SECURITY NOW!

Transcript of Episode #488

The (In)Security of 2014

Description: For our last show of 2014, we first catch up on two very busy holiday weeks of security craziness; then we step back to review the major events of this past very busy and security event-filled year.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-488.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-488-lq.mp3

SHOW TEASE: It's time for Security Now!. Hey, Steve Gibson's here in-studio with me. It's going to make it a lot of fun as we go through all of the bad stuff that happened in 2014. And Steve will tell us what we should do to make 2015 a better year. Stay tuned. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 488, recorded December 30th, 2014: The (In)Security of 2014.

It's time for Security Now!. And this is a little disorienting to me because normally Steve Gibson...

Steve Gibson: That's my hand on your shoulder.

Leo: ...can't touch me. But this time he can. He's actually up visiting because we're going to do our New Year's Eve party tomorrow.

Steve: You betcha.

Leo: And Steve wanted to actually - is it tomorrow? Yeah, it's tomorrow, barely.

Steve: Starts for you at 4:00 a.m.?

Leo: Starts in 12 hours, 13 hours? Yeah.

Steve: Yikes. And I'm getting up at 6:00 for breakfast.

Leo: You're going to make breakfast? Last year you made coffee.

Steve: I don't think I'm making it. I can make coffee. I've got coffee nailed. Breakfast, uh, not so much.

Leo: It's so great. I'm trying to think. We've only done a handful of Security Nows in-studio. We did a couple - you've been in my office, I know, once.

Steve: A couple times.

Leo: And then in Toronto we did it a few times.

Steve: Oh, well, that's where we began all this.

Leo: Right.

Steve: Yeah.

Leo: So when I was...

Steve: In hotels, remember? When I'd be coming up, we would do a recording the night before.

Leo: I remember doing one at the Drake Hotel in my room with - Amber was there, I think. I was lying on the ground. Maybe that was another time. Maybe that wasn't Security Now!.

Steve: I remember wandering around Toronto.

Leo: And once - one we did on the roof.

Steve: Yup.

Leo: Of the Drake Hotel, yeah.

Steve: And I used to bring up the Heil mics, and we'd set up a whole little, like, mini studio. You had a recorder.

Leo: Did you really? Wow. Wow.

Steve: Yeah. With an SD card.

Leo: It's nice, it's so nice to have you in-studio. Steve and I have known each other for probably 15 years.

Steve: Yeah.

Leo: And share a love of good cabernets and an interest in security. And each week we talk about security. This is a live show. We did, last week, we did an interesting - we always do a holiday special.

Steve: Right.

Leo: And we used your lecture on SQRL.

Steve: Right, which I gave in Las Vegas on November 7th. DigiCert hosted a security summit, their first security summit. Which they just did a great job with, really interesting stuff. And so our podcast watchers and listeners had a chance...

Leo: They've known about SQRL for a while. But this was really finally hearing the details.

Steve: Yes. And I did say two weeks ago that I would be demoing it today. Anyone who can see the screens know that I'm not demoing it today.

Leo: Why not?

Steve: I actually have it running. It is working, but not public.

Leo: Okay.

Steve: Because when I - I got the implementation finished. And I'm a big believer, which is why I generally take my time, that first impressions matter. And there are a couple, when I saw it running, I realized, oh, there are a couple things that I'm not exactly comfortable with the way it works. And so it's like, hey, there's no hurry.

Leo: There is no hurry.

Steve: I mean, it's all I've done for a year. This is what I've been on for a year.

Leo: And for those who just kind of - the elevator pitch on this is it's an authentication, a website login process that does not involve passwords.

Steve: I think what we will show, what we will see, is it is a practical, and that's the key, I mean, it's a practical replacement for usernames and passwords.

Leo: Love it.

Steve: It can live alongside them. And in fact that's one of the things that delayed me was I initially had just - my demo was just using SQRL to log in, to sort of - I sort of, like, created a fake login-ness on GRC because nothing else on GRC logs in. And then I thought, wait a minute, people are going to say, well, that's fine, but how's that ever going to get adopted? So what I needed was to duplicate a normal login session that you'd have, like on Amazon, where you still have username and password, or SQRL.

Leo: Or SQRL.

Steve: Yes. And so what I've done is I reimplemented that, and I have now you can log in with username and password. You can log in just with SQRL. You could initially have a username and password account, like everyone does now, associate your SQRL identity with it, then remove your username so that you're able to sort of straddle over into a SQRL-only authentication. And when you remove your username and password, then there's nothing for the website to steal.

Leo: This is clearly an idea whose time has come. Passwords are really frustrating. They're driving people crazy. They're a security flaw in some cases. They're certainly an annoyance in all cases. We did an interview yesterday on Triangulation with a New York Times reporter, Ian Urbina, who did a really great piece in November on the secret life of passwords and how people come up with their kind of standard password. It was fascinating.

But one of the things he said at the end, and I think this is true, is that he hopes that our kids will not be using passwords; that this is a brief - our grandparents didn't have passwords, and our kids won't have. But this is a brief period of time when passwords, everybody has to have passwords. And we pretty clearly see how bad they are.

Steve: Well, and it's interesting, too, because it's a place where there's been no innovation. Remember the way this all began, back on mainframes, where you'd have some Hazeltine terminal. That's what - that's the way...

Leo: That's how you'd log in.

Steve: ...you would log in. And so then we went to UNIX, and we got networks. And that same, you know, who-are-you-and-prove-it model, we're still with now, decades later. So there's just been no - there's been no progress.

Leo: Key to your success with SQRL will be getting websites to adopt it.

Steve: Yes. And that's why one of the cool things about this is that there is, for a website to adopt it, it's one API call. All you do is you need to verify the signature of - the signature that the site sent you just needs to be checked. So, and in fact I just got email from someone who's got it completely running in Drupal, like, nailed.

Leo: Nice, nice.

Steve: And there are PHP implementations. It's now available in the Android Store, and there's one for iOS on the way. So first off, obviously, we need clients, where...

Leo: Ah, interesting. So I'd have to have an app on my phone.

Steve: Yes, yeah. And you can use the app on your phone to take a picture of the QR code, and then it authenticates sort of like behind the scenes. The neat thing about this is, when you see it actually work, it's like, wait.

Leo: That's all?

Steve: That's it?

Leo: That's all I have to do?

Steve: I mean, I'm...

Leo: It's like Apple Pay. I'm done?

Steve: Well, exactly. So...

Leo: It's very similar, in fact.

Steve: So my belief is there are sites where there is a low tolerance for logging in, like blogging. How many times have we read someone's blog and thought, oh, I'd like to make a comment.

Leo: Yeah, but I don't want to have to log in.

Steve: Exactly. And then they want to make you create an account.

Leo: Right.

Steve: So those sites...

Leo: Or they use social logins like Google and Facebook, and we're giving information now to Google and Facebook.

Steve: Right, exactly. So this allows you to create an identity sort of on the fly with zero pressure. And I think once people see that, they'll start saying, hey, I'd like to have that elsewhere.

Leo: I think that's the key. Once users adopt, then the sites are going to have to...

Steve: And as you said, now is the time.

Leo: So we had a host dinner last night, which was a lot of fun. I posted pictures on my Flickr page, Leoville, and on my Facebook. But it was so much fun. And of course I'm standing next to Steve as people come in. And everybody said to you: "So? Did North Korea do it?" It was the question of the night. So, did North Korea do it?

Steve: Okay. So what we're going to do, since I'm not demoing SQRL quite yet, a week or two, is I want to - and here we are at the last, next to the last day, New Year's Eve eve. I want to do sort of a walk back through what happened in 2014 because, boy, I mean, talk about a crazy year.

Leo: But is this the worst year for hacking?

Steve: I think it is.

Leo: I think it might be.

Steve: I think, I mean, there's never been anything as devastating as the Sony hack that just happened here at the end.

Leo: And the Target, and the Home Depot, and you can go on and on.

Steve: Yes, yeah.

Leo: Lots of breaches this year.

Steve: I think, I mean...

Leo: It was the Year of the Breach.

Steve: It was a bad - it was a bad year. And what's interesting is, those of us who are as close to this as you and I are have sort of been expecting this. It's sort of like the way viruses have been around forever, and they could have been a lot more evil than they turned out to be. And we sort of never really understood, well, these viruses could be wiping out people's computers.

Leo: Originally it was vandalism.

Steve: Right.

Leo: It would deface a website or put a funny thing on your computer that you couldn't get rid of. Then it became putting stuff on your computer that would make the bad guy money, things like spam reflectors or DDoS machines.

Steve: Or taking over your machine in order to use it as a...

Leo: To co-opt it, to add it to a bot army. But then with CryptoLocker, and I guess this was the year of CryptoLocker, it suddenly really did become an issue, a real expense.

Steve: Right.

Leo: Because you couldn't unlock your data unless you paid them.

Steve: What I think we're really seeing is, as they say, the chickens coming home to roost. These are problems that are latent in our architectures. And, I mean, there were obscure things, like SSL bugs, and we'll talk about those here in a minute. But there were also just larger problems, like the problem of securing something the size of Sony Entertainment. It's just - you can't. I said a couple weeks ago when we were talking about it, you said to me, "What would you do, Steve?" And I said, "I couldn't secure something that size that has humans involved like that." I couldn't. Anyway...

Leo: That's the problem. Humans are the problem.

Steve: So we're going to - so this is the Insecurity of 2014. And then but I also want to catch up on - because it's been a busy two weeks. We talked two weeks ago, and oh my lord, stuff has happened. So we know that during his last press conference of the year, Barack stood up in front of the world and said that North Korea hacked Sony, and he wished that Sony had called him prior to making the decision not to air the movie. Now, having seen the first 20 minutes, which is all I could tolerate...

Leo: You downloaded it? Or did you - yeah.

Steve: Jenny really wanted to sort of thumb her nose...

Leo: At North Korea.

Steve: Yes. And so I paid $6.

Leo: We should - I think at this point it would be prudent to point out that buying or seeing the movie in no way is striking a blow for freedom. But okay, go ahead.

Steve: No. No.

Leo: Just so you don't have to.

Steve: I'm so embarrassed now that - oh. You'll know...

Leo: It's that bad?

Steve: It is beyond bad. I mean, it is so adolescent that, I mean, and comedy...

Leo: You've not seen a James Franco/Seth Rogen movie before. You haven't seen "Pineapple Express" or "This Is the End" of the world or - you've not seen these movies.

Steve: No.

Leo: So you didn't really know what to expect.

Steve: No.

Leo: Those of us who've seen them maybe are a little more inoculated than you were.

Steve: How old is your son?

Leo: He's 20. He loves this stuff.

Steve: Oh, he's way too old for this.

Leo: It's like 12-year-old humor.

Steve: Oh, it is, potty humor. I mean, and not just a minute of it, but four minutes...

Leo: Endless minutes.

Steve: Endless. It's just unbelievable. Anyway, so the consensus among security experts is that - getting back to the topic. We're having a ball. This is great. The consensus among security experts is that the evidence for North Korea being behind the hack is weak and weakening. That is, I mean, and yes, it's hard to understand how the President of the United States could assert that the FBI has asserted to him that they have sufficient evidence to draw the conclusion - oh, but they're not going to share it all with us - if it weren't true. But, for example...

