a lawyer, but who is an expert in telecommunications. And he says it's actually more complicated than just, oh, the FCC no longer has the right to weigh in. So it's complicated. It's not quite as sweeping as I had originally thought. I agree with you. I thought, oh, this means that FCC has no jurisdiction over the Internet. Not so.

Steve: Right.

Leo: But it's not - it's shaky. And the problem is this District of Columbia Court of Appeals is historically just very antiregulatory. So people go to them to say when they want regulations, government regulation overturned.

Steve: My problem is that the people who argue against 'Net Neutrality take the position

that we're in a competitive marketplace, and that the people who, the providers who perform onerous filtering will lose market share.

Leo: Right.

Steve: But I'm here in Southern California, and I have no choice of cable provider.

Leo: There's no market, right. There isn't a market.

Steve: There's no competition at all.

Leo: And that's what Comcast said is, oh, you see, the market's going to be fine. We don't have to worry. And then they loved that because they have a monopoly in many, many, many, many markets. Or at least a duopoly. So my correspondent - whose name is Christopher Mitchell, he's director of Telecommunications as Commons Initiative, Institute for Local Self-Reliance - said that it's not so much a you-can't-do-it as you-did-it-wrong.

Steve: Right.

Leo: The problem is, of course, they will have to go back to the D.C. Circuit every time and roll the dice on what the D.C. Circuit says because it's kind of - they're kind of activist judges there.

Steve: Or get the legislation that...

Leo: That's what I think.

Steve: ...makes this very clear.

Leo: And he says, and I agree with him, what we need to do is treat the Internet as infrastructure, like water and power, and Comcast as somebody who is sitting on top of that infrastructure. Unfortunately, of course, it's not government run, and shouldn't be government run, I don't think. But it's private industry-run infrastructure, so it's complicated.

Steve: It's the Wild West.

Leo: Yeah.

Steve: Even now. I mean, and the stuff we talk about here often demonstrates that.

Adobe has now formally started telling users to do what we told our listeners to do last week. You may remember that it was discovered that there was a way to cause PDF files to execute programs. And last week I instructed - I think it was last week, might have been the week before - instructed our listeners in the same vein as disabling JavaScript in Acrobat and the Adobe Reader, that they ought to go into the options under Trust something or other, and disable the ability to have PDF files run executables. Well, Adobe is apparently now formally considering setting that off by default, where it's always been on by default, which would be a big improvement. In the meantime they're saying, well, just go in and...

Leo: Turn it off.

Steve: ...turn it off because it's a problem. Oh, and there's been a demonstrated functional proof-of-concept worm created from this, meaning that documents could - that it's possible to create a worm, meaning something that operates without any user intervention and spreads across the Internet using PDF documents as its transmission medium.

Leo: Geez Louise.

Steve: So I think that finally got Adobe's attention, and they said, uh, okay, we think maybe we'd better turn this off. I mean, yes, I think so. And this was sort of a twisted new approach on scanware. We've talked about scanware a lot, you know, the XP antivirus dialogue that comes up and says your machine is infected, please purchase this - we've scanned your machine, and we found a problem. Please pay us money, and we will disinfect your computer.

Well, there's now a trojan called the W32.torrent.a trojan - that's what F-Secure called it - which is getting into people's machines. And when they're running BitTorrent, it pops up a notice saying that their system has been scanned, and the transfer of copyrighted materials into their computer has been confirmed, allowing them to pay $400 in a pretrial settlement to avoid further prosecution, which would involve five years in prison and $250,000 in fines. And apparently people are paying.

Leo: You're kidding.

Steve: No.

Leo: People are fooled by that.

Steve: Yeah, I mean, well, they're panicked. They know what they're doing is violating copyright.

Leo: And they've heard that these letters go out.

Steve: Exactly. And so it's interesting, I mean, this is a social networking leverage. It takes advantage of them being aware that people have been sued. This notice pops up. They don't realize this is different from what has happened to other people. And it's like, oh, I only have to pay $400? That's a pretrial settlement, and then I'll bet let off the hook? And people are doing it. So...

Leo: Wow. Wow. That's so - that's sad.

Steve: Yeah.

Leo: That's just really sad.

Steve: I don't know whether to feel sorry for them or not because, I mean, they are using BitTorrent, and they are moving movies around, and music presumably, and lots of big copyrighted things. So...

Leo: Yeah, I mean, they're only paying because they're guilty.

Steve: Yeah.

Leo: I mean, they feel guilty, anyway. Or they think they're guilty. They're scared, that's for sure.

Steve: And then, lastly, there's a new zero-day flaw which has been uncovered in Java. Ever since Java 6 Update 10, which is about eight updates ago, there have been some additional utilities that Sun has packaged with the Java installation which it turns out has enabled a specially crafted website or specially crafted websites, in plural, to download additional Java code into a machine, causing it to run local executables, essentially giving it all the kind of power that you don't want to have in visiting a website. Sun is being a little bit lackadaisical, saying, well, yes, we don't think that's that big a problem. We're going to just wait until we do our quarterly Java update. So it's like, okay, well, let's hope that this doesn't actually start being a big problem. The good news is, Java is, unlike something like Internet Explorer, not installed in a huge number of machines. So the size of the target is arguably smaller than it would be...

Leo: Isn't Java on every machine?

Steve: No, not the whole JVM. Normally you get that installed only when certain applications require it to be brought along.

Leo: I see. So if you've got - if you're running Java...

Steve: We're not talking JavaScript.

Leo: No, I understand.

Steve: Yeah, okay.

Leo: But what do you - okay. So you need the JVM if you're going to run any Java application; right?

Steve: Exactly.

Leo: Oh, I think almost everybody has Java on their system. Don't you?

Steve: No, I don't - I wonder what the percentage is. I don't, so...

Leo: Really?

Steve: Yeah. It's like on one machine of mine, I think.

Leo: Huh. God, I have it on everything. And it doesn't come with Windows anymore. It used to. It used to come with everything. I'm pretty sure it comes with OS X. Huh. Now I'll have to check. I thought everybody had the JVM on there. Because frequently, you know, if you - for instance, I mean, there's a lot of - if you use GoToMeeting, GoToMyPC, you're using Java.

Steve: Right.

Leo: Oh, that's interesting.

Steve: I don't know what the percentage of deployment is. That would be interesting to know.

Leo: Yeah. It used to be like Flash. Used to be everywhere.

Steve: Right, ubiquitous.

Leo: Ubiquitous.

Steve: I did get a nice note from an Ernie Moreau, who wrote that SpinRite saved his vacation. He said, "My name is Ernie Moreau, and I live in" - wow - "Kelowna, BC, Canada."

Leo: Yeah, Kelowna.

Steve: Kelowna. It's a silent "w." Kelowna, BC, Canada. "This is just a simple SpinRite-saves-the-day story." Hey, we love them when they're simple. But this isn't that simple, actually. He says, "I was vacationing in Toronto with my family. We were at Canada's Wonderland, an amusement park just north of Toronto, when I got the call. 'Ernie, the web server won't respond.' So I found a park bench and had my wife take Dylan, my five year old, to the kiddie rides. While calming my boss down, who was on the phone, I asked him to do a hard reboot. It booted straight to a Blue Screen of Death."

