SECURITY NOW!

Transcript of Episode #430

Listener Feedback #178

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-430.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-430-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here. It's a Patch Tuesday. Steve will have - or it was yesterday - has some information about that. Plus your questions and Steve's answers. We've got a lot of questions and answers to get through. So stick around. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 430, recorded November 13th, 2013: Your questions, Steve's answers, #178.

It's time for Security Now!, the show that covers your security and privacy online, with this guy, our Protector in Chief, Mr. Steven - I want to say "Tiberius," but now I know it's Maury, kind of takes the fun out of it. Steven Maury Gibson. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you.

Leo: I should check your Wikipedia. Has it been corrected, or...

Steve: So, okay. So I learned something last week.

Leo: Uh-oh.

Steve: Everyone likes having a little snippet at the beginning of the show, talking about what we're going to talk about. But it's really bad if we tell them what we're going to talk about...

Leo: Uh-oh, and don't.

Steve: And then don't.

Leo: Oh.

Steve: Because among the things that I said I would share, and I, because it was sort of superfluous, I pushed it out toward the end, was my favorite iPhone 5 case that I found after truly getting them all.

Leo: Yeah, forget all the security stuff, Steve. What about iPhone 5 cases?

Steve: And my Twitter feed went nuts.

Leo: Did it really? Oh, come on. Really?

Steve: With people, as they were, in fact, throughout the week, as they were listening to the podcast, saying hey, you never told us. And it's like, oh, okay. That's true.

Leo: Okay. Come on now, 20 people at most.

Steve: Okay, 20, yeah.

Leo: You've got 70,000 people listening to you; 20 people cared. Let's not go overboard here. So what is, what is...

Steve: Enough to tweet.

Leo: Enough to tweet. What is your favorite? Are you going to do it now, or you want to just tease us?

Steve: No. Actually, at the top of the show - I'm not making that mistake again. At the top of the show I'm going to cover all the things that I promised to cover at the end of the last show, before we start the new show.

Leo: Okay. But before we do...

Steve: So we're pulling up the tail end of last week. Then we're going to plow in, talk about the week's news. So we have all of last week's tidbits. We've got a Patch Tuesday, the second Tuesday of November in this case. We've got great Q&A, a bunch of Bitcoin happenings, and good stuff to talk about. So, yes, a great podcast.

Leo: Yeah. And you will, in moments, learn what Steve's favorite iPhone case is.

Steve: Mm-hmm.

Leo: Before you do, just what coffee are you drinking tonight?

Steve: That's just mine. That's Starbucks Espresso that I grind and then drip brew.

Leo: But which Starbucks? Which one do you buy? What's the flavor? Do you get Caf Verona? Do you get the...

Steve: No, no, no. There is nothing for espresso except espresso. It's just espresso.

Leo: Oh, okay. They don't have a fancy name for it.

Steve: No, espresso.

Leo: Okay. [Untranscribable].

Steve: And you're going to have it. When I'm up there...

Leo: I know, you're going to...

[Talking simultaneously]

Steve: ...I'm making you a cup.

Leo: Steve Gibson, Leo Laporte. You want to start with the case?

Steve: Yeah. Because that's what we didn't...

Leo: We didn't do.

Steve: We didn't wrap up last week. I said nothing was going to keep me from telling everybody.

Leo: Ah, we've got another commercial, Steve. Oh, wait a minute. There's a fire, oh, no. All right, go ahead. I won't stop you.

Steve: Okay. So for me, the case is really important. One of the things, the first thing I noticed about the iPhone 5 is it desperately wants to leap out of your hands and fall on the ground.

Leo: And you're talking a 5s.

Steve: The 5s, yeah, which I bought. And I, as I've mentioned, I switched over from a BlackBerry finally. I had a neat, sort of a really high-endurance rubber case for the BlackBerry that I liked a lot. And several times it did get out of my control and drop on the ground, and there was no harm done, thanks to having a case. So there's just no way I'm not having a case. I mean, the iPhone 5 is just beautiful by itself. But it's just dying to break. I mean, as we know, nature hates...

Leo: A perfect device.

Steve: Exactly. Sharp edges and...

Leo: It abhors a perfect device.

Steve: It absolutely does. It's always going towards entropy, and it wants to turn my beautiful iPhone 5 into something far more entropic than Apple originally designed it to be.

Leo: That's a good point.

Steve: I mean, I'm nervous holding it because it just feels like it's going to, again, just it's slippery. It's gorgeous, but it needs a case. So I set off on the quest, as I do whenever there's a new device, for a case. And the only way to really figure it out is to try them. So I truly have about 50 that I got of all different kinds. And I have a big box of them. And other people will get, like, after - the cases that I didn't like, if they want a case for their iPhone 5. I took the box to Starbucks one morning because there were a bunch of people who had iPhone 5's with no case. And even their phones were making me nervous, just like 10 feet away I was worried about their phone because it's like, oh, my god, look at that. It's gorgeous, but it's trying not to be. So I gave them, I said, here. It's like, remember in the old days when you used to go to the dentist. You could pick a toy out of the big...

Leo: Yeah, the treasure chest, yeah.

Steve: The treasure chest, exactly. So I said, here's cases I'm not using. Which do you like best? And so happily now everybody at Starbucks has their iPhone 5's covered in a case that I'm not using.

Leo: That's funny.

Steve: Which they're quite happy with because they love the price, which of course was free. For myself, I settled on the ultimate case. After trying all the cases that Incipio, I-n-c-i-p-i-o, that's the company - and actually I really like their cases in general. They've got, I mean, they go way overboard, though. They've got some that, like, are rated to 30 meters below the waterline. You can dive with it. Or it can fall in the toilet when you're using your phone at the wrong time, whatever. Those, however, you feel like you can't even reach your phone any longer. It's a miracle that the touchscreen works through this thing because, I mean, it's like dragging a tank around with you. So we don't want that. Other bad cases are flimsy, or there's a new trend. I like the feel of rubber. I don't like the feel of that silicone. It's just a little too greasy feeling. Anyway, so the correct case is the Incipio DualPro. They call it a DualPro because it's actually - it's two parts. It's got an inner lining, which is very silicone-y/rubbery, and so you fit that around the phone first.

Leo: I hope you got the pink one.