Leo: Well, that's the, I mean, both Bruce Schneier, and you're going to talk about Marc Rogers of CloudFlare, have kind of said what we know isn't conclusive. But the FBI and the President also said there is information we cannot reveal, presumably signals intelligence, or maybe even pure espionage intelligence, that revealing that information would reveal the source and thereby make the source useless. So the presumption is that for them to be so unequivocal, maybe there must - there must be something, a signals or something that's conclusive.

Steve: Yeah, because it would be really bad if it came out that they were...

Leo: We happen to be able to tap into Kim Jong-un's phone or something. Yeah, yeah.

Steve: Right, or - exactly.

Leo: Which we probably are. And he probably said, oh, wasn't that funny when we hacked Sony. But maybe not. And this is the thing. We live in an era, after many attacks on credibility in the federal government, we live in an era when nobody believes the federal government. Nobody is - maybe if Dwight Eisenhower had said, "No, trust me, we know they did it," we'd believe it. But nowadays, nobody believes it. It's just not enough to assert, well, we have information. It's just like saying we know about WMDs in Iraq. It's just not credible.

Steve: So Marc Rogers - oh, thanks.

Leo: Thank you for that. Go ahead. We'll just edit that out.

Steve: Marc Rogers, knowing who's...

Leo: This is the CloudFlare guy; right? He's chief security researcher for CloudFlare.

Steve: Chief security guy for CloudFlare. He's also head of security for Defcon.

Leo: He runs Defcon.

Steve: Exactly. So, I mean, knows his stuff. So he points out that some of the evidence that we were given were the IP addresses that were used. Well, it turns out they're public proxies. Everybody uses them. They're well-known ways of bouncing your traffic through another server in order specifically to throw someone off the scent.

Leo: Right. They're in the U.S. They're in Thailand. They're in Italy. They're in Poland. They're all over the world.

Steve: Yeah, Bolivia, Singapore.

Leo: So the use of those is not in any way conclusive. And in fact this does kind of make people think, well, maybe the FBI doesn't know what the hell it's talking about, that they would cite this as evidence.

Steve: Yeah. I think it's just always - it's always difficult for someone to say, oh, I know it, but I can't tell you how. You know?

Leo: Yeah. And the evidence that they provided was really not conclusive.

Steve: Right. So Marc observed what others have observed, which is, for example, first of all, is the fact that the attackers only brought up the anti-North Korean bias of "The Interview" after the media did.

Leo: Right.

Steve: It was never part of their original presentation.

Leo: Weren't the first communications they had requests for money from Sony?

Steve: Yes. Yeah. Like the day before or two days before the first drop of data, they said pay us. Now, it was always in fragmentary English. I remember seeing the wording of that. And they didn't even give a dollar amount, or at least it wasn't disclosed. So I don't know whether in fact they did. But it seemed like just simple extortion from somebody on the inside.

Leo: Now, I might mention that, if you are the North Korean government, and you're going to perpetrate some cyber warfare scheme, that it would be smart to obfuscate it with oddball requests in poor English.

Steve: Well, yes. And of course the flipside argument works, too. And that is, wouldn't the hackers love the cover story of it being North Korea? Because we're not going to attack North Korea. Well, or if we do, we're not going to talk about how and when and what our methods are and so forth.

Leo: It will be a proportionate response.

Steve: But the idea is it deflects the FBI, apparently, from the trail, given that they really believe that. Also he noted, Marc noted, that the hackers dumped the data. And he asks in his Daily Beast story, would a state with a keen understanding of the power of propaganda, such as North Korea has, be so willing to just throw away such a trove of information? He said the mass dump suggests that, whoever did this, their primary motivation was to embarrass Sony Pictures.

Leo: Mission accomplished, by the way.

Steve: Well, yeah. And his theory is, again, the Occam's Razor argument. What is the simplest explanation? The simplest explanation is an annoyed employee at Sony, somebody who was on the inside who had this kind of access was able to put this together.

Leo: And there is actually evidence that they had inside information. Server names and passwords were hardcoded into the malware. So that would be information only known by somebody inside Sony.

Steve: Well, or somebody - the APT, the Advanced Persistent Threat model that we're now having to grapple with is where somebody gets into your network, burrows in, and now sits and watches for some length of time.

Leo: Right. And in fact there's evidence that that had happened, that in March Sony was compromised.

Steve: Right.

Leo: And ignored it.

Steve: Right, exactly, months before. So maybe somebody was there. Now, if you had that kind of presence in the network, they could gather data for six months.

Leo: And write some specific code and take advantage of that information.

Steve: Exactly. I mean, so...

Leo: So that's inconclusive, as well.

Steve: And so I think one of the things - and we've talked about this, and we've seen me, I was late to the party to believe about Stuxnet being what it was. I'm willing to say I don't know. I don't have the answer.

Leo: Okay. But the thing that comes up when we say all this - and I agree with you. It didn't smell right. But I don't understand what's in it for the President and the FBI in asserting, I mean, this is, you know, for a nation to assert that another nation has attacked it over the Internet is a fairly significant thing.

Steve: Well, attacked one of our companies, though.

Leo: Okay. And a Japanese company, to boot.

Steve: Right.

Leo: But that's a fairly strong thing to say. What's in it for them? Why would they assert that if the evidence wasn't conclusive? What would their...

Steve: I think just political pressure to have an answer. We're supposed to be able to know.

Leo: We should know.

Steve: Yeah. I mean...

Leo: The risk, though...

Steve: ...imagine him standing up there and saying, well, I don't know.

Leo: Well, or there are ways to couch it. It wouldn't be prudent to talk about this yet where the investigation is ongoing.

Steve: Yeah, true. And besides, I'm on my way to...

Leo: And I've got to get out of here. So thanks. See ya. But also the issue is, if it does, if evidence does surface that it wasn't, that's highly embarrassing.

Steve: Right.

Leo: So it's a dumb thing to assert that, oh, we know it was North Korea, unless, it seems to me, that they knew it was North Korea. So this is why I'm puzzled. You know what's the truth? We probably - we'll likely never know what happened.

Steve: I don't think we will. And that's one of the problems with network-based attacks. Unlike physical world attacks, where you leave some blood because you cut yourself on the jagged edge of the glass when you went through the window...

Leo: Right, there's evidence.

Steve: ...or fingerprints or skin flakes or whatever, electronic attacks just don't have any of that.

Leo: And one thing that you learn in security is that attribution is always very difficult because of these proxies, because of log erasures and things like that.

Steve: Yeah, and all of the things that we're used to now being standard mechanisms in movies, I mean, they're a little overdone. "Well, they bounced around the world seven times, Captain, before they..."

Leo: But they did. And in fact we even know the proxies they used.

Steve: Yeah, yeah.

Leo: All right. So, and in fact, in the past when hackers have been prosecuted, almost always it's because they...

Steve: Talked.

Leo: ...boasted; right?

Steve: Yes.

Leo: So it seems unlike - if whoever did this is smart and just shuts up...

Steve: Ooh, and you don't want the hammer to come down on you.

Leo: ...and goes away...

Steve: Not on this one.

Leo: ...that we'll probably not know what happened.

Steve: I think we have to expect that we really won't have an answer.

Leo: And I'm kind of saddened by the assertion from the United States government that it was North Korea because now they're incented not to release any further information. Like, case closed, because anything they released could actually undermine their case.

Steve: There's another obligation now, and that is response. Because the State Department has said, well, we're not going to tell you what we're going to do, or you really won't know when, but we will respond proportionally. I mean, Barack did say that we're...

Leo: I think, though, that that was more to say we're not going to bomb them.

Steve: Right, right.

Leo: And he was very careful, and I think this is the right thing to do.

Steve: No mushroom clouds.

Leo: Say this is not a terrorist act.

Steve: Right.

Leo: Don't want to use the "T" word.

Steve: What he called it, he called it "vandalism."

Leo: Vandalism. And I think when he said "proportionate," he didn't mean we're going to respond strongly. I think he meant to say we are not going to bomb them.

Steve: I hope...

Leo: That would be disproportionate.

Steve: I hope this was not our denial of service attack.

Leo: By the way, was that the response? Because on December 22nd North Korea went offline.

Steve: Yeah. Shortly after Barack's last press conference of the year, as he heads off for Christmas vacation, that Friday evening, connectivity to North Korea started getting flaky. And it sort of slowly degraded over the course of the weekend until Monday morning it was pretty much gone.

Leo: Right.

Steve: Now, if that's like a denial of service attack that the U.S. mounts...

Leo: We could do better?

Steve: ...they need to call me.

Leo: How much Internet does North Korea have? They don't have much; right?

Steve: Oh, my god.

Leo: And it all goes through China Unicom.

Steve: Most city blocks in New York have more IP addresses than North Korea.

Leo: Wow.

Steve: Than the entire country. North Korea has officially 1,024 IP addresses.

Leo: That's it?

Steve: They have 10 bits of IP space.

Leo: And it all goes through China.

Steve: Yes. And so that's actually one argument for us not having attacked North Korea, because if that was, our attack would have been carried by China's telecom services.

Leo: By the way, I don't think that's something we would want to do at this point.

Steve: Precisely.

Leo: So it sounds like, and it does, the way - the sputtering and its getting stronger, it sounds like just some kid, script kiddie.

Steve: Uncoordinated, like, oh, let's get them back.

Leo: Yeah.

Steve: On the other hand, even that, I mean, DDoSes these days knock gigabits...

Leo: Trivial. It wasn't even a good DDoS.

Steve: It wasn't. It was hard to explain it. So anyway.

Leo: It's like - somebody in the chatroom said it's like DDoSing my apartment building. It's not so hard to accomplish.

Steve: Right. Anyway, so also there was something that went on with North Korea, and we don't know what that was, either. But it sure was not impressive. I saw charts of the outages, and it would kind of come and go, and then kind of go more, then come back, and then go more even. It was just like, what?

Leo: I get the distinct impression that the government made the announcement about North Korea right before Christmas and the holidays and is just hoping everybody will forget about it by the New Year.

Steve: A perfect example is, as we know, on Christmas Day, eve and day, Xbox live...

Leo: They were brought down.

Steve: And PlayStation Network.

Leo: By Lizard Squad.

Steve: Well, okay.

Leo: Who the hell are they?

Steve: So there are serious strong networks taken off. So if Lizard Squad aimed themselves at North Korea, there'd just be a - it'd be dust over there right now.

Leo: There was an interview with Lizard Squad. In fact, they showed one of the guys.

Steve: It's like, what are you doing?

Leo: Again, this is how you get caught, folks. Actually, we shouldn't say anything. It's a good idea, you know, you should give an interview when you hack something. Let the world know what you've done.

Steve: Yes, please do. That's right.

Leo: But in this case you saw a picture of the guy, and he said, you know, "We just did it for fun." And he said, "You should go out and get some fresh air. You shouldn't be playing games on Christmas anyway."

Steve: And then they sort of - they, like, again, sort of because they didn't really know why they were doing it, they changed their story, and they said, oh, we're trying to teach

Microsoft and Sony a lesson.

Leo: Oh, please.

Steve: We want them to improve their security.

Leo: Yeah, yeah, yeah.

Steve: Except that a DDoS isn't about security.