Leo: Oh, no.

Steve: "At this moment my training kicked in. After listening to 200-plus episodes of Security Now!, I knew what to do. I told my boss, 'Do exactly what I tell you to do. This is not a test. On my desk is a red binder. In the binder there's a disk labeled "SpinRite." Stick it in the machine and reboot. Run it at level 2. Call me when it's done.' 'That's it?' he said. 'That's it.' I told him that it would take several hours to complete, but it was a lot quicker than getting the next flight home."

Leo: Yes.

Steve: "When he called me back, I had him reboot the system. Everything came up as it should, working perfectly. This allowed me to come back the following weekend, when my holidays were done. Since I have the machine backed up 12 ways to Sunday, I wasn't too worried about the drive crashing again. The following Monday, just to be sure, I rebuilt the machine with a new hard drive. No worries. SpinRite saved my vacation. Thanks, Steve." Oh, and he says, "One last thing. I have an iPad now, and love it, and would like your recommendations of which Peter F. Hamilton book to start with." I would start with "Fallen Dragon."

Leo: I agree. What a great book that is.

Steve: It's a single book to read, not a multivolume set. And...

Leo: It's long. It's not like it's a short book. But it's a great book.

Steve: Oh, yeah, I mean, it's wonderful. Like I don't think Hamilton ever wrote anything short.

Leo: No. And by the way, you won't be buying that in the iBookstore, I don't think. I haven't checked. But they have a very limited selection. You'll be buying it...

Steve: There's nothing there.

Leo: There's nothing there. But you can get it on Amazon, and the Kindle app is just fine on the iPad. It's what I read most of my stuff in is the Kindle.

Steve: Exactly, me, too.

Leo: And then you get the benefit, by the way, of being multiplatform. The iBookstore thing is, you know, you're done. But you can run this on a Kindle if you have one. You can run it on your iPhone if you have one. You can run it on your PC or your Mac if you have one. I think - what is Amazon's rule? Five devices?

Steve: Is there a limit?

Leo: I think there's a limit.

Steve: Makes sense that there would be because I was thinking, now that I'm familiar with it on the iPad, I was thinking I would try it on a PC. I had never had an occasion to do so, but, but I'm really impressed.

Leo: Yeah, they have desktop. It's great because - and the whisper synch and the whole thing, it's just a better platform. And I think it's kind of interesting that Apple allowed the Kindle app on there because it's a trojan horse. I mean, it's really, it's like...

Steve: I'm so glad, though.

Leo: Oh, I'm hugely glad. You know, I think Apple is realizing that they can't be too draconian, or people are just going to rebel.

Steve: And didn't we just also hear that they have allowed Opera to...

Leo: Never thought that would happen in a million years. That's a huge shocker.

Steve: Yeah. I'm happy with Safari, that's there. But I'd like to see if there are more features in Opera because I would like a really full-featured web browser on the iPad.

Leo: Yeah, well, first of all, it's not iPad yet. But...

Steve: iPhone.

Leo: It's iPhone. And I have to say it is not more full-featured. But it's certainly worth looking at. I wouldn't turn my back on it. It's free. Steve, we have questions. You have answers. That's what you do best. #90.

Steve: Great feedback from our listeners. And so we'll plow through it.

Leo: John Moehrke in Milwaukee, Wisconsin, starts us off. Should I say who he's with?

Steve: Sure.

Leo: He's with the medical division of General Electric. Steve, I grit my teeth every time you say SSL is broken. Yet most of the time it isn't SSL that's broken, but the policies some have chosen to use to simplify our lives. So as an example, last episode, the problem with SSL server certificates, this isn't broken SSL, this is a broken policy. I recommend SSL very often to protect healthcare. I'm involved in all of that stuff going on in Washington, D.C. around healthcare IT.

I often have to reverse misunderstandings. In addition, I have to point out that the recommendations that we're giving with healthcare are to use multi-authenticated TLS to a well-controlled certificate or CA branch that is highly controlled, following a system inspection and business agreement. This isn't just server authentication to a list that some browser vendor chooses. He has a site: healthcaresecprivacy.blogspot.com. So this is a guy who focuses on this: healthcaresecprivacy.blogspot.com. Thank you, John.

Steve: Yeah. And of course I agree with him.

Leo: He's absolutely right, yeah.

Steve: We have seen a couple instances where SSL itself, the protocol is broken, and we've covered that in excruciating detail and talked about how that could be exploited. But he's absolutely right that, when things like our discussion from last week happen, where we're talking about the problem with can we trust the certificates that our browser is receiving, and part of SSL is not only encryption, as we know, but is authentication, then we're relying on the integrity of the certificate authorities to have appropriately verified the credentials of anyone they issue certificates to.

So the problem is that it's a sophisticated technology, a sophisticated system. And when we connect one way to a browser, I mean, to a remote server with our browser, we're getting authentication, we hope, of that remote endpoint. Now, he talks about, in his note there, he says healthcare are using mutual-authenticated-TLS to a well-controlled certificate or CA branch that's highly controlled following a system inspection and business agreement. So he's making very clear and, I think, properly delineating that, if you have mutual authentication, meaning certificates at each end, whereas for example in our browser-server model, the client-server model, we're only getting single-ended authentication. He's saying mutual authentication using an issuing certificate authority

that, you know, again, where you have strong reason to trust, and there's a lot of control being applied, then there's nothing wrong with that.

And I would say absolutely true as far as we know. We always have to say "as far as we know" because, until we found out recently that SSL v2 had a big problem, we thought it was perfectly secure. Then we learned, whoops, that renegotiation hack allowed some games to get played. So absolutely, as far as we know, the only problem that we were discussing last week involved certificates that we couldn't trust. The problem, of course, is that we want, and arguably need, to be able to trust those certificates. So, true, the technology is not broken. But exactly as he says, the policies are, well, they're a lot more gray than we thought they were two weeks ago.

Leo: Right. Yeah, and I'm looking at his blog, I mean, this guy is - this is clearly his bailiwick. I mean, he says he's a principal engineer specializing in standards architecture in interoperability, security, and privacy for GE Healthcare. He's a member of the Privacy & Security Workgroup of the HIT Standards Committee and co-chair of the Security, Privacy, and Infrastructure Domain Committee of HITSP.

Steve: And he's listening to this podcast.

Leo: Yeah, I mean, this is a - yeah. Actually, it's a good point, and I do wish we had brought it up, which is, it is possible to use SSL certificates safely. It's just the default that we use, as browser users, we focus, frankly, we focus on consumer use most of the time. So the point is that it's possible to do it securely.

Steve: Yes. And in fact, as you might imagine, a number of people had comments from last week's episode, and we'll be getting to them and cover various aspects of this. So again, thank you, John. You're exactly right. SSL has had some problems. But I don't want him gritting his teeth and wearing them down because...

Leo: It's bad for you.