Steve: For Jenny. Jenny got the two-tone pink, that one, the one that's on the screen right now. That's the one I got for Jenny.

Leo: And you got, I'm thinking, black and gray.

Steve: No, I got black and black. They actually have black on black.

Leo: Oh, pardon me. I was a little too fancy. I'm sorry.

Steve: Yeah, well, black and gray, somebody else got that, someone I - I don't think it was Mark.

Leo: I like the black and red. I'd get that one. So the inner case has color, and then the outer case a shell.

Steve: Yes. And so the advantage is, first of all, it doesn't have that slippery silicone-y feel, which isn't grippy enough. You want something that's going to - just sort of wants to stay in your hand, rather than escape from your hand. And so anyway, that's the one. The inner lining gives it good shockproofness, and the outer lining makes it feel firmer than if the whole thing was just shockproof. So that's the one, Incipio DualPro. Oh, and on Amazon it's, like, $8.

Leo: What?

Steve: $8.34 or something. It's very...

Leo: Oh, the list is 30, which is fairly reasonable for a case.

Steve: I know. Yes. And Amazon has it for 8 or 9, like less than 9, I think it's 8-something.

Leo: Excellent. All right.

Steve: So that's it. Now, the other thing that happened that I had in my notes from last week is that I was recommending the Calomel add-on for Firefox because those guys were - did you find it there for, like...

Leo: $8, $8.05.

Steve: Yup, that's a bargain, baby.

Leo: Wow. That is a good deal.

Steve: Grab it. It's a great case. That's my chosen case. Although now I'm looking over here, and these people we were talking about before, those Tylt people, the T-y-l-t people, they've got some, too. So it's like, oh, darn it, got to get one of those.

Leo: See, this is an addiction that never ends. You might as well - seems a shame. You've got such a beautifully designed phone. Jony Ive's just got to roll in his grave. Even though he's not dead.

Steve: I know. Except, I mean, and it is, it is - in fact, every time I was changing cases, there was a moment where nature was conspiring against me. Am I going to drop this gorgeous piece of...

Leo: You know, my kids never have used cases, and they drop them all the time, and they smash them all the time. And I beg them, I plead with them, I yell at them, I say you must. Daddy won't buy you another phone, you know, everything. But they don't want - the kids don't want cases. They want to show off, I guess, what they got.

Steve: It is gorgeous.

Leo: They dress like that, too.

Steve: And by the way, you know that the least, the least popular color of the iPhone 5 turned out to be the gold. It's like, almost no one wants the gold.

Leo: Of course, that's what I bought, and everybody I know bought.

Steve: Sarah got one, I heard she was saying that.

Leo: Yeah, I have gold.

Steve: And black, black is more than half. The, what is it, then white is like a third, and then gold is the remainder. So, yeah.

Leo: I didn't realize it was so - huh. It might be too ostentatious for some.

Steve: So the Calomel add-on for Firefox is cool because it shows you about perfect forward secrecy. It also rates GRC's security as, like, awful.

Leo: Who? Who?

Steve: It's like, ouch. So after I recommended it, people began sending me email and tweets saying, hey, why is GRC's security so crappy? And it's like, okay. Unfortunately, a company that's going to be making a big deal about security is all about finding something wrong. Because if it just says everybody is wonderful, you're going to start saying, oh, well, okay, why am I running this?

So here's the problem, is it's caught us in this dilemma. We've been in this dilemma for a while, where you had to choose between perfect forward secrecy or being immune to the BEAST attack. And it used to be that SSL Labs - so, first of all, none of this is really about what's secure or not. I mean, the fact that we're not offering, that GRC is currently not using preferentially a perfect forward secrecy cipher doesn't mean that our security is crappy. It means, like, nobody else is, either, but we're not. And arguably, okay, GRC should be.

Instead, we've been protecting people from the BEAST attack, which is also, like, dumb because you have to send millions of connections and variable-size packets and go through all this ridiculous stuff to create this theoretical BEAST problem. SSL Labs used to be rating people who did not prevent the BEAST attack poorly. So I put a BEAST attack mitigation at the top of GRC's cipher suite so that SSL Labs would give me an A, which we now have. Unfortunately, Calomel gives me an "oh, my god, why are you even bothering" rating because they rate perfect forward secrecy higher.

So I'm unable to keep everybody happy, except that SSL Labs just changed their rating and decided, okay, BEAST is not a problem anymore because all the browsers support it. And in fact, with Mavericks, the Safari browser was the last holdout where the browser wasn't handling BEAST attack mitigation on its own, which it is now. So that allowed SSL Labs to change things around at their end and downplay the importance of BEAST.

So GRC now needs to, again, play this ridiculous shuffling game of cipher suites to put perfect forward secrecy ciphers, which are the ones that use ephemeral Diffie-Hellman key negotiation, at the top of its list. So I'm going to do that. Except that I hate rebooting my server because it takes GRC offline for several minutes because servers are now so slow to reboot that that annoys me. And I haven't had to reboot since sometime in March. So I'm reluctant to do that, but I will.

So that's the whole story, for anybody who's worrying about why GRC apparently has crappy security. We don't. It's just that the Calomel people are very unimpressed with the fact that we're not offering perfect forward secrecy, and we are offering BEAST attack mitigation, although now all the browsers are doing that for the user so the server doesn't have to. So I'll get it changed.

Leo: How hard is it to implement perfect forward secrecy?

Steve: Nothing. It's just - you just change your cipher suite order around so that the server agrees to offer those at its preference. And then the browser says, oh, look, they're offering this. So we'll take that.

Leo: Awesome.

Steve: Yeah. Not hard at all. Also I promised last week to talk about my feelings about the iPad Air. I love it. I absolutely do. I think it is great. The mini went on sale yesterday, and I tweeted that news to everybody, and a bunch of people who were following me didn't know that, and so they ordered their mini. I ordered one because I need to see which I like best, the iPad Air or the mini. They have the same resolution in terms of pixel count. The mini is just obviously smaller and lighter. So I just - there's no way to know in the Apple store. You hold it, and it's like, oh, look how small this is. But you have to use it for a while to get a sense for that. So I will let people know. It's like five to 10 days delivery they're quoting when I ordered it. So we'll find out.