Leo: Right.

Steve: And I don't - I thought, well, do you not know the right word?

Leo: Oh, it's BS. It's just BS.

Steve: Yeah. And so, and get this.

Leo: They're script kiddies.

Steve: The way they finally stopped was that Kim Dotcom gave them vouchers for his Mega.

Leo: Here, have some free storage.

Steve: Yeah. And they said, oh, thank you.

Leo: Oh, thanks. We'll take that.

Steve: They tweeted, "Thank you, and we'll stop now."

Leo: Morons. I'm just really - they say in the interview they could take down NASDAQ if they wanted to.

Steve: Right.

Leo: The over-the-counter stock exchange.

Steve: But that's not very interesting, yeah.

Leo: But we just like - we're having some fun. But that is scary, it is scary that these things, these people exist, and they have the ability to do something like that that really is so damaging to so many people. It feels wrong.

Steve: And it's not going to get better. What we have to understand is that this is old technology. This is a SYN flood where...

Leo: Is that how they did it? You've been SYN flooded.

Steve: Oh, my goodness.

Leo: You've actually - and this was five years ago; right?

Steve: Yeah. I used to just, it's like, okay, here we go again.

Leo: And it's hard to block. The only way to really prevent it is add bandwidth; right? Because you can't have a public website that ignores SYN requests.

Steve: Right. You need a monster proxy like CloudFlare.

Leo: That's what they do.

Steve: That's one of the services. CloudFlare sits in front of your website and is able to terminate the connections so that a SYN comes in, and they'll send back the SYN ACK. Your server doesn't see it until the connection is completed.

Leo: And then passes it along.

Steve: Then, yes, and they're also a caching proxy. So your site, even when there's a big load, sees only one request, and then they store it locally.

Leo: It's very hard and not economically feasible to design a server that has enough bandwidth to handle all of these requests.

Steve: It's not even the server. Because if the pipe...

Leo: The pipe.

Steve: The pipe to the server, if that congests, then your server is starved.

Leo: You don't even see these SYNs.

Steve: Yeah, I mean, I just had a couple T1s back then, and it was like it was trivial to knock me off the 'Net.

Leo: So, and of course now with amplification attacks using NNTP and other technologies, it's possible for a single person to get enough bandwidth to attack even the fattest pipe.

Steve: True. So any denial of service attack is a violation of the underlying protocol. That is, no one should be sending out SYN packets over and over and over.

Leo: Basically it's knocking on the door of the website and not caring what happens. The website has to respond because it doesn't know if it's legitimate or not?

Steve: Well, and what's interesting is that there is a network somewhere that is allowing those out.

Leo: Outbound SYNs.

Steve: Yes. The egress filtering is really what we need.

Leo: We've said this before, that if ISPs were all responsible, this wouldn't be a problem.

Steve: Right. And notice that these are spoofed SYNs. So the SYNs that are going out carry an IP address...

Leo: That doesn't match the ISP.

Steve: Exactly.

Leo: Yeah.

Steve: And so they could say don't allow any packets out that aren't...

Leo: From our network.

Steve: ...from our network. And it would stop it immediately.

Leo: Yeah.

Steve: So I think, unfortunately, this is going to have to get bad enough that...

Leo: Isn't it bad enough yet?

Steve: It's just...

Leo: Nobody could play Xbox or PlayStation games on Christmas Day.

Steve: You know, the analogy that occurs to me is like the crumbling U.S. infrastructure. We have, like, sink holes in L.A. with huge floods when a pipe breaks. And it's like, oh, my god. And so we fix the pipe. And then it happens down the street. Oh, my god. And we fix that one. And so no one fixes the infrastructure. We just keep patching the problems. And unfortunately this is like that. It's spotty. I don't know if it's ever going to get bad enough.

Leo: So we talked before about the amplification attack using the time server, NNTP.

Steve: Yes.

Leo: Is that what Apple patched, do you know?

Steve: No, they didn't.

Leo: It was an NTP flaw. The DHS, actually, Department of Homeland Security, put out a bulletin.

Steve: Yes, yes. It was, okay, and it was bad. And that was why, for the first time ever, Apple forced an update.

Leo: Their auto patch.

Steve: Yes. Normally...

Leo: They put that technology in two years ago, but have yet to use it.

Steve: Actually, they...

Leo: Did they use it before?

Steve: They used it for some malware.

Leo: Oh, okay.

Steve: Some malware signatures.

Leo: Right, I remember that, yeah.

Steve: They have pushed out that way, where it just does it. You don't have to ask for it or okay it or approve it or anything because this is a remote code execution buffer overflow in a service which is running by default.

Leo: The time protocol.

Steve: Oh, baby. I mean, that string of words I just said is the worst...

Leo: Scary.

Steve: Is the worst there is.

Leo: So you're saying every Mac has an NTP daemon running at all times.

Steve: Yes, yes.

Leo: And that this NTP daemon could be overflowed, which means malicious code - did they actually have a malicious code exploit? Or is it just - it was a crash?

Steve: No, no. It has not been seen in the wild.

Leo: Okay.

Steve: So the people looking at the code went, "Holy crap. We have to patch." I mean, this was like one of those bad events.

Leo: You find the overflow, and then the hackers start working to see how they can jump to an area of memory and...

Steve: And there's no doubt they're trying to do it now.

Leo: Eventually they would be able to execute code.

Steve: Well, because, for example - okay. So an NTP server, Network Time Protocol, you're able to ask it what the time is.

Leo: Right. That's how your clock gets set on your Mac and Windows machines.

Steve: Exactly. And it's got technology where it asks like the U.S. Naval Research Center somewhere or something in Utah...

Leo: It asks NIST or WWV in Fort Collins.

Steve: Exactly, Fort Collins, Colorado. So the problem is many people offer it as a service. They say, "Oh, I have an NTP server. If anyone wants to know the time, why not tell them?" Well, and that's where these reflection attacks come from is you ask, a tiny request goes in, and a big response comes out. So you spoof the IP of the request, saying that over there he asked me. And so the big answer...

Leo: Yeah, Xbox Live wants to know what time it is.

Steve: Exactly. The big answer goes there. Now, here's the problem. That server has a vulnerability. So that if you ask with a specially crafted packet, that open, exposed, public-responding NTP daemon, you can take it over. And it's typically running as root. You get the privileges of the daemon, and it generally runs as root. So this is a remote code exploit on all Network Time Protocol servers on the Internet. All of them are vulnerable before, what did I say, 4.2.8. So they patched it in 4.2.8. Now, remember, though, before everyone panics, you have to be exposed to the public Internet.

Leo: If you have a router, you're not vulnerable.

Steve: You're not vulnerable. Now, on an Intranet you would still be vulnerable. So if somebody got into your network, and you had an NTP server running like Sony, they got into Sony, and Sony had a server protected from the outside but running NTP, you could, from within the network, use it to gain root access.

Leo: Oh, wow. To all the machines in the network.

Steve: Well, to that server.

Leo: Oh, that server, okay.

Steve: You could run your own code on that server.

Leo: Got it.

Steve: So all of us behind home routers, even those of us who are behind firewalls that don't open a port for NTP access - I think it's port 123? I'm just - that's really from old memory. I don't remember now what NTP protocol is, but I think it's like...

Leo: I can tell you. I'm going to look it up right now. So, for instance, here we have a network, but we're running behind Astaro Firewall. Presumably it's going to block that kind of...

Steve: Presumably you're not offering time services to the Internet.

Leo: No.

Steve: Why would you be? I'm not.

Leo: Wow. So that patch, that's kind of cool that Apple could do that. Do you know, has Microsoft patched it on Windows? Is it an issue on Windows?

Steve: No, because this just happened. And Microsoft is going to stick to their...

Leo: They don't have the same mechanism, do they, for just I'm not going to ask, I'm just going to fix.

Steve: Good question.

Leo: They may, and it may not be publicized.

Steve: I think they always ask you. They do, like, give bonuses sometimes, like extra crypto suites.

Leo: It's a good thing, though, for a true emergency. The problem is sometimes these patches break things.

Steve: Well, and so I think the problem is that apparently Macs are publishing NTP, but Windows doesn't.

Leo: Oh, interesting. All right. So it's not an issue.

Steve: Yeah, so Windows and, again, behind a router, you're...

Leo: Service port is 123, the chatroom confirms.

Steve: Ah, 123.

Leo: And so does the IETF. Okay. Fixed.

Steve: And you can use UDP or TCP, so either protocol.

Leo: How much did Kim Dotcom give them in vouchers, just out of curiosity?

Steve: Didn't see. But I just - I saw...

Leo: "Here's 10 bucks of free storage. Would you knock it off, Lizard Squad?" Okay, okay.

Steve: Well, they were just flattered. It's like, oh, okay. And they tweeted a thank you from Lizard Squad's Twitter account. They said, hey, we got...

Leo: I'm not sure which is worse, that there are people out there who have such moral flaw that they don't kind of connect the suffering they're causing with the fun, the lulz they're having, or that it's even possible to do this because this stuff is so janky. It's all bad.

Steve: And it's the fact that you do have anonymity, to a large degree.

Leo: Right.

Steve: I mean, we know that doors and windows in our homes are not actually secure. You could throw a brick through a window and then climb through it. So it's the fact that you have to physically do that, and you risk being seen, and all the complications.

Leo: Right, right.

Steve: That's what ups the ante for a real-world attack. But you can literally be in your bedroom, on your computer, launching DDoS attacks...

Leo: No risk, really.

Steve: ...to North Korea with your five bots.

Leo: Or seemingly little risk, yeah. There's also - there is a social contract. Locking your door doesn't really prevent somebody from kicking it in or going around the back. But it's a signal. And it's a social contract we all kind of just adhere to. And this is somehow missing in certain people. Of course there is. Of course it is.

Steve: Yeah.

Leo: Now, here's some good news. I was very pleased. The Edward Snowden leaks continue on. We are now in Year 2, Snowden Year 2. And this is the good news. There is stuff the NSA doesn't like, or at least as of 2012 couldn't break.

Steve: Yeah. Der Spiegel carried a story showing some recent documents. They analyzed them, and what we learned was interesting. The NSA ranks the - okay. First of all, the NSA, get this, calls encryption a "threat."

Leo: Yes.

Steve: It's a threat. It's not security. It's a threat. So, okay. So they have a scale, a ranking system of how bad is the threat. So "trivial" is obviously one.

Leo: That means we can crack it, we can read it, it doesn't get in our way at all.

Steve: Well, and they give the example of monitoring a document's path through the Internet.

Leo: No problem. Easy peasy.

Steve: It's like, okay, we know that's trivial. Okay. Trivial is number one. "Minor," a minor threat is like recording Facebook chat.

Leo: Oh, that's not as easy, huh? But minor.

Steve: Not so easy. Yeah, you've got to actually get up off your chair and go push a button somewhere to do that.

Leo: Okay.

Steve: Okay. Number three, "moderate."

Leo: Moderate.

Steve: A moderate threat is, for example, decrypting emails sent through Moscow's Internet mail.ru service. So they're trying to encrypt it, but that's a moderate problem. It doesn't slow them down. They may have to call someone...

Leo: Right. Hey, Ivan, would you flip the switch over there?

Steve: ...like in the next building.