Steve: And I'm glad there's someone like this who really understands the stuff, who's involved in helping to form policy. Because I was talking to my own GP, who's got a whole room full of paper records, and saying, you know, this is all going to be going online here one of these days. And he just shakes his head, and he says, oh, he says, I'm so worried about that. I said, well, good.

Leo: Is he worried about it from a security point of view, or just the cost?

Steve: Security. No, absolutely, he happens to be a techie. He was, you know, when we first met and were comparing notes, he was bragging about the size of the RAID that he had at home for all of his media stuff.

Leo: Oh, that's neat. He is a techie. Wow.

Steve: Yeah.

Leo: Question 2...

Steve: He said, "I have terabytes." I'm like, oh, good for you.

Leo: Question 2 comes from Nasko Oskov, another security expert, at Netsekure.org. He's describing his project relating to subverting SSL. Steve and Leo, I wanted to let you know about a small project that started the moment the "Subverting SSL" paper came out. I've collected some data on most widely used root CAs, such that the list could be trimmed down to 20 to 30 CAs. He's actually posted the list on Netsekure.org. I've also started a personal project, 30 days with almost no trusted CAs - does he maybe mean untrusted CAs? - where I deleted all - oh, no. He means no trusted CAs. I deleted all trusted roots and am adding them one by one as things break. Ah.

Steve: Yup.

Leo: So he's seeing how important this list of trusted roots is. So when he gets to a site that says, hey, there's no certificate, then he'll add that CA. I'm tweeting about each cert that I'm adding and will describe the whole experience in my blog. I'm going to include guides on how to properly disable these - by the way, removing, he says, is not the right approach. There's a better way to disable certificates, both in Firefox and Windows Certificate Store. I thought this might be of interest to you and the listeners. Thanks, Nasko. Wow, that's really neat.

Steve: It is. And so I wanted to bring this to the attention of the subset of our listeners who wanted to take some action of some sort following last week's podcast. I mean, it generated a huge amount of feedback because people were upset by this. And many of them said, well, wait a minute. The problem is that Windows is implicitly trusting 260-some-odd different certificate authorities. I don't need to trust all of those. I don't need the Hong Kong Post Office to be in my certificate store, and I'd rather it won't.

So what this guy has done - and I would encourage our listeners to go to Netsekure.org. And he's right there on the front page at this point in time. He's got an interesting list of the number of sites. He went to, I think it was Alexa, and got, like, all of the top ton of sites, and then sorted them and analyzed them for who their certs were signed by. And so he shows a most number of occurrences to least number of occurrences signatures of certificates that he's run across.

At first I was surprised that VeriSign was, like, the first instance of VeriSign on this list that was sorted from most to least, it was like in the fourth place. But then as I looked closer I realized that there were many instances of VeriSign or their subsidiaries that were occurring in the list. So if you added all those up, VeriSign is still, as we believed, the number one issuing CA globally. But so he's done a lot of work with this. And I know that a chunk of our listeners who want to do something would want to pursue it. And the reason, for example, that deleting the CAs, for example, out of Windows, the Windows trust store, is as we described last week, Windows repopulates it. If it's not in the trust store, and your browser can't find it, Windows behind the scenes goes and gets it for

you. So you want to disable it so that Windows won't replace it, rather than delete it.

And I'll remind people again that Firefox runs its own set of CAs, that is, it brings them with it. And so it's independent of Windows. Whereas the other browsers running on Windows - Chrome, Safari, IE, I'm not sure about Opera - they rely on the built-in Windows security facility, the Windows trust store. I think Opera does, actually, because I don't think it has its own security engine. Firefox and Mozilla have NSS, which is the security technology that all of the various Mozilla projects are written on top of.

Leo: So his blog, once again, is Netsekure.org, if you want to find out more about that. I'm interested in the technique for replacing the certs. I think this is a good project. Somebody probably will end up writing a - I imagine it's a registry hack you could do this with.

Question 3 comes from Mariusz S. Cybulski in Guelph, recommending a better disposable email solution. Hello, Steve. Love your netcast. Congratulations on having the best security netcast, once again, podcast award winner. In 242 you talked about Disposeamail and how everyone can see the email sent to the disposable address. Well, how about this site, SpamGourmet.com. It allows you to create an account that only you have access to, and all over a secure HTTPS connection, not just the logon.

You get to select how many junky emails you get sent to your real email account, which you configure with them ahead of time. You can have them send up to 20 emails, but can always reset if you need more. Anything past that threshold, more than 20, let's say, gets eaten by their servers. I guess this means to the address that you've registered with them. So if I register spam@spamgourmet.com, I can then tell SpamGourmet I only want to see the first few that come to you. After that, eat them. Is that what he's saying? Is that your understanding?

Steve: Yeah, I'll tell you all about it.

Leo: Oh, okay. Best of all, you get to create a new email on the fly, which is automatically linked to your account with them. This is a great free service, and they also provide several domains, not just SpamGourmet.com. You can select from a list. Helps if a company blacklists one domain because they're harvesting for your real email, and they don't like it when you give them a disposable one, which by the way happened to him when he visited iCoke.ca. But the other domains, you know, they add new domains all the time. All right, well, okay, how does this work?

Steve: Okay, so this is cool. They seem to be really good guys. They've been around for at least six years, so they're not just some new upstart. They've got an online forum with posts dating back to 2004. And I created myself a persona there. And it looks pretty nice. The idea is, okay, the Disposeamail's hook was that you didn't have to create an account, you never had to be known by them...

Leo: You don't even have to do it - you don't even have to visit them. You can just do it.

Steve: Right, you just - well, and but there's some of that here, too, which is very cool. But in Disposeamail, literally, you just make up a something@disposeamail.com, and mail will go there and be accepted, no matter what the name in front of the "at" sign is. The problem being that if, for example, you use "test," then anyone could put in "test" when they go to the website and look up this big bin of all the mail that's been sent to that account at Disposeamail.com. So there's absolutely no privacy. And unless you use really unique account names at Disposeamail.com, there would be a high probability of collision. And even so, no security there.

So SpamGourmet.com is different. There you do have to do a little work ahead of time. You go there, put in a username and password in order to identify yourself to the system. So you create an account. It's all free. And again, they really do seem to be good people. They solicit donations kind of quietly. It's not in your face in any way. And they don't send you other junk. So then you are able, without talking to them ahead of time, again, without having to, like, go pre-create accounts, you can have any mail sent to anything.youraccountname@spamgourmet.com. So say that you created an account called MickeyMouse. So you would give any other website xyz.mickeymouse@spamgourmet.com. And by default three emails will be accepted by SpamGourmet.com with that prefix and will be invisibly forwarded to your real email address, which you also register with them. And after three, it will block any additional ones.

Leo: So you get the, oh, this is the account authentication email. You get the first couple or three or whatever. Because sometimes you do want the emails from that address.

Steve: Correct. Now, what you can do is, and because they anticipate this, by default you only get three. But if you give them the email address, say it was xyz.20.mickeymouse@spamgourmet.com, that sets their counter...

Leo: Oh, that's clever.

Steve: ...to 20, and it counts down.

Leo: So it's not a setting, it's actually in the address.