And last on my list, actually second to the last, is a couple weeks ago I mentioned SpinRite's real-time data viewport that allowed you to actually see the data on your drive. And it was a cool way to determine whether the drive had been wiped because on a non-wiped drive, you'll actually see the data flashing by the window. Many people commented that they had never realized that and liked that fact.

So I just wanted to follow up and mention that you can also, one of the features of SpinRite 6 is you can tell it at what percentage of the drive you want it to start, which allows you to use this viewport window, and that, to quickly check, like, the middle of the drive and toward the end of the drive, just to make sure that it all got scanned. Because remember we were detecting lazy employees who were not scanning the whole - who were actually not scanning the drive at all, they were just eliminating the partition table and maybe the directory or something at the beginning of the drive. They were doing some small little delete at the beginning which was not protecting their employer's data. So you could interrupt SpinRite and then restart it at 50%, take a look, like look through the little window, the magic looking glass, to see what the drive looks like there. Then interrupt it, go to 99.9, and look at the end of the drive just to see whether the whole thing was wiped out. So a little usage tip for people who like that little viewport.

And finally, I also promised that I would give people an update on the SQRL project.

We're a week further along. We're continuing to come along beautifully. Pretty much everything has been agreed to in the group. We wrapped up the questions of what we were going to do for v1.0 for phishing and man-in-the-middle attack mitigation. The format of interchanging arguments back and forth has been arrived at. And now I'm working on updating GRC's web pages to be current to what has been agreed. We only then need to resolve the detailed interaction protocol, and then it's time to start writing code.

There is a wiki which is up that is being independently maintained by a bunch of the guys who are participating in the newsgroup, but also sort of doing sort of a more formal-style specification than I am. I'm sort of more tutorial and more graphics and sort of expository approach to this is how it works and what it does. So we are continuing. It's got my fulltime attention. We're working to just nail down the final aspects of the specification, and then I and everybody else who wants to do their own versions will be writing code to support this logon system. And everyone is quite excited about it.

Leo: That's neat.

Steve: And I had in my notes something that I didn't get to last week because it was also sort of at the end. And I wanted to thank our listeners on Jenny's behalf because apparently they were just wonderful with, like, following up on the news of the book that she had published. Remember that she had a book published, actually, and I talked about it when you were on vacation, Leo, titled "Is God Real or Pretend?" And one of our listeners - she got a bunch of email from listeners mentioning the fact that they were listeners. And I guess she has her email address, like, at the end of the book. And so they were writing to her. And she asked if they would be so kind as to post those as feedback on Amazon.

And so one of them I just wanted to share from a listener because it was so neat. Someone, whoever you are, said - their title was "No wonder this is a bestseller." This was dated October 23rd. And they wrote, "'Is God Real or Pretend?' is such a brilliant concept to begin with, and so smartly executed. To have a young boy searching for the answer to this age-old question with members of his own family having vastly different opinions is a fantastic premise. On top of that, Ms. Horsman has written a book for everyone that she so cleverly camouflaged as a children's book," our listener of Security Now! said, "I learned several things I never knew before. I've never read a children's book that deals with such an incredibly heavy topic, let alone written in such an easy-to-understand style, with commonsense conclusions." And this reviewer goes on.

But anyway, I just wanted to thank our listeners on Jenny's behalf for being so neat about that. I really appreciated it, and she did too. News, my friend? You ready for some news?

Leo: Yeah, why don't we - I detected the pause. And I think this might be a good time. We have questions.

Steve: We do.

Leo: We've got news. Why don't we, yeah, let's do the news. I have two more commercials. I have an Audible and a proXPN. So I think after the news we'll do the Audible. How about that?

Steve: Okay.

Leo: All right?

Steve: Okay. So this is important. I tweeted this a couple days ago. This is a growing problem that Microsoft did not deal with yesterday in their second Tuesday of the month, Patch Tuesday. And that's this tagged image file format zero-day flaw which is ramping up rapidly in the level of exploitation. I wasn't aware, but you were, Leo, and many of our listeners were, that the TIFF file format is in such heavy use now. I'm just sort of seeing, I guess, GIF and JPEG, or GIF, depending on how you pronounce it, and PNG file formats. But obviously TIFF is still very popular.

Writing for Information Week, Mathew Schwartz said: "Warning: Attacks against a zero-day vulnerability in Microsoft Office are more extensive than first believed. That finding further reinforces security experts' recommendation that businesses install an emergency mitigation technique released by Microsoft as quickly as possible." We did talk about it last week. I wanted to remind people that I created a bit.ly link, bit.ly/notiff. That will take you to the Microsoft page where there is one of their little, quick, one-click Fixit buttons, which simply adds a line to the registry, making it very easy for anyone to do. And that line disables the TIFF format codec.

So what's happening is we didn't get a fix yesterday for that. We did get a different IE zero-day fix that I'll talk about in a second. But this one is still a problem. So if you're not a person who is using TIFF format images, it's probably a good idea, there's really no reason not to disable it. When Microsoft does their patch, they will remove this temporary fix from the registry and fix the problem. And I'm sure we'll get that in December's Patch Tuesday, if not before. I mean, they may do an out-of-cycle update because this thing is really causing problems and is ramping up. So that could certainly happen.

But for now I wanted to tell people that the security community is getting more and more concerned about this because we're seeing the incidences of this happening. And it is trivial to exploit. That's the problem. All you have to do is get an image to be seen. So email with a TIFF image embedded in it; Office documents with a TIFF image. I'm not sure about drive-by IE. But people are just being too vulnerable to this. So disabling that would be a good thing.

And we are second Tuesday of the month. We got eight patches from Microsoft addressing 19 vulnerabilities. Thirteen of those 19 were the worst kind, remote code execution, high priority, no action required on the part of the user. So it would be a good idea to update yourself. One of these things was something we haven't seen for a long time. That was a WordPad exploit. It was in the GDI, the Graphics Device Interface layer, which unfortunately Microsoft, as we've talked about before, moved down into the Windows kernel for the sake of efficiency, but which makes it much more prone to exploitation.

So you want to just - essentially, this is not a big set of patches, but they are important. And one for IE addresses a brand new zero-day flaw which was just disclosed, but yesterday the exploit details appeared on Pastebin. So the fact that the exploit itself is public worries people a lot more, and they're expecting to see this also ramp up very quickly. So the advice in the security community is do not delay on implementing these any more than you have to. And Microsoft is now prioritizing these, and the IE patch is among the top three highest priority recommendations because it's expected to be seen in high exploitation soon.