Leo: Yeah.

Steve: Okay. So then the last two are "major" and "catastrophic."

Leo: Now, again, for us, catastrophic is good.

Steve: Yes.

Leo: For them, it's bad.

Steve: It's a catastrophic threat.

Leo: For us it's good. That means we're secure.

Steve: Okay. So a major are all the things they basically can't handle. And like in the documents, TrueCrypt, nothing they can do about TrueCrypt.

Leo: They can't do it. Oh, that's good.

Steve: They're hoping the guy used a weak password because, as we know, that's the only way to crack TrueCrypt. OTR, the Off The Record protocol, the real-time chat protocol, well designed, strong crypto, and unfortunately it is a major threat, Leo.

Leo: I hoped it had been catastrophic.

Steve: It's a major threat. No, no, it's catastrophic if you go through Tor and use Off The Record.

Leo: Oh, then we're really screwed.

Steve: When you mix them up, when you do more than one at once, then it's a catastrophe.

Leo: Didn't we learn that they have kind of infiltrated Tor to a great extent?

Steve: Well, on my list - I keep trying to get to it, but the world won't let us - is we're going to do...

Leo: Some day we're going to talk about it.

Steve: We're going to do, soon, DeTor is the title I've had, and I keep pushing it down in my things I want to get to. Because it turns out that there is - it's less anonymous than we were hoping. That is, and we sort of suspected this.

Leo: Because the endpoints have been co-opted, yeah.

Steve: We've talked about the exit nodes. And if you analyze the traffic well enough - okay, so what the professor said was, who analyzed this, a sufficiently well-motivated entity...

Leo: The NSA.

Steve: ...could deanonymize about 80% of the Tor traffic.

Leo: Okay. That's significant.

Steve: So that's not what anyone wants, yeah.

Leo: But OTR is good. It's interesting they mention Zoho. I don't know why. Zoho is a free office or web-based office solution.

Steve: It must have good crypto.

Leo: That has encrypted email.

Steve: Oh, and I forgot to say that Skype - I hope the NSA is enjoying this podcast.

Leo: Really, which - you're not on Skype, dude.

Steve: That's right. I just realized that that joke doesn't work today.

Leo: So Skype was which? Trivial, minor, moderate? Where was Skype on that scale?

Steve: Trivial, because...

Leo: Trivial. They have a backdoor.

Steve: Well, yes. Microsoft engineered eavesdropping into it in February of 2011.

Leo: Oh, thank you, Microsoft.

Steve: And there's an FISC, FISA something court, like request, that is just sitting there, that allows them to now break into any Skype calls they want.

Leo: And probably, in Microsoft's defense, they probably don't have a choice; right? If you get a FISA Court or a national security letter...

Steve: Although, as far as we understand, it's a blanket eavesdropping capability. And that's what the rest of the industry is still resisting. You know, VPNs don't have it, as far as we know. Google is not doing it. Apple, for example, encrypting the iPhone. I mean, everybody else is resisting this so far.

Leo: Who uses OTR? Does RedPhone use that? Threema, I think, uses it. SecureText uses it. Are those OTRs?

Steve: There was that web-based implementation of OTR. I'm blanking on it. It had a little bit of an implementation problem, but they fixed it.

Leo: This is the Off The Record.

Steve: Cat, something Cat.

Leo: Cryptocat.

Steve: Cryptocat, yeah.

Leo: Used OTR.

Steve: It uses the OTR protocol.

Leo: Okay. So that's good. So look for OTR.

Steve: Yes, it's a good protocol.

Leo: End-to-end encryption.

Steve: Yeah. And, I mean, they didn't mention Threema. It was not - because it's not that this was an exhaustive list. So Threema's technology is solid, too.

Leo: Right. So, good. If you want to - but, now, first of all, this was 2012. So we don't know what's happened in the intervening couple of years.

Steve: Right.

Leo: But to me this felt like good news. What about VPNs? Completely cracked.

Steve: Yes. And what we believe - now, so...

Leo: As has SSL.

Steve: Well, the problem with VPNs is that we know that there are, as with Tor, there are exit nodes. There is the VPN server that you're terminating to. And if that's a public server...

Leo: So you may not be able to get in the tunnel, but...

Steve: They could just set up camp right there. I mean, because we know...

Leo: We know where it's exiting, yeah.

Steve: ...that they're going to have access to the fiber and just tap the fiber in order to get to it.

Leo: Does perfect forward secrecy help with TLS and SSL?

Steve: We believe that the problem there is - the weakness in TLS and SSL is the public key infrastructure because no one doesn't any longer believe...

Leo: Anybody can have a CA.

Steve: Yes.

Leo: And certainly the NSA has a certificate authority.

Steve: There's no way that the NSA isn't trusted. I mean, yeah. If you look through the array of certificate authorities that we have in our secure store now, hundreds of them. And there's just no way that they can't have a certificate minted on demand that allows them to impersonate a website and set up an unseen man-in-the-middle attack.

Leo: So the reason I interpreted this as good news is the message is they don't have a hundred percent view of what's going on. There is some stuff that, at least as far as we know, they cannot see into.

Steve: Math works.

Leo: That's what protects us, math.

Steve: And we have great math. It is implementation vulnerabilities, and there are some architectures which are weak. The architecture of the public key system is weak. And remember, famously, we were doing the podcast when I looked at the list of...

Leo: The Hong Kong Post Office, baby.

Steve: ...the certificate authorities, it's like, there used to be 12. Now there's 400. And we're trusting every single one of them.

Leo: Right.

Steve: Yeah. So, okay. So what I think, and I'm sort of stepping on our conclusion here, but it fits right now, and that is the upshot of this first year of Snowden is today, as we wrap up 2014, security has gotten better. I mean, the response to the now one-year-old

Snowden leaks has been Apple saying, okay, we're going to make security a feature, and we're going to, I mean, absolutely do it. And of course they've been criticized, by the people who consider security a threat, for, like, selling security. And it's like, no. I mean, they've been accused of, like, selling access to molesters and pornographers and bad people. It's like, no. We just want to allow people to have the security that they're expecting from the product.

And of course Google is following suit. And, my god, you can't even count the secure messaging protocols and phone apps and all of the Internet communication security that has ramped up, seeing that as a market opportunity in the wake of Snowden's revelations that showed us how much interest there really was in dealing with the threat of encryption.

Leo: So Steve Gibson is in-studio, which is really nice. He came up from his Fortress of Solitude in Irvine.

Steve: Really does change the dynamic.

Leo: Yeah. I actually talk to you, for one thing. And it's great because tomorrow is New Year's Eve, and we're going to do the big party, and you're going to be part of that. But I think this is a good thing for our last Security Now! of 2014, to do the chronology. The things that happened. A look back.

Steve: Yeah, just sort of like, if nothing else, it's been a fun year. But there was a lot of stuff that happened. I mean, we have all new vocabulary: Goto Fail, Heartbleed, BadUSB, Shellshock, POODLE, and Regin.

Leo: Oh, this was all this year. Oy.

Steve: Yeah. I mean, it's been a busy year. So of course, as we were coming, I guess it was late in 2013 that the P.F. Chang hack happened. It was sort of in the Southeast.

Leo: It was Black Friday of last year that the Target hack happened.

Steve: Right.

Leo: And the P.F. Chang happened.

Steve: And then we got, early in 2014, we got more of a sense of scale for that.

Leo: Yeah. It went from, what was it, 11 million to 70 million, something like that, records revealed?

Steve: Yeah, I think 70 million was the number for Home Depot, and Target was 40 million.

Leo: Forty million credit cards, but 110 million customer records.

Steve: Yes.

Leo: Oy, oy, oy.

Steve: Yes. And...

Leo: There's only, what is it, 400 million people in the U.S. That's like every adult in the U.S.

Steve: And it was estimated that the cost of replacing all of those disclosed cards came to about $400 million.

Leo: Oh, wow.

Steve: And we did report a few weeks ago on the podcast that Posner, our old friend Judge Posner, said no, we're not going to let you throw the case out. This is going to go to trial. We're going to...

Leo: Yeah. The banks are suing Target over this and saying that they want to recover that cost.

Steve: Yes, on the argument that Target did have enough information to prevent it; and negligence, not some weird cyber hack, but negligence was the underlying factor here. And so we're going to test whether that flies.

Leo: That will be a fun trial to watch in 2015.

Steve: Ooh, it will, yeah. So we have that to look forward to. Now, early in the year, and we'll remember this because this was another fun thing we talked about, we discovered that many consumer routers had a wide-open backdoor, way up at about half of the port space. Ports run from 1 to 65535. And right in the middle is 65536. Three six?

Leo: No.

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

Leo: I memorized this.

Steve: 32768.

Leo: 32764.

Steve: No, well, yeah, but eight is in the middle.

Leo: Eight's in the middle.

Steve: 32768. So it was four down from the exact center of the port space was a port listening for connections.

Leo: Wide open.

Steve: And if you set the hosts - remember when a web browser makes a query, one of the things it has is the hosts header that identifies what it is.

Leo: All operating systems have this.

Steve: And for weird apocryphal reasons, they all say Mozilla, among other things, because that was the first browser.

Leo: First browser, yeah.

Steve: And so even IE says, oh, yeah, I got some Mozilla here somewhere. And we doubt that. But so if you reversed the phrase of the person who apparently put this in, and I can't remember what the phrase was now, but anyway the point is you put that in the hosts header and make a web query from the outside on the Internet to that port. It says, oh, hiya, what do you need? What can I do for you? And there's, like, 14 commands.

Leo: There's commands; right? Yeah.

Steve: It's like commands you can execute. Now...

Leo: Is this like a service port?

Steve: Well, the theory was that this was the way ISPs or router manufacturers or somebody, I mean, it was undocumented. And someone just ran into it.

Leo: Possibly it was an Intel reference code, we've seen that before, and just got duplicated.

Steve: We have seen that before in the - I just almost had it, and I lost it.

Leo: Yeah, I can't remember, either.

Steve: It wasn't - was it Bluetooth?

Leo: Yeah, no, it was in the - the baseband radios in cell phones had an error in code because everybody just copied, literally cut and paste, the reference code. I think it was from Qualcomm, not Intel.

Steve: And it was never - you were never supposed to use it. But it's like, well, okay, this works.

Leo: Hey, they wrote it already.

Steve: Why reinvent that wheel?

Leo: So I'm guessing that's probably why because it's not just Cisco and Linksys, which is one company. This is also Netgear. It was other companies.

Steve: I think it was - it wasn't Sercomm. It was everybody, it was all the routers based on one manufacturer who had this.

Leo: Oh, okay. The chipset, probably, yeah.

Steve: Okay. So that was right over Christmas and New Year's.

Leo: You wrote a little program to test for this. Didn't you? There was a way to test for your router being...

Steve: Oh, yeah, yeah, yeah. You can just see if it accepts a connection. So you're able to use ShieldsUP!, for example, and just see if it accepts...

Leo: Oh, okay. Look at 32764.

Steve: Exactly. And if it connects, it's like, whoops.

Leo: Hello.

Steve: That's not good. Okay. So get this. So the next thing that happened was everybody updates their firmware. New firmware is issued by Cisco and Linksys and all of those. And now that no longer happens. So we assume all is good.