Steve: Exactly. You can specify it at the time that you first send this address to someone else. And, for example, you might say, like, amazon.10.mickeymouse@spamgourmet.com. And so the nice thing about this is that you would know where the email address had originated, as well, by the prefix that you put in front of your own account name at SpamGourmet.com. Then that's sort of like the easy mode. There's then a, like, more control mode where you're able to essentially manage the database that this creates. You can see all of the email that has come in. You can reset the counters. And then there's some really nice features because one of the things you'll notice is that this would inherently accept anything.youraccountname@spamgourmet.com. And they recognize, okay, that could be a problem if this got around because spammers could put, you know, they could change the prefix, knowing that it was going to come through to you, since you haven't needed to pre-create, that is, to pre-enable these prefixes.

So what you're able to do is you're able to specify keywords or key phrases which have to appear in the prefix in order for them to - so you basically are able to create filters on the prefix in front of your name at SpamGourmet.com. Anyway, I wanted to bring it up because it is - I know that our listeners were interested in Disposeamail. We got a bunch of feedback about that. So here's a slightly more sophisticated - you do have to set yourself up for it in advance. But I'm impressed by what I've seen. I read the FAQs that they've got on the site. It's actually kind of humorous, their FAQ page. So if you'd like to read something kind of fun, theirs is. And it looks like they're aboveboard. I would tend to trust them based on everything that I've seen. So I wanted to bring it to our listeners' attention, much as our listener wanted to bring it to our attention.

Leo: Yeah, sounds pretty good. Sounds great. And I'm sure there are many others. I mean, this is a fun thing to kind of play with and implement, and I imagine not too difficult to do.

Steve: Oh, and if you don't want them to be doing it, apparently all the code is available, and you can run it yourself.

Leo: Ah. That I really like. It's open source. Chris Clark - finally a name I can pronounce - in Vancouver, BC, at a town I can pronounce. He's an iPhone/iPad developer, and wonders about the iPhone's security model: Steve and Leo, you've spoken recently about the fundamental flaws in the design of our computers and operating systems related to security. I was wondering what you thought of the iPhone OS way of doing things. Applications all operate in their own sandbox without access to other apps' data and have fairly tightly controlled access to system data, like photos and contacts, through the published APIs. Third-party software cannot run in the background and has to be cryptographically signed by the publisher and is vetted by Apple before being put up for sale in the store. This vetting process includes a scan for use of undocumented APIs and at least a cursory glance from a human to check that the app isn't actively malicious.

The system isn't perfect, and those of us who work on the iPhone and iPad software frequently run into the walls of these restrictions, restrictions we've never had on a desktop. But I wonder if all this makes for a fundamentally more secure system, or if it's just security theater. There have been well-publicized problems, like the SMS hack. But does the locked-down App Store model save us from, well, everything else that's wrong with modern networked computing? Thanks for a fantastic podcast. I've been listening forever and will continue as long as you keep it going. As a computer science graduate and occasional dabbler in programming - I'm a designer by day, but I find the CS background really helps me interface with my programming team - I've found the series on fundamental computing really enlightening. All the best, Chris.

Steve: So I think it is substantially more secure. We know that nothing is perfect. We know that there have been problems. For example, we talked about the problem that people encounter when they use jailbreaking software to open up their iPhones in order to install - essentially get around the whole App Store model, and that a side effect was that a server was installed that allowed the spread of viruses and, I mean, trojans installed and all kinds of bad stuff. So it's still possible to get in trouble.

But there just - there cannot be any question but that a beneficial side effect of the

platform being closed as it is, I mean, we know about negatives to it, but a beneficial side effect is it's fundamentally going to be more secure. And Apple would certainly be reactive to any malicious app that is discovered if something snuck through their filtering and screening and checking. But just the fact that they're doing all that goes a long way to - compared to the wildly, massively, completely open platform that we have in the Windows and Mac and Linux environments, the completely, the inherently free-for-all platforms. Apple's iPhone/iPad environment is, by comparison, radically restrictive. And heightened security will be a consequence. I'm not saying it's perfect. But there's no way not to see that this is much more secure than an open platform would be.

Leo: And, you know, as time goes by, and it becomes more, you know, right now there aren't a lot of phone exploits. There have been a few, Bluetooth snarfing and so forth. But I think it's undoubtedly the case that, as more people use Smartphones, that this is going to become the platform of choice for hackers. Or one of the platforms of choice.

Steve: Yes.

Leo: They're always on. They're easily accessible because they're floating around. And I think in a way a very proactive approach towards security now will pay off in the long run once this becomes an issue.

Steve: Yeah. I do regard the iPhone and the iPad as different from that standpoint. Although, of course, the iPad, once it gets the AT&T 3G connection, will have a great deal of connectivity, too. And as we know, networking and connectivity is the friend of malware and viruses. So it does make it more risky. But exactly as you say, Leo, having a very lessons-learned-from-prior-platforms approach and being really proactive, as Apple has been, certainly goes a long way toward controlling this.

Leo: And I know from day one, I remember when Steve did the iPhone introduction. I know that they used the word "security" right from the beginning. So I think it was something that was built into their original design. And so, yeah, I think it's appropriate. I mean, when you're - here you have an opportunity to do it. You're designing a new OS from scratch, or almost from scratch. Why not?

Steve: Yes. And we've also heard recently that Apple is clamping down on the use of non-Apple development tools. And there again, by them providing the API, by them providing even the systems that developers use to create the apps, the anti-open source or the pro-open source people are less happy because here's Apple extending its control even further than the iStore, than iTunes and the App Store, out into messing around with how developers create the apps. But that will again have - there will be a beneficial impact on security. If you can use any language and hash it down into some sort of an app that runs on their platform, now, that's more dangerous than if you are restricted to use their development tools which they control and have much greater say over. I mean, these, I mean, all the lessons that we and our listeners have learned over the last four and a half years tell us this will be much more secure.

Leo: You know, they didn't mention security, they probably should have, when they were talking about this decision to block third-party tools. That's interesting maybe that Apple kind of has a stealth long-term strategy. They see a world in which security becomes more and more important, and they may have the go-to platforms if they start right now in locking it down.

Steve: I read an article from someone in the last week or two that was arguing that this was sort of the end of the open Internet, that this was closing the Internet down. And I'm thinking, no, no, no, no. I mean, the Internet will survive, and it will be just what it is. This is an arguably closed platform for accessing the Internet. But by no means is this limiting the Internet itself.

Leo: Well, you're going to have Android. You're going to have other choices. I mean, there will be Android tablets. And people who care about that will have a choice. It's not going away. But I have to say, given the choice between doing the politically correct thing and the secure thing, with people like my mom, I want her to use the secure thing.

Steve: Yes.

Leo: And that's very, you know, I hadn't really thought about this. But this really could be a significant long-term advantage to Apple.

Steve: Yes, well, while Microsoft and Adobe, for example, continually flounder...

Leo: Just struggle.

Steve: ...in just endless, endless problems with security, Apple cruises along saying, eh, not a problem here.