We got also a Flash Player update from Adobe. We're now at 11.9.900.152. IE10 and 11 on Windows 8 will update automatically. We know that Chrome updates automatically. To check whether you're updated you want to go to Adobe.com/software/flash/about. In Firefox it showed me that I was not at .152. I was at .11 something. So I will need to get myself updated. And people who are not protecting themselves, the only reason Flash ran for me, because I'm running NoScript, is that I'd already trusted the Adobe.com site to run things in it, so it did. People who are protected by NoScript really don't - they have less to worry about.

Bitcoin. Gosh, lots of news. Have you seen the value of a bitcoin, Leo?

Leo: Last I checked it was 260 bucks. What's it now?

Steve: Seven...

Leo: What?

Steve: I'm sorry, not seven, 417. But I just...

Leo: Oh, I see 429 was a high.

Steve: Yes, 428 was when I looked.

Leo: Holy cow. What is going on?

Steve: It's not clear what's going on. It was 350 on Friday. Now we're at 428, 429. It's really cranking along.

Leo: I've got to look in my wallet. You've got 50?

Steve: My 50 bitcoins are worth something now.

Leo: But like any investment, the timing's everything. Do you sell now and watch it go up, or do you...

Steve: Well, that's just it. It's always worth noting. I think some - maybe someone - I think somebody quoted Kevin as saying, you know, our Kevin, as saying that he was selling at 350. I think that might have been what it was. And of course now we're at 429.

Leo: We have a bitcoin donate box, as you know, on the front page. And I haven't checked in a while. My balance is now 7.3 bitcoins. So I'm rich. I'm sorry. Wow, that's crazy. Of course now that I'm off the meth, I don't really - and Silk Road, you know, is closed, I don't really have anything to do with them, but...

Steve: Yeah.

Leo: I guess you could buy cupcakes in San Francisco with bitcoin, so that's a lot of cupcakes.

Steve: Or you can use them to donate. The EFF takes them again.

Leo: That's right, that's right.

Steve: So that's a nice thing.

Leo: I already give, I can't remember what it is, a couple hundred bucks a month to EFF, so...

Steve: Here's the problem.

Leo: In real American dollar.

Steve: Bitcoins have become money, and people are having a hard time holding onto them online. There was a major breach last week, $1.2 million, which is now 1.5. So they didn't denominate it in bitcoins at the time. It was 4,100 bitcoins. And this was an online exchange called Input.io. Now, the problem is we know that it's difficult. I mean, security is hard. That's the overriding topic of this podcast. Now you've got the typical problems, I mean, we had a lot of fun at Adobe's expense last week. And, I mean, they deserved it because their password technology was so lame. I mean, it was so badly broken. But this is Adobe. So here we've got some random Input.io bitcoin exchange. Who knows who they are, what their security policies are, how good their backend stuff is. Well, apparently it wasn't good enough because they lost 4,100 of their customers' bitcoins.

Leo: Whoops.

Steve: Whoops, yes. And the guy said, I'm sorry, but I don't have that many bitcoins. I will do what I can to make the best of this. I've got 1,540, and I'm willing to pay my customers back, what, a quarter or so.

Leo: Wow.

Steve: But that's all they could do. So then a frequent tweeter friend of the show, Ian Beckett, sent me a note about [a news item from] PandoDaily. [GBL] is a fraudulent bitcoin exchange, a Chinese bitcoin exchange who cost clients - and this was, again, this is not in bitcoins, but this was in dollars. At the time, this was I think yesterday, or maybe the day before, might have been Monday, $4.1 million in fraud. So this was a fraudulent exchange that set up shop, said, hey, we're a bitcoin exchange, put your bitcoins here. And at the time that they had $4.1 million worth of them, they just went off the 'Net. They said thank you very much, and they disappeared.

Leo: It's like a honeypot, really.

Steve: So the lesson, yes, the lesson is do, I mean, everybody, store your own bitcoins in a machine, preferably not one on the 'Net. I mean, this is real money now. This is becoming serious. So you do not want your wallet, I mean, there are, like, online wallets. Bad idea. Do not trust an online company with your wallet. Unless your mother is a security genius, and you would trust your mother with your money. But you're just not - you don't want to trust some, I mean, this is real money. It's one thing to lose your identity. It's another thing to lose, you know, what are my 50 bitcoins worth now at $430. That's serious coinage.

Leo: Yeah. Wow.

Steve: So, yeah. I would say to everybody it's becoming serious when bitcoins are worth real money.

We had some humor from the Twitterverse that I wanted to share. A Kevin Meagher, M-e-a-g-h-e-r, tweeting as TheKevinMarr, M-a-r-r, he said, referring to last week's Adobe password fiasco, he said: Steve, you have answered the age-old question: Ginger or Mary Ann?

Leo: Okay.

Steve: And you have to be of a certain age to understand the reference to the question.

Leo: We're talking the two comely women on "Gilligan's Island."

Steve: "Gilligan's Island," yes.

Leo: One who was a movie star, the other who was a country girl.

Steve: Yup, Ginger or Mary Ann.

Leo: And Ginger is the movie star, Mary Ann the country girl.

Steve: So Kevin noted that Ginger made it onto the list. Ginger was 94, and Mary Ann was nowhere to be found.

Leo: Just like in the show's opening theme. "The movie star, the professor, and Mary Ann." They had to add that later. It used to be "and the rest."

Steve: So, and our frequent contributor, this is not related to the podcast, but Simon...

Leo: These are in passwords? People were using Ginger and Mary Ann in passwords? Or was it Ginger and not Mary Ann?

Steve: Yeah, Ginger was a password. Yes. Ginger made it. She was 94. Not as popular as Monkey, so...

Leo: I'm thinking Ginger is somebody's dog's name, and that's why it's so popular.

Steve: That's probably it.

Leo: Sounds like a dog's name, doesn't it?

Steve: If you name your dog Monkey, there's probably something wrong with you.

Leo: And not many people have dogs named Mary Ann. Ginger, though.

Steve: Ginger is probably a more popular dog name, yeah. So Simon Zerafa, just out of nowhere, I don't know where he comes up with this stuff, he said @SGgrc, so he mentioned me in his feed, he said, "As a child, I was obsessed with the difference between sine and cosine. As I got older..."