Leo: Right.

Steve: It's not.

Leo: What?

Steve: We're going to come back to that here in a minute.

Leo: Okay.

Steve: Because the next thing that happens then is that on February 21st, Goto Fail...

Leo: Oh, my gosh. This was the worst.

Steve: ...enters the world's vocabulary of Internet problems, which was a tiny, like, what, well, goto fail. It was a tiny error...

Leo: One line. One line.

Steve: ...in source code that was like - and you could even look at it. And this is why debugging code is so tricky, is you can look at it, and it seems fine.

Leo: It was a case statement that got bypassed. And unfortunately the case statement was testing certificates.

Steve: Yes. It was a particularly important moment in the code.

Leo: So, and this was in iOS and OS X.

Steve: Yes, because they're using a common code base, which this demonstrated. And what it meant was that signatures had never been checked.

Leo: Been tested. Oh, just forget that.

Steve: It's like, we'd like you to sign it right, but you really don't bother, you know, just change a few bits here and there. And so this had just, like, gone unseen. And we assume and hope that nobody was taking advantage of it. And so Apple, remember that Apple was a little cagey on this one. They pushed the fix out first, and then afterwards they told us.

Leo: Finally admitted it, yeah. But what was interesting was the notion that this might have been introduced by a bad actor intentionally. That if you were going to...

Steve: Make it look like a mistake...

Leo: Make it look like a - this is exactly what you would do. And it's just that spot.

Steve: Yeah.

Leo: Apple never talked about that.

Steve: No. And if so, it was clever. And in fact I remember a lot of people talking about that, because this came from open source originally, it ought to be possible to track down a log.

Leo: You have a version log, a changelog.

Steve: A changelog, yeah.

Leo: And you should be able to see who did it. Never heard.

Steve: No. No.

Leo: Just quietly buried. In fact, a lot of the stories from this year, because we have such short memories, just disappeared. This was the year TrueCrypt bizarrely disappeared.

Steve: I know.

Leo: And we still don't know what happened.

Steve: Two months after that, what is it, April, mid-April, like, you know...

Leo: The TrueCrypt authors...

Steve: Like one morning we wake up, and the TrueCrypt website is gone, and it says you'd better not use this because it may contain security errors, and we're not going to fix it. We're checking out.

Leo: You had the best, I think probably the most sensible theory, which is that these guys just were fed up with the open source background noise you always get, people complaining.

Steve: Oh, thankless, thankless.

Leo: Thankless job. And not that they had found a flaw, but they just didn't want to be responsible anymore. So they said go use BitLocker. We'll see you later.

Steve: And we're going to 64-bit systems. We're switching from...

Leo: We don't want to keep it up to date.

Steve: ...master boot records to GPTs, the GUID Partition Table. That would all have to change. I mean, they would have had to have put in a huge amount of work. And I think they had what they wanted.

Leo: It was a singularly graceless retirement.

Steve: It was, yes.

Leo: It wasn't very graceful.

Steve: Thank you very much for TrueCrypt all these years, but you could have done a better job of saying goodbye.

Leo: Now, the good news is, and actually we still haven't heard the second part of the audit, but the audit is ongoing now, yeah?

Steve: Yes.

Leo: So a third party from Johns Hopkins has raised money and is actually going through - because the code is available. It's not open source, technically, but the code is available.

Steve: Right, it's "available source," as they call it.

Leo: So he's been going through the source, or somebody, some team has been going through the source.

Steve: Well, so, yeah. The first phase was done. And that only checked the boot technology and the getting it going part. It was not a full-blown crypto review. So, but no one has any reason to believe that that's a problem. And we know for a fact, for example, because we've covered it, that the FBI is often thwarted by TrueCrypt. The Brazilian government sent them a drive...

Leo: In 2012 they were.

Steve: ...because some real estate guy had stuff on it that they were unable to get.

Leo: Is the audit still going on? I think so.

Steve: Last I heard, Matthew Green was still on top of it, and it was going to proceed.

Leo: So soon, I hope, we'll know. I guess this is harder than one imagines.

Steve: Oh, it's work, I mean, and you do need money to pay people to dig in there that much.

Leo: Now, your advice at the time was go ahead and continue to use TrueCrypt. In the absence of any known flaw, it's safe. You still think that's the case.

Steve: I still have it on the website, and I'm offering it, and it's downloaded often.

Leo: Well, that's another point. You can't get it from the old source, but Steve has the last good version. They actually released a version after that that was a damaged version, intentionally damaged version.

Steve: Right. And in fact this demonstrated - I did an interview with someone not long ago where he asked me why I believed this was well planned. And I said that that final iteration of TrueCrypt, I think 7.1a was the last official release, and they probably went to 7.2, or I don't remember how they incremented the number. The point was they neutered its ability to encrypt drives, leaving only the ability to back it out, to finally, to permanently decrypt the drive. But that change was massive. You had to go through all kinds of places in the code in order to do that. So they spent a long time preparing to say goodbye.

Leo: Isn't that weird.

Steve: Even though none of us were impressed with the way they did it.

Leo: The last I've seen, Matthew Green said he was going to finish the audit this year. So I don't know where that stands. We've got to call Matthew. Because he raised 60, $70,000 to do it. And he says...

Steve: It might be taking longer. But if he's got that much money...

Leo: He also - I'm looking at an article from Krebs on Security at that time, in May - was putting together a team to kind of take over the TrueCrypt code. But we haven't heard anything about that, either.

Steve: No. And I remember when there was someone who was in touch with one of the authors, and I saw Matthew asking that third party to ask the authors for license privileges because Matthew was respecting the fact that this wasn't technically open source. Now, it has been forked, but those are not authorized forks because this wasn't forkable. They were saying, "We're going to let you see our code, but it's still ours. We're not wanting it to be used as a template." Now, and in fact, one of the other offshoots has updated TrueCrypt a little bit, just adding a bunch of features that don't really matter.

Leo: There's also TrueCrypt.ch, and they're creating something very oddly named CipherShed.

Steve: Yeah. I think there's a VeraCrypt, also.

Leo: Yeah. So there are people trying to do it. But the last post is from September, and they say we're closer to alpha, and then nothing. You yourself had a crypto project you were about to embark on. And then after learning about these national security letters and the demands that the U.S. federal government has made to put backdoors, you decided, "I'm not going to do this."

Steve: It was Posner who said - he was attending a cybercrime conference, like a month ago. And he said, "I don't think it should be legal for cell phone manufacturers to create technology the federal government cannot access." So I still - the jury is out, almost literally. Actually it'll be an Act of Congress rather than a courtroom, whether Congress could simply require that commercial entities create a cryptographic backdoor. It could happen this year. Or, that is to say, next year.

Leo: It seems strange that we would have a judiciary and a Congress that would have such an abiding trust in the federal government forever. We've had such historical records of - and this country was founded based on kind of a lack of trust in federal government.

Steve: And set up in order to create checks and balances, of course.

Leo: Yeah. That makes me nervous. When all the branches of the federal government agree, "Oh, trust us." That makes me nervous.

Steve: Then we had arguably the best logo that's ever been...

Leo: Heartbleed, baby. I know where you're going with that one.

Steve: Now, and that's really - we learned a lesson.

Leo: Usually exploits don't come with a logo.

Steve: If it doesn't have a logo and a catchy name, it's just hard to take it seriously.

Leo: What was Heartbleed? Refresh my memory.

Steve: Okay. So Heartbleed was a defect that was found in the TLS protocol because there's something called a "TCP heartbeat" which allows you to sort of send a heartbeat packet to sort of keep TCP alive at the TCP protocol level. And it turns out that there was a buffer overrun in that, that was found. So the idea was you could send a malformed packet to a server that had heartbeats enabled. And that's the other thing. Nobody uses them. Nobody needs them. Nobody ever needed to have them enabled, but everybody did because it was enabled by default in OpenSSL. So you could send a packet to this server, and it would send back a gift, 64K...

Leo: Just random.

Steve: ...of whatever happens to be...

Leo: Just whatever's in memory.

Steve: ...whatever's in memory.

Leo: Here you go.

Steve: Yeah.

Leo: We don't know. Here's something.

Steve: Thanks for asking. Thanks for asking in that strange way you just did.

Leo: But it could include, not necessarily, but it could include things like logins and passwords unencrypted.

Steve: Correct. Correct. And so everyone ran around, like in a craze. And then the guys at CloudFlare said, you know, this is just random crap in memory.

Leo: Yeah, not necessarily useful, yeah.

Steve: We're not convinced that you're ever going to have the server's keys.

Leo: Wasn't there an exploit, though, wasn't there a demonstration?

Steve: Well, they created a honeypot. They put up a server, and they said, here's a server. Go. Oh, but before they did - so they fixed up, they cleaned up their whole network of, I think they use nginx. But they were using SSL as the security protocol, as everybody does. So they were aware of the problem. They shut down the TLS heartbeats, which is all they had to do, just turn that off, because it shouldn't be on anyway. No one uses them. Then they set up a honeypot because they were not sure that it was actually, you could actually get credentials from the server. And they said, "Here's a machine at this IP. Prove it. Send us a message signed by the server's private key, and then we'll believe you." They got some. That's when they said, oh, my god.

Leo: This could be serious.

Steve: And they replaced their entire certificate infrastructure.

Leo: Whoa.

Steve: Remember, hundreds of thousands of certs because the Heartbleed flaw doesn't leave a log. This happens before logging engages. It's right, like at the front door, if you knock funny, it just dumps out 64K of memory. But you don't connect or do anything. So you don't get into the logging system. No one's logging at that level. So they realized...

Leo: No record of it.

Steve: They didn't have logs, and it was exploitable. Anybody could have exfiltrated the private keys in their architecture.

Leo: It turned out it wasn't login and password you had to worry about, it was certificate keys.

Steve: Yes, it was the server's identity, the server's private key. And so a number of researchers, security researchers jumped on the problem, demonstrated that it was exploitable. And then the only responsible thing for everyone to do was to rekey. You had to. And that's where I got all bogged down with the revocation issue, remember, because this was the whole revocation thing where Chrome's got a handful of certificates, and suddenly here's a hundred thousand have just been revoked by CloudFlare. Chrome can't handle that. Chrome just doesn't bother with those. And that's where I got into the whole CRL...

Leo: Yeah. Well, what is the upshot of all of this? Has Heartbleed been fixed? There was a new OpenSSL.

Steve: Yes.

Leo: Did everybody patch?

Steve: It got fixed, and everybody patched, or turned off heartbeats is all you really had to do.

Leo: You could just - a line in the config turns it on.

Steve: Exactly.

Leo: But we also have this now worry that maybe many certs have been compromised.

Steve: Right. And we have basically a broken revocation system. We do not today, even now, have a revocation system which functions because...

Leo: So I can't, as a website, say, hey, don't use that old certificate, it may be compromised. Here's my new certificate, and that other one's not good anymore. It doesn't work.

Steve: Because a bad guy, until it expires...

Leo: Might have that certificate.

Steve: Until it expires. So certificates have, what, like a two- or three-year...

Leo: So I could pretend to be Amazon with its old compromised certificate, and there's no way for Amazon to say don't use that.

Steve: Right, because Amazon serves...

Leo: Is that still the case today?