Leo: It's a lot easier to do it with a new platform, too, because then you don't have to support legacy. You can say, okay, let's do it right from scratch. I'm thinking now that probably was a real big part of the spec for this new OS, this iPhone OS.

Steve: Is Apple able to reach out and yank malicious apps back out?

Leo: They have a kill switch.

Steve: Wow, that's very powerful.

Leo: That's scary to people. And Apple has never used it. But it's a scary thought

that Apple might say, for competitive reasons, for anti-competitive reasons, oh, we don't want you to use Skype on the phone because our partners say we want you to use their cell phone software. They could use it that way. They haven't used it at all. But boy, it is a great thing if you find a malicious application, and you can immediately wipe it from all systems.

Steve: If they're able to maintain the requirement that an app has to be cryptographically signed, if there's not a way to get around that, and I guess that's exactly what the...

Leo: Only by jailbreaking.

Steve: ...jailbreaking does, exactly. If they're able to enforce that, if a user doesn't jailbreak their iPhone or iPad and is willing to stay within those rules, then imagine if Microsoft by comparison were able to just reach out and kill a trojan. Well, they don't have the ability to do that because there's nothing like this kind of grip and control that exists on the open platforms. Apple has that. And so I can see, yes, it's a mixed blessing in that, as you say, Apple could kill off a competitive program. But to me there's a tremendous advantage that, if something was discovered to be malicious, and arguably that would probably surface very quickly, for Apple to be able to just kill it off throughout the entire ecosystem, I mean, even the fact that that ability exists, I would argue, militates against developers bothering to create something malicious because they just know it'll have an extremely short life.

Leo: Right.

Steve: The second it becomes known, it'll get killed.

Leo: It's really intriguing. I had not - I knew about the security features, and I hadn't really thought of the competitive advantage that that provides. Question #5, Dave Popovich in Port Saint Lucie, Florida. He wonders, is the iPad safer for online banking?

Steve: Speaking of which...

Leo: Hi, Steve and Leo. With all the talk about the iPad, I was wondering how you felt about it being reasonable as an alternative for a dedicated machine for online banking. I'm currently using a Dell Mini 9 that is only used for banking and taxes. The screen is cramped, and the battery is failing, and I was looking for a way to rationalize an iPad.

Now, I know the key word above was "dedicated," and obviously the iPad is not that. But on the iPad, with its closed environment - you can only install apps through iTunes, forget jailbreaking and things like the Google Marketplace for Android - would it be a safer alternative than using my regular PC that I use for everything

else? I never get any "this website wants to install something" pop-ups on my iPod Touch - nor do we get those on the iPad. You just get a Lego block that says, "Sorry, can't display Flash." And there aren't any plug-ins for the browser. Also the device has a lock screen for privacy. And finally, if it could be used, then do you feel a dedicated application is safer than using the browser?

As always, awesome podcast. I've been a listener for years. Thanks again. And I have not been sick since I began supplementing my Vitamin D. Me, too, by the way. I've avoided a lot of nasty 'flus that friends have gotten. He says, I don't take any allergy medicine anymore, either. And my partner's been sick with the 'flu twice, and he doesn't take Vitamin D. Looking forward to your response. Very interesting.

Steve: So this is exactly what we were talking about. And we're looking - and we've talked about booting from a Linux boot disk in order to get a clean boot, in order to do online banking. I don't know whether - he says online banking and taxes. Now, as I understand it, some of the tax prep software has gone browser-based, so that you're not installing an app locally. As far as I know there's currently no tax prep software for an iPad. So you would be limited to what you could do with a browser. But the Safari browser on the iPad has caused me no trouble except it won't run Flash, which is annoying. But...

Leo: Well, but now I'm sure you're thinking you're happy about that, too, from a security point of view; right?

Steve: From a security standpoint, exactly, because, I mean, look at the problems Adobe has with Flash. So I would argue absolutely, I mean, exactly as we were just saying with the prior question, I think that the iPad, given that it is essentially a purpose-specific platform that is tightly controlled all the way back up the chain to the tools the developer uses, through the vetting that the apps get and the fact that they need to be cryptographically secured, and that Safari is, as he says, deliberately limited in not being plug-in land, where you're allowing all kinds of third-party stuff to be running in the browser, I think it's a perfect dedicated machine. And it's not very expensive.

Leo: TurboTax, I just tried, requires Flash. There's a number of free online tax preparation solutions, so I'm going to try a couple of these. But TurboTax from Intuit is not one of them. Anybody who listens to this show and hears "You need to install Flash to run our tax software" is going to run; right?

Steve: To install, exactly, our software where you're going to put in all of your private, personal details.

Leo: In Flash? I don't think so.

Steve: Yeah.

Leo: So I think this is an interesting point. Now, obviously the iPad's not going to protect you against security issues outside the iPad. Man-in-the-middle attacks, flaws with SSL, bad certificates, servers that are not secure, and on and on and on. But you're not going to have any bugs or beasties on the iPad itself; right?

Steve: There's a little tiny lock up in the title bar of Safari on the iPad. I don't know whether that lets you inspect a certificate or not. So you may be limited in your ability to inspect certificates. I mean, it is - it has the feeling of it's been sort of pared down, and you've got the essentials of web browsing without all of the paraphernalia and bells and whistles that we're used to in a fully mature, open-platform browser. But yes, I mean, for visiting your bank and conducting transactions, I think it's very difficult for this thing to get infected.

Leo: H&R Block will not do it, either. It's "You are using an operating system H&R Block Free Edition does not support." You know, I'll say one thing, and this actually just happened. My daughter had a party at our house. And I left a Netbook there for her to control the sound system with, using the Sonos software. And somebody stole it. And this Netbook, it's too bad because this is the one computer in my whole house that wasn't locked down, password-protected and everything. It did have - I had used the browser to log onto some sites. But I do use LastPass. So I changed the LastPass password. I changed - so it couldn't automatically login to LastPass. I changed Google and my email passwords in case the email program, for instance, was automatically logging in, things like that.

But, boy, it really brings home a problem, which is that we - we don't think about it a lot, which is if you lose the hardware, or a bad guy gets the hardware, think about - I'm going to do a little thing on the radio show this weekend - think about what's on here and what, if somebody malicious had access, or worse, took your hardware and had it at home, what could they do? And, now, one thing on the iPad, and I think this is a great thing, it does have a four-digit PIN lock. And it has a setting that, if after 10 tries the person doesn't guess it right, erase all data.

Steve: Wow, nice.

Leo: So I immediately turned that on on this thing and erased all data because, even though I'm using LastPass, I have been letting the browser remember passwords. And that of course is the real, one of the real threats. And the email package remembers passwords, so that's a real threat. So I made sure I PIN'd it and had it erase the data. And I wish I had done that on the Netbook.

Steve: I think that's a very good point. As we've spoken, I have never traveled out without a laptop that has a fingerprint reader. And I always configure my BIOS and the hard drive to password-protect the hard drive and the BIOS so that, if somebody got the laptop, all they can do is low-level reformat the drive in order to push the password off of it. I mean, so...