Leo: That's one weird kid.

Steve: Yeah. He says, "As I got older, I realized it was just a phase." So...

Leo: John didn't like that joke.

Steve: And I always have...

Leo: Geometry humor, there's nothing like it. Trigonometry.

Steve: Yeah. Well, and then I told him, I said, "I think I'm going to use it on the show, Simon." And he says, "Well, just don't go off on a tangent."

Leo: Oh. Oooh.

Steve: Ba-doom-boom.

Leo: Ba-dum-bum.

Steve: Yeah. So I did get, and I haven't shared with listeners for a quite a while, a testimonial. This was a good one that I thought was interesting, and there's a moral to the story also. This is from a listener of ours, Tyson in Texas. I ran across it this morning dated the 9th of November, so it was last Saturday. And the subject was "SpinRite saves the year." And I don't quite understand the subject line, but he wanted to get my attention, and he did.

He said, "Hi, Steve. I just wanted to share with you an interesting little SpinRite story of mine. I purchased a copy of SpinRite a few years ago after hearing you talk about it in an early episode of Security Now! and have used it many times since to bring failing hard drives back to life. On one occasion, a friend brought his laptop to me, saying that it would no longer boot into Windows. In fact, it simply said 'No bootable device.' He said that this was his work laptop, which contained all his documents and files pertaining to his business. I asked him if he had a backup of these files somewhere else, and he said that he did not. Oops.

"Of course I knew immediately that I was going to run SpinRite on the drive, but wanted to first back up any files that I could access in case the drive was so far gone that the very act of running SpinRite might push it over the edge, and it would be gone forever. The drive did appear in the BIOS, so I booted the laptop using a Windows recovery CD and tried accessing the drive through a command prompt to see if I could at least verify that his files were still intact. But the drive was nowhere to be found. I tried again using a bootable Linux CD. No hard drive found. I then removed the drive from his laptop and attached it as a slave to my desktop PC. Windows would not even acknowledge that the drive existed.

"Finally, I loaded up SpinRite. It saw the drive and began running very, very slowly. After several hours, SpinRite had not even completed 1% of the drive, but the bits were still churning away, so I knew it must be doing something. I told my friend that the only option I could see at this point, having tried everything else, were to either give SpinRite all the time it needed to attempt recovery, or say goodbye to his files forever, for which there was no backup. He agreed to let me keep his laptop until SpinRite either completed the process or got stuck trying.

"We set the laptop aside in the corner" - oh, and so he put the drive back in his laptop and then restarted SpinRite on his laptop. He didn't specifically say that, but that must have been what happened, letting it just run in the corner of the room - "and left it to run overnight. When I came in the next morning, to my surprise, SpinRite was still running and had now completed about 2% of the drive. Nevertheless, the status showed that the bits of the data were still being read, so I continued to let it run, day after day after day. After about two full weeks of continuous operation, SpinRite had churned through about 50% of the drive and showed a TON [he has in all caps] of red, unrecovered sectors. With nothing to lose, I continued to let SpinRite run, glancing over its progress every day or two.

"Finally one day I walked over to the laptop and saw SpinRite had actually completed. The process had taken just over one month. I restarted the computer and held my breath. To my amazement, it booted straight into Windows without ANY [he has in all caps] trouble, and ALL [in all caps] of my friend's business documents were present and undamaged. I quickly backed everything up to a flash drive and then burned a second backup to a CD. I advised my friend to buy a new hard drive since this one was bound to give out at any moment, and also suggested that he start making backups of everything from now on.

"After this experience, Steve, more than ever, I am a true believer in SpinRite. It may have taken over 800 hours of continuous operation, but it COMPLETELY [he has in all caps] recovered a hard drive that appeared to be totally dead and hopeless. Not only did it recover the important documents, but even allowed the system to boot as if nothing had ever gone wrong in the first place. Thank you for this amazing program. I'll be buying your new upcoming version of SpinRite as soon as it's available." Actually, it's going to be free for him since the next version will be a free upgrade for everyone. And he signed it "Tyson from Texas."

So I just wanted to say to people that that kind of lengthy recovery is very unusual. Typically it's a few hours, not hundreds. And the other thing is, I mean, this is an instance where the first thing I think of is, oh, my goodness, if this person had only been running SpinRite from time to time, this level of catastrophic damage would have never had a chance to accumulate. A laptop is a rough environment for a hard drive. It's just inherently getting bounced around. And if there were this kind of damage spread across the entire drive, again, running SpinRite every, like, every quarter, every three months, would only take an hour or two and fix problems before they have a chance to get this advanced. It is the case that if it is in this horrible condition, and you've got time, SpinRite will typically repair it, as Tyson found out. But, boy, preventative maintenance, especially for a laptop, really does make sense. And here's another instance of SpinRite doing the job.

Leo: To the rescue. We have questions; you have answers.

Steve: Two things. Somebody tweeted while you were doing the Audible sponsorship. They were asking, with all of these bad bitcoin exchanges out there, what do I - are there any good ones that I would recommend? And the advice is to use the exchange for exchanging between bitcoins and currency, but do not use it to store your bitcoins. That is, pull them out and essentially take them offline because you really need virtual currency to be kept somewhere under your control, and preferably in a machine that's not even on the Internet because, as we all know, malware, I mean, there's no question that malware will start looking around in machines for bitcoins.

Leo: For bitcoins.

Steve: That's just too valuable.

Leo: And all they need - what do they need if they wanted to steal my bitcoins? How would they steal my bitcoins? They steal the file? Because there are certain files associated with my wallet.

Steve: Yeah, and the wallet is encrypted, and so, yeah. If you have a good password, that's the other thing you want is you want a very, very strong password. We've got a great question we're going to get to. Remember I mentioned last week that I was tempted to call the episode "256 Bits Is the New Black." That's another thing we didn't get to, but I used the question in today's Q&A. So we'll be talking about why 256 bits is enough bits because bitcoin, a user's bitcoin address, essentially, is 256 bits. That's also the BitTorrent sync address, and it's also the strength of the master key in SQRL. So I've looked at 256 bits and what that means extensively. And we're going to once and for all put that one to rest.