Steve: Yes. Amazon is serving the new one, but the old one, if it ever got loose...

Leo: Your browser won't know.

Steve: Until it expires due to its own aging.

Leo: Right. No word from the browser.

Steve: Right.

Leo: So that's never been fixed.

Steve: No. Can't fix that.

Leo: Thanks, Chrome. Do other browsers handle it better?

Steve: There is a system, the OCSP, Online Certificate - OCSP. Online Certificate Status Protocol? Probably. Acronym soup. That's a system that allows the browser to query for the real-time validity, the status of the certificate. So that system exists. The problem is that, if the browser doesn't hear anything, if it doesn't hear "No, it's bad," then it says, "Okay, fine." That's the fail soft.

Leo: It may be down.

Steve: Yes, exactly, maybe having a bad day.

Leo: Slow. I don't want to slow things down. Let's just go on. Let's just get...

Steve: Maybe you're in North Korea, and you have a good connection. So then what we want is we want fail hard. And you could turn that on in Firefox and then - and I have it on, and a lot of our listeners do because we were sort of curious.

Leo: But it's not on by default.

Steve: No, it's not, because it could keep you from getting to sites. And oddly enough, Google seems to be the one with the worst OCSP servers. They're unable to affirm the validity of their certificates in a timely fashion. And the only troubles that I see reported are people saying, "Hey, I got OCSP hard fail enabled, and I have problems with Google sometimes."

Leo: Worse than that, Imperial Violet, who works for Google, said don't turn it on.

Steve: Adam Langley.

Leo: Adam Langley said don't turn it on.

Steve: Oh, I know. Adam Langley, well, you know.

Leo: He and Steve don't get along so good.

Steve: And it's not getting any better as time goes on.

Leo: And this is Larry Seltzer's article in which he defends it. It's a really - it was a great back-and-forth. We had a lot of fun, and Larry mentioned you.

Steve: Yup.

Leo: And I don't know if the right answer has ever been deduced.

Steve: Okay, so the right answer, we're getting there. The right answer is called "stapling." Stapling has the server that is offering the certificate getting a fresh response from an OCSP server, or like the certificate authority, and stapling it - like stapling two things together, thus the word - stapling a short-term affirmation to the certificate it's issuing. The problem is we still don't have the infrastructure for that. I mean, again, things need to change in order to - or evolve further. So people recognize it's a problem, and Heartbleed showed that it would be really nice if we were actually able to revoke all of the certificates on the Internet once that may have been exfiltrated due to an old vulnerability that we don't know that no one exploited.

Leo: You're listening to Security Now!, Steve Gibson in-studio. And we're going through all the fun and games of 2014.

Steve: Okay. So we talked at the beginning of the year about the backdoor found in the routers over Christmas and New Year's. Toward the end of April, it turns out it was still in the firmware.

Leo: Nobody'd fixed it.

Steve: Well, they'd - well, okay. They locked the front door, or the backdoor, but with a key that wasn't very strong. So what happened, it turns out that somebody looked through the code and realized that that same host string thing was still there, and the port was still...

Leo: Open.

Steve: ...being opened. But you had to first receive like a knock at the backdoor. You had to send a knock packet, an Ethernet packet, containing certain stuff. And so the router would see that and go, oh, and unlock the backdoor.

Leo: Let me let you in.

Steve: Exactly. Now, that would be a concern, except that it's an Ethernet packet, not an IP packet. Which means it has to be on the LAN.

Leo: That's good.

Steve: Yes. Because that means it's constrained to your cable...

Leo: It's not routable.

Steve: It's not routable. So it would be within your cable provider. Now, there's a vulnerability because, on a cable topology, everybody's on...

Leo: Your neighbors could knock.

Steve: Yes. Exactly. And so that's still in the routers.

Leo: But they'd have to be your neighbors.

Steve: They would have to be on your local segment, within the same Ethernet routing space.

Leo: Wow. And we mentioned, and I see in your notes, it was Sercomm that made the chipset or whatever that all these different companies used. So it was, if you had the Sercomm components, you'd be vulnerable.

Steve: Yup.

Leo: BadUSB.

Steve: Oh, boy. You know...

Leo: BadUSB. Now, before BadUSB happened, there was a guy who was a well-known security guy, I can't remember what his - was he at Black Hat or - who said, "I had a virus jump the air gap."

Steve: Oh, yeah, yeah, yeah.

Leo: And everybody said, come on, you can't - nothing would do that. He couldn't understand how this virus had jumped the air gap.

Steve: He couldn't get rid of it. It kept coming back.

Leo: He would erase everything, format the drive, and it would still jump into his BIOS or something.

Steve: Right. Oh, that's what, yeah, he was thinking it was his BIOS was being infected. And the problem is all BIOSes are so different that you couldn't have a universal BIOS virus. It'd be like a Windows virus infecting a Mac. It can't.

Leo: Right, yes. They're too different.

Steve: Yeah.

Leo: Okay.

Steve: Just very different DNA. So BadUSB freaked out people, I think, disproportionately.

Leo: This was at Black Hat.

Steve: Yeah.

Leo: In August.

Steve: And what the presenters at Black Hat demonstrated was that a manufacturer of the core of many thumb drives - so many different manufacturers of thumb drives buy from the same outfit. That BIOS, the firmware of the USB controller, was rewriteable.

Leo: It was not on a ROM, a read-only memory.

Steve: Right, correct.

Leo: It wasn't even on a programmable read-only memory. It was on EEPROM, an electronically erasable.

Steve: And remotely accessible.

Leo: Oh, boy.

Steve: So you could give some commands that were kind of off the book through the USB port and send it new firmware.

Leo: Here, USB.

Steve: Be different.

Leo: And by the way, not just thumb drives, but anything connected via USB.

Steve: Be a keystroke logger. Partition yourself off and have malware in a hidden region which will be injected into the computer. Or pretend to be a keyboard and type something of our design.

Leo: Anything that used this firmware. So it could be an iPod, or it could be a hard drive or a thumb drive or even a keyboard, if there's enough memory.

Steve: Yeah.

Leo: But you say it's not, what, it was overblown.

Steve: It was nice that we knew about it, but...

Leo: Yeah. Kind of shocking that it was possible.

Steve: Yeah, and I don't believe - I don't remember now whether normal driver software in the computer was able to issue the special codes needed.

Leo: It might need some special software.

Steve: So it couldn't be a worm. It couldn't jump around by itself. You could deliberately, you know, bad guys who got access, physical access to the thumb drive could reprogram it and make it be BadUSB. But your thumb drive couldn't get infected by being plugged into a machine...

Leo: That had malware on it.

Steve: ...because it didn't have access to it.

Leo: Right, right. So it hasn't in fact been a big issue.

Steve: Yeah.

Leo: I don't think anybody's fixed it. It's not like...

Steve: No, I mean, everybody still has those thumb drives.

Leo: Yeah, yeah.

Steve: Yeah. But so it scared a lot of people. And we looked at it closely to gauge how big the problem was. And it was like, okay, well, nice to know. But it's probably not going to get you.

Leo: It's BadUSB. Certificates. Google did a few things this year to kind of, in their opinion, push forward security.

Steve: And I love the idea because what Google is seeing, and they're not wrong, is no one fixes security until the house is burning down.

Leo: Right, right.

Steve: We're always waiting till the last minute.

Leo: So they've used Chrome as a way of kind of pushing forward HTTPS Everywhere, the abandonment of the bad SHA-1 hash...

Steve: Yes. Well, and then so what was controversial about that was that it was already - there was a scheduled sunset for the use of SHA-1 put in place by Microsoft, who also has substantial market power.

Leo: With Internet Explorer, yeah.

Steve: 2017. That's when it was going to happen.

Leo: Okay. Two years.

Steve: 2017. And Google decided, no.

Leo: Let's do it now.

Steve: Let's do it now. Why wait? Well, there's lots of reasons, it turns out, to wait. Because people have other things to do. They have schedules and so forth.

Leo: This is something that we're going to start seeing soon, like in February, I think?

Steve: Yeah.

Leo: Your browser will see a certificate that uses this broken hash technology.

Steve: Okay. It's not, though. And that's why it's controversial.

Leo: Oh, that's right, it's not broken, it's just...

Steve: It's not broken.

Leo: Potentially computers are going to get so fast they'll be able to decrypt it.

Steve: Not even that.

Leo: Not even that.

Steve: Not even that. There is nothing wrong with waiting till 2017. Microsoft wasn't wrong. That's what upset everybody was that there's no hurry.

Leo: It's not an existing problem.

Steve: Correct, it's not.

Leo: It's kind of planning for the future when computers do become fast enough.

Steve: Yes. And so that's why it was controversial was Google said we're going to start penalizing websites in 2015, two years early, if they still have an SHA-1, if their certificate is signed using SHA-1.

Leo: And the penalty would be, what, in Chrome...

Steve: You'd start seeing scary things. And they have 60% market share. So that's bad.

Leo: It hasn't happened yet, though.

Steve: It hasn't happened yet. GRC's certificate, mine, is signed with SHA-1.

Leo: So when we start seeing warnings...

Steve: No.

Leo: No?

Steve: Because I have it expiring on midnight of December 31st, 2016.

Leo: Okay. Oh.

Steve: And so this is why it's so confusing, is Google is going to start scaring people if the certificate would be valid in 2017.

Leo: So they're checking the expiration date.

Steve: Yes.

Leo: And saying, okay, you use SHA-1, and you will continue to...

Steve: And if you don't change it, it would be valid in 2017.

Leo: Did you change your expiration date? Can you do that on a certificate?

Steve: No. I have friends at DigiCert.

Leo: Ah, you got new ones. Got it.

Steve: I rekeyed so that I was expiring...

Leo: Why didn't you just get a better - why didn't you just abandon SHA-1 at that point?

Steve: Ah. Perfect. Thank you. We're a good team.

Leo: Why didn't you do that, Steve? Tell me.

Steve: It's because there are still systems out there that only know SHA-1.

Leo: Ah, okay.

Steve: They cannot handle - and it happens that XP are among them. And there's still a huge number of XP machines. Now...

Leo: So if people went to GRC, and you had deprecated SHA-1, and they went there, what would they see? That this site...

Steve: No, it won't come up.

Leo: It wouldn't load.

Steve: You can't load. Now, many sites only switch you to secure when you log in. GRC is HSTS. It's, no, HTTPS Everywhere.

Leo: HTTPS Everywhere.

Steve: So you can no longer use GRC without being secure. So if I had switched to SHA-2...

Leo: You would have left out a lot of people.

Steve: They couldn't get to GRC at all.

Leo: Wow.

Steve: And so what this does is this allows me to continue offering GRC to everyone for the next two years, until the end, all the way through 2016, without generating any warnings even from Chrome. And those people who are on XP will be getting warnings from everyone else.

Leo: But as a result, your grade at SSL Labs is now a C, my friend.

Steve: I know. I was A-plus. It was brief. It was brief.

Leo: So this is to me a little controversial. You've mentioned Qualys's test, and we've talked about it a lot.

Steve: I love it.

Leo: And you love it.

Steve: And Ivan is a great guy. He's doing a really good thing.

Leo: One of the things Ivan did at some point was say, well, if you're using SHA-1, I'm going to downgrade you.