Leo: And I kind of mocked that stuff because I thought, oh, that's business people,

I'm not going to do that. And then this happened, and I realized, wait a minute, no. That's me, too.

Steve: Yeah. I'm going to - I've been using my iPad without the PIN lock. And I'm going to do the same thing, Leo, right, you know, next time I'm in front of it I will add that. That's a very good point.

Leo: We forget how much we put on there.

Steve: I just, I do want to make one note. You commented about Vitamin D. I suppress all of our listeners talking about Vitamin D. But I just want to just acknowledge all the people that have written and given me their numbers. There was one guy I read today who, after listening to the Vitamin D podcast, he and his wife and his daughter were checked. All of them were low. His daughter was at 11. He was at 25, and his wife was at 29. They're now taking 5,000 IU a day, and the daughter 1,000 IU. And many reports of never having been sick since listening to the podcast and taking Vitamin D, where they were in this perpetual annual cycle of getting sick every winter, and they went through this winter, this past winter without getting sick. And, like, people all around them had the 'flu, and they would always traditionally have gotten it, but this time they didn't. So there just has been a tremendous amount of positive benefit from that. So I'm certainly glad I took us way off the range one week and spoke about it because...

Leo: Yeah, me, too.

Steve: ...it's really been useful for our listeners.

Leo: And I'm one of those people who has not gotten sick. Question #6, John McCormack of Twin Falls, Virginia wonders what happened to ShieldsUP!?

Steve: Ohhh.

Leo: Steve and Leo, thanks for the always useful podcast. Over the years it's grown to become a fixed and welcome asset to my life and vocation. But why and how did GRC and ShieldsUP! recently die? Thank goodness it seems to be back now. Last week, when for several days I was unable to use the service because it claimed it was "too busy," which I've never seen before, I started wondering what was going on. Tell us, Steve, what happened. Were you under attack?

Steve: Well, self-attack.

Leo: Whoops.

Steve: For a couple months, something had been odd. The CPU had been going up to full

saturation, and sometimes it would come back, sometimes it would stay there for hours, then drop back to normal. And normally all of the - we have a very simple server. I've got nothing heavyweight, no SQL. All the code is mine. I'm not using active server pages or anything other than just my own assembly language. Consequently, no matter how busy we are, the server's like at 1 or 2 percent of processor utilization, like none. And so I didn't know what was happening. Well, Tuesday The New York Times, in their gadget tech blog, mentioned ShieldsUP!. And I didn't really feel that, or wasn't aware of it. But what happened was the following day, last Wednesday, at 3:00 p.m., Lifehacker mentioned...

Leo: Oh, interesting.

Steve: ...ShieldsUP!. And all hell broke loose.

Leo: Interesting.

Steve: I mean, we just - the computer, essentially the whole website just froze.

Leo: I'll have to tell Gina this. She'll be very happy to hear it.

Steve: Erica was someone who did the post. I don't know Gina. But, I mean, it had a huge effect. And so - but frankly, I've never seen this happen before to the site. I mean, it was, I assumed it was beyond buried. Yet, I mean, and lots of people were, especially while we were the No. 1 item there on Lifehacker. What I understand now is about every hour they post something new. And so I began hoping that, as we moved further down into history, this would get better. And I had never had any kind of a throttle on ShieldsUP!. I hadn't needed one. But I quickly wrote some code to limit the number of people who could be using ShieldsUP! because that seemed to be the problem, even though it had never been a problem before. And each of the - when you do a full service ports probe, that's more than a thousand ports that I'm probing, and I do each one several times to make sure that a lost packet doesn't report that a probe is stealth when it's actually closed or open because I want to make ShieldsUP! very reliable.

Anyway, so after several days we were still having a problem. And I found some technology that Microsoft had put together which allows you to take a snapshot of the IIS server in its running state, which was exactly what I needed. So I did that. I analyzed what it said. And there were - 16 percent of the threads running in the server were all being held up by one particular thread. And in looking at it, I suddenly had one of these oh-my-god moments.

What had happened was, I left my own developmental memory auditing code in the production server. What I did years ago to help deal with leaks, where memory is allocated but is never freed, is I wrapped the allocation and free and resize APIs in my own monitoring, basically my own auditing code so that, when I stopped the server, the instance of it that I'm developing on, it will tell me if any memory was ever allocated that hasn't been freed. And it tells me, I mean, it knows where the memory - how much memory was allocated, and which allocation call allocated that block of memory. So it's complete auditing of my use of memory.

And it's allowed me to have an end result that literally can run for years. I mean, it's very uncommon for Windows itself to be up for years. My server can be up for years, and even the web server running under the Windows server. Just it's a hundred percent leak free as a consequence of this technology, which just helps me catch my forgetfulness, which is easy to do when you're writing really sophisticated stuff that's got threads going all over the place, and you're allocating and releasing memory all the time.

So what happens is it's never supposed to be in the production server because of the overhead of tracking all of that. I'm allocating and freeing memory at a high rate, and adding the auditing technology really slows it down. But what had happened was, I had left it in. I had turned it on, and it had been running in the production environment for months. And so I was seeing something wrong, but not bad enough that I was able really to track it down or motivated to pursue it, or the problem would go away by the time I would see what was happening. So in this case, thanks to Lifehacker, they put enough of a strain on the server that I was able to track it down and remove it. And we've just been running perfectly ever since.

Leo: Oh, that's great. So you probably wouldn't have been slowed down by Lifehacker had this...

Steve: No. And in fact I wrote back to Erica because I did put up a notice at one point, I mean, immediately said we've been mentioned by Lifehacker, and it seems that we're unable to carry the load. So first I just turned ShieldsUP! off completely, just because I needed the rest of the site to be running. And then, anyway, so I wrote to her, and I said, hey, thanks for this. First of all, thanks for the mention, but also it helped me find a problem that I don't know when I would have found it otherwise. And so what I did was I added technology to prevent the auditing system from installing itself on the production server automatically, so I'll never have to worry about it happening again.

Leo: Yay.

Steve: So it made things better.

Leo: Brilliant. You're brilliant. Mike King in Question #7 asks - he's standing on the Eastern Shore of Maryland wondering about PDFs on the iPad. Can you give a report in your newsgroup on your experience with the iPad so far? I can't wait for this week's Security Now! netcast/podcast. The big question, can it read PDFs?

Steve: So I realized that his email must have predated my lengthy description of my feelings about the iPad after my first few days with it last week. But I did want to - I want to take advantage of his question to clarify that I have found, and I wanted to let our readers know, that it is not necessary, and I'm sure you know this, Leo, to install that really nice app that I found called GoodReader, that the iPad natively reads PDFs just fine.

Leo: Yes, that's right, yeah.

Steve: You can click on links in email, if you trust the source of the link in the email...

Leo: Well, you can email yourself PDFs, which I often do.

Steve: Yes, exactly. It's a way of getting them into the iPad is you email yourself a PDF, and then you're able to open it just with Safari, that will open the PDF with no trouble. What you don't have natively, except keeping email around and email attachments, is any kind of a file system. And so GoodReader does allow you to create folders and subfolders and basically create a nice library of PDFs within its own environment. So it brings that to the iPad. But I did want to make sure people understood that, just as it came out of the box, it was a very, very capable PDF reader.