But I also wanted to mention, and I forgot, a really interesting report that was just published, it was actually on the blog of the Backblaze people. Backblaze is a major - and you may want to click on that link in the show notes, Leo, if you can, and bring up - they've got some great charts, really interesting analysis. Backblaze is a major cloud storage provider. They're unlimited cloud storage. They've been, over the course of several years, they've put 25,000 drives online, which they now have spinning, so they've been able to acquire a really good, evolving set of statistics, very much the way Google has with Google's big indexing project, of the life of drives.

And what they found, they've got some - there's a really cool graphic that shows sort of like three stages: Year 1, Year 2, and Year 3. And what they've determined is that 80% of drives last four years. Which is to say that 20% of drives will die during the first four years of life, and 50% of drives die by year six, is the other thing that they have found. And there's an interesting - they also graph over the first three years. By the way, the link is long. If you went to blog.backblaze.com I'm sure you could find it because it was 11/12 [2013] is the date of their blog. Yeah, there's a neat chart there that you have on the screen now showing the nature of infant mortality where drives die frequently when they're new, but then they sort of burn in, and their death rate drops. And then, as they get older, their death rate goes up again.

[blog.backblaze.com/2013/11/12/how-long-do-disk-drives-last]

Leo: This matches pretty closely Google's results on its longitudinal drive study.

Steve: Yes, yes. And that other - the chart that I really like shows the three years - Year 1, Year 2, Year 3 - where in the beginning of Year 3 the rate of death begins to go up again. Drives begin dying. But I did think it was also interesting that 50% of drives die by year six. And again, I would love to take SpinRite into their facility and get some sense for the nature of drive death, what do they mean by that, because we do know that preventative maintenance performed on drives is fabulously successful. I've got, you know, obviously I've been selling SpinRite now for more than 20 years. And there are people where, very much like people who take Vitamin D and they no longer get sick, although everybody around them is sick, there are people who are using SpinRite on their drives, and theirs never die. Whereas they're, like, fixing other people's drives all the time because they're not running SpinRite. So it really is effective preventative maintenance.

Leo: Yeah, but you've got to figure a company like Backblaze, it's not worth their time or the risk of trying to recover drives. If a drive...

Steve: Exactly.

Leo: And that's why these numbers are skewed a little bit by their lack of tolerance for any failure. Any error at all, they're going to throw it out.

Steve: They yank it out and slide a new one in.

Leo: I'm sure Google does the same thing.

Steve: Yep.

Leo: Google's results very, very, very similar, if you look at their annualized failure rates, broken down by age groups. They maybe say it starts dying a little sooner. It sounds like Backblaze says four years. Google says that the drive failure rates start to go up pretty rapidly after two years or three years.

Steve: And you know, Leo, I'll bet that the reason is Google probably works the heck out of their drives.

Leo: Oh, yeah. They're on fulltime, yeah.

Steve: Yes. So a big, well, a global indexing system is probably thrashing its drives; whereas a cloud storage facility, the drives are probably just spinning, but not moving fast.

Leo: Unused, yeah.

Steve: Yes.

Leo: That's a good point, yeah. Although Google does correlate utilization rate with failure rate. So there's some interesting stuff. Both of those are really worth reading. I'll leave it to you to summarize what they mean. I'm not sure. Do you have a favorite drive manufacturer?

Steve: You know, they keep getting bought. I loved Maxtor. I loved Quantum. They're both gone.

Leo: It's basically Western Digital, Hitachi, and Seagate. Those are the three companies now.

Steve: Yes, yes. And Hitachi bought IBM. IBM had really good drives. I think Hitachi's very good. I have an anti-Western Digital bias that I cannot justify, and it's not fair.

Leo: You're not alone, by the way. A lot of people share that.

Steve: Yeah. I think they're the most consumer - I don't know. I just - I don't use Western Digital. I buy Seagate or Hitachi. But I don't think that's fair. I mean, it's not - I know I will hear from people saying I've never had a Western Digital...

Leo: Each of them have problems. Western Digital had some really bad BIOSes for a while that were a real problem. And I think that soured a lot of people on Western Digital.

Steve: Yes. And there have been, you know, all of them go through phases where they've got, like, some process problems, or they'll have like a batch of bad ones that hurt people.

Leo: I think it's a commodity at this point.

Steve: "Commodity" was the word I was looking for.

Leo: Yeah. I think that there's not much - they're like pork bellies. One's pretty much like the other.

Steve: Yeah.

Leo: I have questions.

Steve: Yay.

Leo: Do you have answers? Let's find out.

Steve: We do.

Leo: Mr. Steve Tiberius Gibson. By the way, they took that out of your Wikipedia entry. Now it just says Steve Maury Gibson.

Steve: That's probably good.

Leo: Hey, did Tiberius show up in that list of passwords? Probably not.

Steve: But I wouldn't use it.

Leo: Not for you.

Steve: What that shows us is you have to get a random source. I use the junk that LastPass generates.

Leo: Yep. It's so good.

Steve: But all of my WiFi passwords I got from GRC. I just copied a string off of passwords.htm at GRC, and that's what I use because nobody is ever going to reproduce that. Nobody. It's impossible.

Leo: I use very weak WiFi passwords.

Steve: It is a pain the ass, though, setting up a new machine.

Leo: Yeah. I use really weak, really weak passwords. They're not monkey123, but I use weak passwords on my WiFi because nobody - how are you going to attack that? You have to be in physical proximity. I'll see him sitting on the curb going let's try this, let's try this.

Steve: Well, yeah, but for me, I can't let anybody into my network.

Leo: No, you're different.

Steve: Yeah.

Leo: Bob Hart, Medford, Oregon, writes: Hi, Steve. You always provide an entertaining and informative show, and last week's was great as always but left me with a question. So now I know that Adobe's poorly encrypted password database and source code was compromised, but the encryption key that they used is still secret. I can see that a string of encrypted data was the same in a lot of cases, but how do we know that "Monkey" corresponded to that string without encrypting it using Adobe's encryption key? I must have missed something. Clarification would be nice. And thanks for SpinRite for keeping my disks healthy.