Steve: Yeah.

Leo: And that's - is that why you got a C?

Steve: Oh, it's bad. There's all kinds of things he doesn't like now.

Leo: There's other things you do.

Steve: You can click on the link and get the details.

Leo: There's other things you do. Oh, oh.

Steve: Yeah, he's like...

Leo: Oh. You're good on certificate and protocol support, but...

Steve: Yeah, look at that. I'm 100s and 90s everywhere.

Leo: You're vulnerable to POODLE. That caps you at a C. You can't get better than a C.

Steve: No.

Leo: You use the SHA-1. That's a weak signature.

Steve: Actually, it's the rePOODle that we'll be getting to in a minute.

Leo: Uh-huh.

Steve: It's because I still offer SSL 3.0, which is now a no-no.

Leo: No-no. And, by the way, Steve knows what to do, and he's chosen to do this for good reason, I think.

Steve: Yeah.

Leo: Yeah. You accept RC4. And but otherwise you're okay. Bad man. All right.

Steve: Yeah. Anyway, I need to reboot the server because I am going to turn off RC4 because we don't need it anymore. And I'll turn off SSL3. And I just haven't gotten there.

Leo: But then you'll be capped at a C anyway because you still support SHA-1. Won't you? I don't know.

Steve: No, I think I can get a B. He'll give me a B because - but I don't get my A-plus anymore.

Leo: So Ivan and Google are punishing people who use this old...

Steve: Yeah.

Leo: But let's reiterate. It's not cracked. It's not broken.

Steve: There's nothing - I wouldn't be using it if there was anything wrong with it. There is nothing wrong with it. And Google isn't, I mean, so what Google is doing, Microsoft was, as of 2017, going to deprecate that certificate. They would no longer accept them after 2017. So what Google is doing is saying, starting in a few months, if the certificate could be used in 2017, we're going to punish you now.

Leo: We haven't seen yet what that will look like.

Steve: No.

Leo: And they didn't say what it would look like.

Steve: And they're saying that it will do something in the user experience. There'll be something that gives you...

Leo: And it could be something minor.

Steve: Could be.

Leo: Could be an unlocked padlock, you know.

Steve: Just like, you know, upside-down question mark or something. We're not sure about this.

Leo: We don't know.

Steve: We don't know what's going on. Maybe a new color.

Leo: And I seem to remember it's, like, soon. It's like February or something.

Steve: Yeah.

Leo: Yeah. We're still in Q3. We've got to keep moving here.

Steve: Okay, yeah. Okay. So Home Depot.

Leo: Home Depot.

Steve: Seventy million.

Leo: No big deal.

Steve: Big problem.

Leo: People already - they already had my credit card from Target, so...

Steve: Oh, I'm sorry, 56 million.

Leo: Oh, that's all, okay.

Steve: Although it actually affected a lot more people, I don't know why, that I know. They were like, oh, my god, my card's been hacked. In fact...

Leo: Would the bank automatically send you a new card? Or do you have to somehow do something about it? Probably be prudent to check.

Steve: I don't know what they did.

Leo: There's no, like, everyone - sometimes the people create...

Steve: My friend found a charge on his card that was not his and called the bank. And they said, oh, yeah, we've been getting a lot of calls.

Leo: Oy, oy, oy, oy, oy, oy, oy.

Steve: Yeah. I'll bet you.

Leo: And when they say, "Oh, hey, did you shop at Home Depot in the last three months? Oh."

Steve: Okay. Shellshock.

Leo: Shellshock.

Steve: Another great name because, again, it's about the name: BadUSB, POODLE.

Leo: Although "bashdoor" is not bad.

Steve: That's not bad. Bashdoor is pretty good. So Shellshock turned out to be a mistake, also very old, that had been there in the bash interpreter for, like, ever.

Leo: Wow. Wow. Wow.

Steve: Where it would, when you invoked bash, it would run through the environment variables that were in the system and execute commands. And it turns out that services running on UNIX, Linux, would sometimes transfer data from the query to the environment.

Leo: Right.

Steve: And so it was very clever because that meant that you could invoke the service remotely. It would accept the connection.

Leo: Yeah.

Steve: And then, like, move some of the headers from a query into the environment.

Leo: It's for convenience, for programmers. Then they can use this kind of temp variable.

Steve: So much easier that way.

Leo: Yeah, yeah.

Steve: But then they would later, for their own purposes, they would use bash for some of their own work. So by them, by the service invoking bash, bash would then go look and parse the environment and find the variables. And so if the hacker had put bash commands in the headers, they would end up getting executed.

Leo: Wow.

Steve: Shellshock.

Leo: Yeah.

Steve: And there are now worms crawling around the Internet using this. Worms were developed.

Leo: So Apple has bash. All Linuxes have bash.

Steve: Everybody's got bash.

Leo: Were they updated by Linux and, you know...

Steve: Yeah.

Leo: Did Ubuntu update? And Apple...

Steve: Yeah, yeah, yeah.

Leo: ...updated their bash.

Steve: Yeah. So the response was, we're not sure why anyone is parsing commands in the environment.

Leo: Stop it.

Steve: Nobody ever wanted to do that.

Leo: Well, I think, I'm guessing, but it does happen in Perl, too, where you'll execute something, and the return statement is stored silently in a temp variable that is used, an exclamation mark or something, that you can reuse.

Steve: There's nothing Perl doesn't do, actually.

Leo: Yeah. And bash does that, too, for convenience. So you execute a command, and you don't have to have an explicit return. You're just going to have in some temp variable stored in the environment the return, and then you can use that in your continued code. But now we can see the problem.

Steve: Yeah.

Leo: It all happens because this stuff was written before ubiquitous Internet.

Steve: Exactly. Back once upon a time, where there was you and your console, it would have been a handy feature. And this is the sort of thing that UNIX hacks have always worked around is that sort of policy. But exactly that. Then we add servers, and no one remembers that bash is going to parse things. I mean, and so, and it also really - you could argue that it required, to know that that was a problem, several different knowledge domains.

Leo: Right.

Steve: An obscure feature nobody even knew bash had.

Leo: Or even thought about how it might be misused, really, frankly.

Steve: Yeah, exactly, yeah.

Leo: Somebody's saying it does have to go through CGI.

Steve: Oh, okay. So...

Leo: So that's a little bit of a protection.

Steve: So a CGI interpreter was a way to get in there.

Leo: Yeah. You'd have to be running a web server and so forth. So, but there are botnets out there created by this, yeah.

Steve: Then we have POODLE, another great name.

Leo: Okay. This is an acronym. I didn't know that.

Steve: Yes.

Leo: What does it stand for?

Steve: Padding Oracle On Download Legacy Encryption. Okay, now, that's a hard - this is one where they had the "P."

Leo: Sounds like a retronym.

Steve: Exactly. They had the "P." Okay, what can we come up with that's like "P"?

Leo: All right. Padding, we got padding.

Steve: And Oracle, that's a common crypto term.

Leo: But they don't mean Oracle the database company.

Steve: No.

Leo: They mean like a...

Steve: No, a cryptographic oracle.

Leo: Like oracle, okay.

Steve: Where you do something, and it gives you a response. It replies to you. So this was in October, only a few months ago. Everyone's still remembering that. And that was - this is the first bite of the POODLE. There were two bites of the POODLE.

Leo: Right.

Steve: The POODLE re-bit. So, and the problem with POODLE was that we knew that there was a problem with probing SSL. And everyone assumed that, by moving to TLS, we would be safe. But the reason there's a downgrade attack is that - so we know the way SSL works is the client says, here's the list of things, the list of ciphers and protocols that I know, hands that to the server. Server looks through them and, in its own prioritized list from best to least good, it chooses the most secure one that it knows that the client also knows. And it says, okay, let's use this. Well, it turns out that, if a hacker got into the conversation and eliminated the TLS offerings from the client...

Leo: The secure choices.

Steve: Well, the TLS secure ones. So what the server would only see is SSL3. So then the server would go, wow.

Leo: That's all you talk.

Steve: Dumb client. Okay, fine.

Leo: I haven't seen anybody like that in a while, but okay.

Steve: So what the client would see back...

Leo: Instead of using public key crypto, let's use pig Latin. And at least you understand that.

Steve: Yeah, exactly. So the server thinks the client's dumb. The client sees the server offering SSL3. The client thinks the server's dumb.

Leo: Otay.

Steve: Because they think that SSL3 is the best they can do.

Leo: So it did require kind of a man in the middle.

Steve: It does. Oh, yeah, you have to spoof that. Now we have got - we've done a downgrade, what's called a "protocol downgrade," where, rather than having the protocol we could have, the hacker has pushed us back down to one that's vulnerable. Now we can use a well-known attack where you send multiple probes in, and you can, over the course of about 16,000 queries, you can start guessing bytes from cookies.

Leo: That's a lot of queries.

Steve: It's a lot of queries. That's why it's like, uh...

Leo: So you still - you're POODLE vulnerable.

Steve: Yes.

Leo: You still support SSL3 on GRC.com.

Steve: Well, actually, yes, I support SSL3.

Leo: And is that for XP users, as well?

Steve: It's not, actually.

Leo: Who's that dumb?

Steve: It's just I haven't rebooted the server.

Leo: Oh. If you reboot, it'll go away?

Steve: Yeah.

Leo: Okay. And then you'll at least pass the POODLE test.

Steve: Then I get a B instead of a C.

Leo: All right. Can you reboot from here?

Steve: I don't like to reboot.

Leo: I don't blame you.

Steve: No, because it's, you know, it stays up for, like, years at a time.

Leo: You like that uptime - four years, 73 years.

Steve: In fact, I reboot so infrequently that I like to go there, just because if any smoke comes out of something, I mean, it's like, I don't know if it's going to, you know...

Leo: That's why you're not doing it from here.

Steve: That's why I'm...

Leo: You could do it from here, but...

Steve: Oh, yeah. In fact, I did VPN in from here because I wanted to see - by the way, I forgot to say that the docs are not yet online because I've never VPNed into my Windows 2008 in the two years that I've had it.

Leo: And it didn't work, or...

Steve: Well, I just never set it up. I didn't have remote filesharing.

Leo: I remember you coming to Toronto and using the smallest computer I have ever seen in my life...

Steve: The little Libretto?

Leo: It was a Libretto, Toshiba Libretto.

Steve: Yeah.

Leo: And you were VPNing into your - it was the strangest thing I've ever seen. Do you still have that?

Steve: Yeah.

Leo: Of course you do.

Steve: I do.

Leo: Is it in the freezer?

Steve: No, that's the one that runs the Kindle on my stair climber is the little Libretto.

Leo: Good use for that.

Steve: So it's a good use for it, yeah.

Leo: You must have excellent eyes, that's all I can say.

Steve: No, no, no. I have a huge screen mounted on a...

Leo: Oh, plugged into the Libretto.

Steve: Yeah. It's like, look at all the screens you have.

Leo: Nice.

Steve: Yeah, exactly. And a clicker strapped to the handles.

Leo: Oh.

Steve: Yeah, so I'm able to do...

Leo: It's like a teleprompter.

Steve: Exactly. Okay. So POODLE gets resolved by turning off SSL3, and...

Leo: Which nobody uses. It would be harmless to do that; right?