Leo: Excellent. Question #8, Brandon in Atlanta, Georgia is under attack. Having recently become married - oh, well, that explains it.

Steve: How that happened.

Leo: He says that as if it had just happened without him having anything to do with it. I have assumed the role of network administrator for our home. I've also recently found TWiT, and Security Now! is far and away my favorite netcast. Security Now! has made me much more aware of my network's vulnerabilities and many bad habits my wife and I have, in particular password strength.

My question, however, is this. I was trolling my router's security log when I noticed several dozen entries that say "Found attack from [variable IPs] in port [variable ports]," and they all occurred at the very same moment. Is this some automated attack from some random machine trying to find insecure addresses? How can I be sure my network isn't compromised? Should I be concerned? Because, quite frankly, I am very concerned.

Steve: Okay. So I just - we hadn't talked about this for a while, and I thought it was worth, for Brandon's sake and similar listeners, to talk about what's going on on the 'Net and router logs. Anyone who logs traffic to their IP is these days just constantly seeing random junk arriving at their IP address. I mean, these are packets aimed at them. They're often to port 23, the telnet port; sometimes to 25, if your ISP is not blocking the SMT port, looking to see if you're running a store-and-forward SMTP email server. And, I mean, to 445, Windows filesharing, to see if you might have filesharing open. I mean, just there's all this junk. I coined the acronym years ago, IBR, stands for Internet Background Radiation. Because it's just that. It's just noise, mostly. It's not an attack. It's not really directed at you because, if you do look at many more, if you were to look at many more than just your own single IP, you would find this debris is just raining down on IPs all over the 'Net. So that's one form of the kind of debris that you find in your log.

The other is actually a consequence of sort of overlogging that routers do. When you're surfing, you will have - when you're surfing the 'Net and just, like, going to random pages, we've talked about how the browser model operates where you request the page from the remote server. You receive the page. That page has lots of assets on it - images, advertisements, Flash things that are wanting to jump up and down and get your

attention, and all kinds of stuff. In order to show those, your browser initiates a flurry of additional connections out to many different servers to pick up those assets.

Now, when that's all done, your router will close, or your browser will close those connections. Your router sees those connections close, and it removes the NAT mappings that existed temporarily to allow those remote assets to get back to your computer. Remember that with NAT, Network Address Translation, no external data is able to get in in the default case, that is, any packets coming in hit the router and die, making the router a very good sort of natural firewall. It's only when your router sees you behind the router, initiating outbound connections, meaning your browser or your email or whatever, that returning traffic is allowed back in through that same connection.

But when you drop the connections, when you terminate them, a well-behaved router will remove those so-called mappings. It will remove the permission for those unexpected - what were expected packets to come back in, making them now unexpected. Many sites will send back a final FIN, a finish packet, after your router has closed the mapping. And routers that are tending to be a little over-logging will log those as attacks.

Which is why, for example, the way Brandon explained it, he got a flurry of packets from different IPs coming back to different ports all at the same time. It was very likely just after, I mean, that's what you would often see after a web page has been fully served. Those connections get closed. The router says thank you very much. Those random scattering of web servers out on the WAN may send a few more last little straggler packets that really are not an attack. They're no harm at all. But the router says, wait a minute, I'm not expecting this. Well, it was four seconds ago, but now it's not.

Leo: It forgot.

Steve: Yeah, it forgot. So it logged them, and it's really not an attack. So relax, Brandon. I'm glad that your bad habits of password strength have been cured. I'm sure you're going to be okay behind your router.

Leo: My bad habits of not locking down my systems have been cured. And I, by the way, I really did go with strong passwords this time around. Once you use something like LastPass, you can have it generate really good passwords that are not memorable, and remember them. And so all you need is a really good password for LastPass. And that you have to remember, of course. I didn't for a while. I changed this all at about 2:00 in the morning when I woke up freaked out, oh my god, there's passwords on there. Not a good feeling.

Question #9, Robert Hickman in Bristol, U.K. suggests a possible solution to the SSL trust problem we talked about last week. In Episode 243 of Security Now! you discussed the problem with the number of signing authorities that are trusted by modern browsers. As you described, when an SSL connection is established, the server sends a cert to the browser, which checks to make sure it's been signed by the signing authority that it knows about. If the connection were being proxied using the signed intermediate cert, the cert returned to the browser would be different and probably signed by a different authority from the one that's signing the website's genuine cert.

Using this knowledge, wouldn't it be possible for a browser and/or browser add-on to

maintain a database of URL or IP addresses with the original signing authority for most sensitive websites like your bank and large eCommerce sites and so forth, your email system like Gmail? Using such a database it would be possible to detect if the signing authority that a website is using changes, and thus perhaps a man-in-the-middle attack. Obviously this would not be a perfect solution by any means due to the vast number of websites and the introduction of an additional trusted party, though it would offer a workaround to the problem. Thanks for the excellent podcast.

You know, this reminds me, we were talking about Opera Mini. Opera Mini does exactly this because it caches sites so that it can squeeze graphics down and speed things up. And so in fact it breaks SSL. It'll provide you, when you use Opera Mini, with a certificate from Opera, not a certificate from your visiting site.

Steve: So it'll even cache SSL connections.

Leo: I believe it does that, yes.

Steve: Yeah. Okay. And so anyone using Opera Mini would need to be aware that essentially you're completely trusting the people running that caching/compressing server, or proxy, with all of your most private and personal details.

Leo: That's my understanding. And I would love to be corrected on that. But that's my understanding. And I remember when this became an issue, and people said, well, you probably shouldn't use Opera Mini for banking and things that you really wanted to have secure.

Steve: I remember that, too, as a matter of fact. So to Robert's point, I didn't talk about an aspect of this paper which we talked about last week that involved the paper authors' creation of a technology to detect when this was going on. I didn't talk about it because I wasn't really impressed by the strength of their approach. They really designed it with an eye toward not having it false positive, meaning not having it alarm people when it shouldn't, because they recognized that would be a really bad problem if it was going off when it shouldn't. And as a consequence of their deliberately conservative design, it was easy to see that it could miss very big opportunities for exploit. It's worth mentioning, though, I mean, in this context.

There are, for Firefox, a collection of existing add-ons that tackle exactly this problem in different ways. For example, one solution would be that - and there's an add-on for that, as they say. If you first go to a site, and you've never been there before, the browser will cache or hash the remote website's certificate and/or certificate chain. If there's more than just a root authority that signed the website certificate, it'll cache the whole chain. And every time you go back, it will make sure nothing changed.

Well, that's clever. I mean, it means that, because we know nothing should change, unless a certificate expires and is renewed, and that only happens every couple years. So it says, if I go to a site that I've been to before, then make sure that the chain of trust for the website certificate is the same as it was last time because that ought to be relatively static. So there is a Firefox add-on that does that. Of course, it doesn't protect you if the first time you go to a site that's being intercepted, it's a rogue interception,

and so you're getting the cert for the first time.