Steve: Okay. So we do not know that "Monkey" relates to the encrypted string because, as Bob comments, we do not know what the key is, and we probably never will. We have to assume that Adobe chose a really good random number just one time, and that's the static key for their crypto. We know that there's only one key because we can see the correspondence between people's encrypted version and their hints because the hints were not encrypted. They're in the clear. Which is dumb, really, because obviously Adobe, since it's reversible encryption, Adobe could have encrypted the hint and then decrypted the hint when it was necessary to provide it to the user. But, I mean, there's no understanding what Adobe was thinking when they created this.

So the way we know that it is symmetric cipher is the hints correspond to the same cipher text. The reason we will never know what the key is, although, wow, we would love to because there's lots of hints that are not clear or blank hints, and if we knew what the key was, we would instantly have every single password, even the really strong ones. Remember, the only passwords that we have are the ones that were so weak that they were used so often that we could then jump across and use the hints that people used to link all of them together.

So the reason we will never know what the key is is that, if our assumption is correct, that it's 3DES, and that's a reasonable assumption, the block length being 64 bits is the giveaway because DES is a 64-bit block, they couldn't have used a single DES. That would be crazy. That would just be a 56-bit key because that's the key length of the 56-bit block encryption DES. Probably they used 3DES. So that's three 56-bit keys, one of those 56-bit keys for each round, each usage of or application of DES in turn. So that's 168 bits. That's a lot.

We'll be talking in a little bit here in a minute about 256 bits and how big that is. But 128, it might as well be - it's out of reach. Remember that AES itself, the AES cipher that was recently standardized on is often used with a 128-bit key. So that is regarded as as strong as we need. So 128 bits is already beyond cracking. 168 bits is 40 more than 128. 40 more means 2^40 stronger. Well, 2^40 is about 10^12. So that's a million million times stronger. So 168 bits, which is what Adobe's probably using, if they use 3DES, is a million million times stronger than 128 bits. And that's already strong enough for SSL and for, like, all the things that we're currently protecting with the Rijndael AES cipher.

So we're never going to know, unless Adobe leaks it, or it was in their source code or something, we're never going to know what the key is. So for really, really strong passwords, we have no clue. But for the weak ones, since so many people reuse the same password...

Leo: Well, and their password hints gave it away. This is where the failure was. The password hints were in the clear. And it turns out, apparently, there's a misunderstanding about a password hint, a widespread misunderstanding that the password hint perhaps should contain the password [laughter].

Steve: Or the hint should not be "Rhymes with assword." That's a bad hint.

Leo: But so many of them said "The password is...."

Steve: Yeah. And apparently this was not a high-value account, by the way.

Leo: Well, somebody pointed that out. A lot of people said you had to make an account if you wanted to download trial ware. So people didn't care.

Steve: How dumb.

Leo: Yeah.

Steve: Yes.

Leo: So we don't know, out of the, what was it, 130 million accounts that were leaked out, how many of those were high value. My account was because I had a credit card associated with it because I bought stuff from it. But I used a strong password, so...

Steve: The problem is that what the guys were getting was your email address and often a password because somebody else was leaking your password by virtue of their bad hint on the same encryption. Then people - in fact, Facebook did this. I never had a chance, I saw this pass by, but I didn't have a chance to track it down. As I understand it, Facebook was looking at that repository, seeing whether they had the same email address as somebody whose password was leaked, and then telling you you had to change your password or something. I didn't - did you follow that, or see what that was, Leo, that Facebook did?

Leo: No, but that's clever. I didn't know that they had done that.

Steve: I thought that was very proactive of them.

Leo: Yeah. Go out and look and see if an email address is the same as a member's email address; and, if it is, send them a note saying you might as well change your password. They didn't do it to me, but - hey, by the way, I did get an email from Joe Siegrist at LastPass. Because remember last week we gave out the very nice feature that LastPass did at LastPass.com/adobe, where you could search the database. But what Joe did that maybe he didn't, you know, wasn't thinking about it, was it would then, if you were found in the database, send you an email at that address. Well, of course any email address could arbitrarily be entered into that search, and mine was, by many others. So I got a lot of emails.

Steve: To see whether your email address was part of the database.

Leo: Right. People were checking my email address, probably, you know. So Joe said, "Just wanted to apologize we hit you with spam. It won't happen again. Love the show, guys. It was a good one yesterday, and thanks for the continued support." So thank you, Joe. That's - yeah. And you know me, I love LastPass. There's no worry about that.

Steve: And I'll mention, Leo, that I had a lot of feedback saying that they really liked last week's podcast. Last week's was one of those, just so much news to talk about, where we went, did a lot of depth on a lot of topics. And when we do that, it's the time I see the most positive feedback.

Leo: Oh, sure. We have a lot of geeks in the audience who want to know, and they care, yeah.

Steve: Well, we got one now.

Leo: Here's your geek. Are you ready? From Twitter, Wayne T. Taylor. He's a 140-character geek.

Steve: Whoops.

Leo: Is that wrong? Did I skip one?

Steve: Yup.

Leo: Well, let's not skip two. That was Question 1. Bob Arles, @metaRobert on Twitter. @SGgrc: BitTorrent Sync - I love it. They have to do this in such cryptic form. BitTorrent Sync problem? If I start guessing secret keys, am I not effectively trying it against all clients with each try? Yes, you are, of course. Yes.

Steve: Yes. Now, this is where I wanted to talk about 256 bits. It unnerves people, the idea that BitTorrent Sync has for your address a randomly chosen 256-bit token, and that's your identity. That's what I'm using, as I mentioned before, for the user's identity on SQRL, my proposed login replacement. That's what Bitcoin uses as your identifier for Bitcoin. That's your unique thing. And so people say, yeah, but what if there's a collision? What if I get the same one? Then I'm going to have access to all of those files of the other person who has the same one. And it's like, okay.

So that's true, first of all, absolutely true. If two people share the same, exactly the same, not one single bit different, exactly the same 256 bits, then for all intents and purposes, for BitTorrent Sync, for Bitcoin and for SQRL and anything else using 256 bits, you're the same person. There's a collision. So this is the so-called "birthday attack." The point of a birthday attack is it asks the question, in a population of people having some number of possibilities, what's the chance, the probability that any two of them share the same birthday? If we're in the case of birthdays, with 365 days in the year, what's the chance of a birthday collision? In the larger case, in the case we're discussing with 256 bits, that's a lot. There's a lot of possibilities. So the question is, what's the chance of a collision? And I want to, for all time, we're now going to coin some standards here so that we put this issue to rest.