Steve: Even XP has TLS 1.0. So I'm going to reboot any day now. When I get home. That gets resolved. Then along comes Regin.

Leo: Oh, boy. Now, we still don't know the official pronunciation. Symantec named it. You first thought it was Regin because it used the registry.

Steve: Registry Install, yes. But there's a video of a Norseman saying "Regin."

Leo: Because he's the King of the Norse or something?

Steve: Yeah.

Leo: Some historic character.

Steve: Yeah.

Leo: All right.

Steve: Regin.

Leo: Regin.

Steve: We know it's Regin. Sort of like the President.

Leo: And it was one of these - it was fascinating. You actually were quite impressed by the technology.

Steve: Yeah.

Leo: It's one of these probably state-sponsored attacks.

Steve: Yeah. And this is one that we didn't - we're pretty sure this is Russian in origin.

Leo: Oh, really. Because I thought at the time we decided it was U.S. or Britain.

Steve: No, it's because Western countries are where it's been found. So it's the Russkies that are poking at us.

Leo: And is this the one that got into things like airline reservation terminals and hotel...

Steve: Yes, and like pulling metadata about people's movements and where they were staying, then determining, like, who was talking to whom.

Leo: And it was really impressive because it had a loader.

Steve: Four-stage loader. Remember, it came in and looked around, and then it said, okay, the coast is clear, and it brought in...

Leo: Come on in.

Steve: ...the second stage.

Leo: And it would decrypt these. These are all encrypted modules.

Steve: They were all successively encrypted. And the thing that was disturbing was we found out in retrospect that the antivirus companies had known...

Leo: Something.

Steve: ...something for a couple years and hadn't blown the whistle because it's almost like they were complicit. They weren't sure whose side it was on. So they didn't want to blow it if it was on their own local government's side. So they just kept quiet until additional information came to light, as finally did...

Leo: So now we think it's...

Steve: We think it's Russian.

Leo: ...Russian.

Steve: Yeah. And this, I mean, this is the first clear evidence we have of the same kind of competence of deep espionage-grade malware that we presume the U.S. has, and so the East does, too.

Leo: And then finally the POODLE bit again.

Steve: Yes. It turns out that the fix for POODLE was turning off SSL3. And so everyone ran around and turned it off and, except me, rebooted their servers.

Leo: Right.

Steve: I'll do that soon.

Leo: You've turned it off, but not rebooted. All right.

Steve: Exactly that. So, but the vulnerable stack was in the frontend appliances, the load-balancing appliances, of 10% of the Internet. So someone thought to scan those, and it was there. So I think it was F5 is one of the companies, and there's a different one, I can't remember. We've talked about it.

Leo: Is it much concern, though? It sounds like it's a lot of work to get kind of a little bit of information.

Steve: It's a lot of work to get a little bit of information. And, boy, some of these cookies are just crazy big now.

Leo: Yeah. I don't know what - so what? You've got my cookies.

Steve: That's why I'm not in a hurry to reboot. Well, and besides, I don't even rely on it. My own eCommerce system doesn't store anything valuable in cookies. I encrypt separately. So it's actually, for GRC it's not a problem, except that I get a C.

Leo: Is the biggest story of the year the Sony hack? I think it has to be. But despite all of this, we've just gone through the whole year, and it was an amazing year.

Steve: It's exhausting. I'm exhausted.

Leo: Yeah. And sometimes you feel like, well, it shouldn't be the last thing that happened in the year. That's just the one we remember best. And yet I have to say...

Steve: Oh, if this happened in January...

Leo: It would still be...

Steve: Yes.

Leo: ...a big, big story.

Steve: I think my question is what effect will this have for IT? We know what effect Snowden's revelations have had for the availability of security. This last year we have to thank Edward for all of this kneejerk, I mean welcome, reaction.

Leo: Right, right.

Steve: And so you have to imagine that there are boardrooms all over the country where the CEO is saying to the CIO, is this what you've been telling me we're vulnerable to?

Leo: Yeah.

Steve: I don't want that to happen. I don't want my emails getting out. And then the CIO says, all I need is money. Just I need budget and time. I've got to hire some guys, and we'll bolt things down. And, oh, by the way, you may not be able to VPN in from your yacht in the Mediterranean without using this key, this dongle that I keep trying to get you to use, but you say it's too much work.

Leo: We immediately started talking about implementing AppLocker here for that very reason.

Steve: Yeah, in fact, when I go to Windows 7, I'm going to fire up AppLocker and go to experiment with the feasibility of a whitelisting system.

Leo: See, that's the issue is a lot of stuff breaks.

Steve: Yes.

Leo: Stuff unexpectedly breaks. It's the same thing with address memory randomization.

Steve: ASLR, Address Space Layout Randomization, yeah.

Leo: Yeah. I mean, there are some things you can do, but they break unpredictably.

Steve: And DEP, Data Execution Prevention.

Leo: Same thing.

Steve: This is why it's in there, but Microsoft only has it turned on for their stuff.

Leo: Not on by default.

Steve: No.

Leo: Yeah. Because it's breaking things.

Steve: No. And remember, too, like you were never a fan of NoScript because it kept popping things up saying bloop, bloop, bloop, bloop.

Leo: Too annoying.

Steve: You're trying to execute scripts. Are you sure?

Leo: Right.

Steve: And we were always annoyed by ZoneAlarm. Whenever you installed something, you'd get orange dialogues that are saying, whoa. It's like, okay.

Leo: We have some concern about AppLocker. But it won't be implemented company-wide. It will only be implemented on certain computers because we can't implement it company-wide. So this is still a very hard problem to solve. And I frankly still think that, if somebody is determined to hack you personally, if it's a spearphishing-style attack against you, it's going to be very hard to implement.

Steve: Yeah. So minimizing the attack surface is always worthwhile. And in the same way that we switched firewalls from blocking things that we knew were bad to permitting things that we trust, I really think we're going to end - this is where we're going. We're going to end up whitelisting. We're going to end up with an operating system where it learns the things that you permit it to run, and apps are going to be signed, and signatures are going to be checked, and we'll be permitting things, I mean, everyone will feel more comfortable if we do it that way.

Leo: And yet I have to say, based on everything that happened this year, I feel like it's also hopeless.

Steve: Well, I said to you I couldn't fix Sony. I mean, I couldn't prevent that. As you said, I mean, with something that size, that many people who are going to click on links no matter how many times you warn them not to, it's like, oh, it's just a little link.

Leo: The only way really to be secure is to get offline.

Steve: Yeah.

Leo: Yeah?

Steve: Camping.

Leo: Camping.

Steve: Yeah. With no tall trees nearby.

Leo: You know, the use of drones in national parks, which is forbidden, has been going up logarithmically.

Steve: They're fun.

Leo: Geometrically.

Steve: They're fun.

Leo: Everywhere drones. I was talking to my hairdresser, she said, yeah, we were at a campsite, and this thing went bzz. She thought it was a UFO. Bzz. Pauses. Bzz. And I said, oh, yeah, that's a drone.

Steve: No kidding.

Leo: Yeah, it's everywhere.

Steve: Have you seen the Bebop?

Leo: Yeah, I'm buying - I want to buy one, but...

Steve: That's the one.

Leo: Yeah, but it's not out yet or...

Steve: I know. It's...

Leo: I was going to get one for Henry for Christmas so he could spy on this sorority.

Steve: They did a beautiful job. Beautiful, wide-angle lens, and then they, in software...

Leo: Isn't that clever?

Steve: It's brilliant.

Leo: This is from the Parrot AR folks.

Steve: The Parrot guys.

Leo: It's their newest version.

Steve: Yup.

Leo: And the camera is super wide-angle.

Steve: It's fixed so you...

Leo: Doesn't pivot or point.

Steve: Right.

Leo: But gets everything.

Steve: Yes.

Leo: And then it picks a section and corrects it.

Steve: Super-high resolution, and then so it does barrel distortion correction and - yup.

Leo: We talk a lot about drones on the show. Father Robert has a cheap drone that he's got, like, 80 of in the basement, I think.

Steve: Oh, they're fun.

Leo: Yeah, this has become the drone network.

Steve: Yeah.

Leo: Steve Gibson is the security guru, and this has been a great year for you. We noticed, I've been looking, I just kind of checked download trends. I don't pay too much attention to downloads. But your show went up 20% last year, went up 20% this year. There is huge interest in the topics we cover, and I suspect that 2015 will bring even more of interest.

Steve: Yeah.

Leo: It's going to be an interesting - we live in interesting times. You can find Steve at GRC.com. That's where SpinRite - we didn't talk about SpinRite.

Steve: No, you're right.

Leo: No plug for SpinRite today. You don't have an email or anything?

Steve: Eh.

Leo: It's Steve's bread and butter, so go buy it.

Steve: Everybody knows about it.

Leo: Everybody should know about it. It's the best hard drive maintenance utility. You must have a copy. If you don't, go to GRC.com and buy it. Everything else there is free, including the feedback form, where if you have questions we'll be answering probably next week, security allowing. That's GRC.com/feedback. Steve also has 16Kb audio versions of the show there, and handwritten transcriptions by an actual human being, Elaine Farris.

Steve: Elaine, yup.

Leo: And so if you like to read along - and this would be a good one to have the transcript of, I think. That's all there at GRC.com. Here at TWiT.tv/sn, we have audio and video, higher quality audio and full HD video if you'd like, TWiT.tv/sn. You can also subscribe to the audio or the video on any podcatch client, iTunes and all of the above. Plus we have our great apps, thanks to our third-party developers on all the platforms including Roku, which would be a great way to watch the show. Thank you, Steve. It's been a great year. I'm so glad to have you in-studio. It's so much fun.

Steve: And we're going to have fun tomorrow.

Leo: Tomorrow, don't forget, 3:00 a.m. Pacific, 6:00 a.m. Eastern time, 1100 UTC. We begin with the ball drop, midnight, as New Zealand ends 2015.

Steve: New Zealand is the first one.

Leo: New Zealand's first.

Steve: Is that 4:00 a.m. our time?

Leo: 3:00 a.m. So I come in at 2:30.

Steve: Whoo, baby.

Leo: And then go on through the day for 24 hours. There's 27 time zones, and we are very close to having somebody from every time zone. There's just a few missing. If you're in the Pacific Islands, TWiT.tv/nye. Let us know so we can get you via Skype. And we'll be saying Happy New Year all the way across. We're doing it to raise money for UNICEF. We're going to have musical performances. Many of our hosts, almost of our hosts...

Steve: Breakfast with me at 6:00 a.m.

Leo: ...will be here. Steve likes to come in early, thank god, so I'm not all alone. Those first three hours are tough. But we've planned a lot. And in fact, I don't know if you noticed, but we've got sawhorses out on the street. We're taking over the street.

Steve: Wow.

Leo: Going to have a carnival out there.

Steve: Neat.

Leo: Crazy.

Steve: Neat.

Leo: Crazy. So I hope you'll stop by tomorrow for that. And of course next week, and every Tuesday, 1:00 p.m. Pacific, 4:00 p.m. Eastern time, 2100 UTC. That's when we record Security Now! with Steve Gibson. Happy New Year. We'll see you next year.

Steve: Thanks, buddy.

Leo: Bye-bye.