But there's a solution for that. There's a different add-on which uses an array of probes around the Internet to check the certs that the website returns to them, the idea being that your connection to the malicious site may be hacked, but different means of getting to the same remote server would not be intercepted in the same way. And so it's a way of sort of getting multiple attacks or multiple angles of approach to a remote server and seeing if they're all the same because they certainly should be. If any of them differed, then there's a cause for concern. And there's even another add-on that caches, as far as it knows, valid certificate chains. And this add-on will just check with that to make sure that this sort of a centralized authority of these are all the certificates that we know about from valid servers, make sure this is the same.

So it's clear that the notion of this problem has been explored before. These are, you know, possible solutions. I'm not particularly moved by them because, I mean, I think the problem is we have a fundamental problem with needing to trust the veracity of the chain that has signed the website. And I guess these are better than nothing. But I wouldn't want to generate a false sense of security from them.

Leo: Yeah.

Steve: But I absolutely wanted to acknowledge all the people that wrote, and just other things that I had run across during my research, that there were various sorts of sort of semi-workable solutions. I didn't write them down or log them or chronicle them. I'm sure if you put in "Firefox certificate checker" or just certificate something into your Firefox plug-ins search, it will find those because it would all be about certificate chains. And some users may want to add that to Firefox.

Leo: Our last question, Steve, from Joe Lyo in Lehi, Utah. He wonders about corporate CAs, corporate certificate authorities. How does one know if they have corporate CAs? Can these be removed by a user? I guess he means like from his own company; right?

Steve: Right.

Leo: Will the browser still work if they're removed? What if one browser, Internet Explorer for instance, has the corporate CA; but another browser, Firefox for instance, does not have the corporate CA? Does that mean that Firefox would not be snoopable by the corporate IT department? Help me make sense of this.

Steve: Okay. This is actually exactly like what we just described with Opera Mini. Opera Mini, as you were saying, would carry a certificate recognizing the Opera Mini proxy as a CA, allowing the Opera Mini proxy to, on the fly, create certificates that the Opera Mini browser will acknowledge. It turns out that Microsoft really, I don't even know why, but there is a facility in Windows that allows corporate IT to remotely install certificate authorities in the clients within the corporate network. So this facility that Joe is worried about, I mean, sort of exists by policy in Windows.

The way to know is simple, though, and it is simply by looking carefully at the certificate

chain. Go to any secure website from within your company. Go to https://mail.google.com to establish a secure connection to Google, or https://amazon.com. Just get a secured connection to something outside your company. And then do whatever it is your particular browser has you do to look at, to inspect the page's certificate. Sometimes you can just right-click on the page itself and check properties of the page, or double-click on the little lock icon down in the tray. What that will show you is what we've been talking about, the so-called "chain of trust."

And be worried if it doesn't make it very clear that it's directly trusted by, like, VeriSign, for example. Either it'll be trusted only by VeriSign, or it'll be trusted, it'll say, like, VeriSign Trust Authority, maybe like in a second step. But if there's anything else in line, if it says, for example, Ajax Plumbing Works is an intermediate CA, then that demonstrates that there has been, essentially, that there is an intermediate certificate authority in line. And it will - it may well be your own company that has created the certificate.

There are now many appliances on the 'Net meant for corporate IT installation which require that their certificates be trusted by the clients. We know that IE provides, I mean, Microsoft provides a mechanism for silently installing certificates into Windows. I mean, we talked about this mechanism also where Microsoft itself has this 260-some-plus authorized CAs that are delivered to your machine sort of on a demand basis.

But anyway, the answer is you can inspect the chain of trust in order to see if anything looks at all suspicious in there. And also he asked about what if one browser had it and another one didn't. Well, it's a perfect example. Firefox, if he were to install Firefox, when freshly installed, if Firefox was unable to surf out of the corporate network, then that would be another indication that something was blocking secure connections. What would be very likely is that browsers would, for example, IE, if your corporate network was using IE, and you were able to surf securely with IE, it might be that the corporate firewall would deliberately block any attempts at direct connections, forcing you to use the corporate proxy and its own signed certificate. In which case, a browser that did not have, that was not configured appropriately for use inside the corporate network, might not be able to get out at all.

And so, for example, installing Firefox or some third-party browser, if you found that you couldn't get to https://amazon.com, then there's another indication that you're in an environment which has been locked down and is preventing any sort of, I mean, true secure connection outside. They're very likely proxying SSL, meaning decrypting it and performing some sort of traffic analysis or filtering or inspection. I mean, maybe all for good reason. It would keep malware and viruses from getting into the corporate network over an SSL connection, which could otherwise not be filtered. But again, it does mean that you do not have an un- well, it means that there's a man in the middle that may be on your side, but he is in the middle, able to look at your traffic.

Leo: Just to clarify on the Opera issue, I went to the Opera website. And this is in their FAQ for Opera Mini. Is there any end-to-end security between my handset and, for example, PayPal.com or my bank? No. If you need full end-to-end encryption, you should use a full web browser such as Opera Mobile. Opera Mini uses a transcoder server to translate HTML, CSS, and JavaScript into a more compact form. It's a proprietary form that Opera uses, Opera Mini uses. It'll also shrink any images to fit the screen of your handset. This translation step makes Opera Mini fast and small, cheap to use. To be able to do this transcription, Opera Mini server needs to have access to the unencrypted version of the web page. Therefore no end-to-end

encryption between the client and the remote web server is possible. So there you go. Just so you know. And that's from Opera's own page, so. Steve, another great 10 questions. Well done. Bravo. Thank you.

Steve: And a nice hour-and-a-half podcast.

Leo: I like it. Steve Gibson is the man in charge at GRC.com. You can go there to use ShieldsUP!, absolutely.

Steve: Now that it's back up and running.

Leo: Now that it's running. Also a lot of other great software, including Wizmo, DCOMbobulator, Don't Shoot The Messenger - actually it is Shoot The Messenger. Do Shoot The Messenger. And many other really great programs. But don't forget the most important one, Steve's bread and butter, SpinRite, the world's best hard drive maintenance and recovery utility, a must-have if you've got a hard drive. Steve does also put 16KB versions of the show up there, transcripts so you can read along as you listen, and full show notes, GRC.com. If you want to get a question in the next question-and-answer episode, which is two episodes hence, you can leave a question at GRC.com/feedback.

Steve: Yes, and please do. That's where we get the questions for our even-numbered podcasts every week. So we want to hear back from you.

Leo: We do do this in video, live every Wednesday afternoon at 2:00 p.m. Eastern, 11:00 a.m. Pacific, which is 1800 UTC. You can watch that at live.twit.tv or watch the video. You can download the video and audio from iTunes and all the other podcast places. Just search for TWiT or Security Now!. We do have video versions available of the show now, I believe. Also we'll be on YouTube at YouTube.com/twit in the Security Now! channel. So video as well as audio of this podcast now available for download as a podcast or for streaming. And all of that's at TWiT.tv/sn for more information. Steve, thanks a lot. We'll see you next time on Security Now!.

Steve: Thanks, Leo.

Copyright (c) 2006 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/