Okay. So there is a - the actual math, the statistics, is amazingly complex. Wolfram has a page with equations you can't even believe that, like, works to explain, to give you an exact value for this. But a useful approximation of the probability of a collision is n^2, "n" where that's the number of people, the number of accounts, the number of - like the number of people in the pool. So that number squared over 2 to the number of bits plus one. So like 256 bits plus one, 257. So the number of people squared, divided by 2^257, would apply. And this is true so long as the number of people in the pool, the number that we're checking for collision, is very much smaller than 2 raised to the power of half the number of bits, or 2^128. Well, since 2^128 is really, another one of these really huge powers, yes, "n" for reasonable numbers, like a billion people or seven billion people on the planet, for example, very much smaller. So that inequality is satisfied easily.

Okay. So plugging this in, plugging these numbers into this equation for a population of a billion users. So we have a billion BitTorrent Sync users - obviously we're never going to have that many. But say, just for the sake of argument, a billion. Or a billion bitcoin users, one tenth the population of the planet are using bitcoin. Or a billion SQRL login users. A reasonable number. Okay. A billion. The chance of a collision is one in 4.3 times 10^60. One in 4.3 times 10^60.

Now, the problem, okay, that's a very big number. Very, very low probability of collision. But not zero. Okay. Well, so we need to get - I want to develop a sense of scale for how small the chances are and how much concern we should give this. Okay. So let's compare this to something that we can get behind. And that is an extinction-level event caused by a major meteor strike on the Earth.

Leo: Okay.

Steve: Okay?

Leo: Yeah.

Steve: One of those, an ELE, an ELE, an Extinction-Level Event, is estimated to occur, on average, about once every 30 million years. Okay, so that's how often it's going to happen, once every 30 million years. Now, what that means is the chance of it happening within the next second, okay, there went one. Whoa. There went another one. Oh. There went a third. Okay. The chance of it happening, of an extinction-level event, of this question no longer being relevant to us because we're all gone.

Leo: Or the weather's really crappy, yeah.

Steve: One in 10^15.

Leo: Okay.

Steve: One every second. One in 10^15 chance that we no longer have this as a concern because we're gone. Okay? A meteor struck the Earth.

Leo: Right.

Steve: That is 10^45 times more likely to happen than a collision between any two people with a billion users of Bitcoin, BitTorrent Sync, or SQRL. 10^45 is a trillion trillion trillion billion. So every second that goes by there's a one in 10^15 chance that we're all obliterated. Oop, there went another couple seconds.

Leo: Yeah, but Steve...

Steve: Every single...

Leo: It could happen. But Steve. It could happen.

Steve: It actually couldn't. It actually cannot.

Leo: No, it could happen, though.

Steve: It actually cannot happen.

Leo: And I can win the lottery tomorrow.

Steve: There's a trillion trillion trillion billion times more likely that in the next second we will all cease to exist, and this will be the last thing on our minds. This will be a problem, I mean, believe me, whether your bitcoin wallet is full or not, it's not what you're worrying about.

Leo: But there is a chance it could happen [laughing]. I'm sorry. I'm just teasing you now.

Steve: It's actually zero. It's actually, I mean...

Leo: It's so close to zero as - yeah.

Steve: If zero fell off the end, yes.

Leo: But it could happen. I'm sorry. Our next question is another tweet from Wayne T. Taylor, @RamblingGeekUK. He asks, Mr. G., is there any point to having a security certificate on my site in light of the revelations about NSA spying? Wow. That's an interesting question. Wow.

Steve: Well, you know, it's like should I give up or not. I mean, I can understand that. And so, and I thought it was an interesting question because there is a lot that SSL provides somebody. Even if you use one of the cheesy free certificates that doesn't provide any verification of your domain name, I mean, SSL, for example, provides privacy through encryption and, presumably, authentication, which prevents phishers, phishing attacks from being effective because your certificate is being vouched for by a certificate authority whom your browser trusts.

So in an open WiFi environment, which is like all Starbucks hotspots and airports and so forth, where you have no logon at all, as we know, all of the traffic is decrypted. Everybody is essentially, I mean, there is no encryption on the traffic. It's in the clear. So anyone doing passive eavesdropping, just like the Firesheep little add-on for Firefox that was instrumental in forcing companies to encrypt themselves, this is why, is that you can't do session state management securely without encryption. You can't give somebody a cookie for them to hold to identify them as they move around your website without encryption because otherwise everything they're doing is in the clear.

So it's unfortunate that you have to go to a certificate in order to get encryption. But certificates now, for like a one-year expiration, are available for free. I think StartSSL is a source for those. So absolutely, there's lots of reason, irrespective of whether the NSA is able to get your key from the certificate authority or go to some extreme lengths to crack your encryption. For the benefit of your customers in the typical everyday use, SSL provides all kinds of absolutely worthwhile benefits. Definitely worth doing.

Leo: Question 4 from Aberdeen, Scotland. Kyle wonders whether Knock is really secure: As always, insert Leo's blah blah blah praises. But I need to say that I do actually appreciate all the good work you do, and the amount of knowledge you help me understand is just amazing. There's no one, and I mean no one - oh, come on, blah blah blah - not even at the university at which I graduated, who can explain these topics as well as you, the Explainer in Chief, Mr. Steven "Tiberius" Gibson. I can't thank you enough. And I, too, will thank you with purchases of SpinRite in the near future. Do that in a Scottish accent, I dare you.

So, Steve, after having looked at the Knock app, which really does work just fabulously, it got me to thinking about how secure it really is. Are you familiar with this app, Steve?

Steve: Yeah, we talked about it last week, actually.

Leo: Oh, all right, yeah. I understand it's technically speaking totally secure, as I trust your explanation in last week's podcast. But physically speaking - and by the way, I can give you some real-world feedback on this because I set it up with a surprising result myself. But physically speaking or implementation-wise speaking, is it secure? I mean, a knock-knock on your phone doesn't represent you in any way. It's not a password, not a fingerprint. It's not even a unique knock-knock. I understand this app is to make things totally convenient, but I wouldn't use it just because anyone could easily fool the system to be you. I just thought I'd get your thoughts on this, as it's interesting to think that sometimes even the most technically secure systems are broken if their implementation is weak.

I mean, really, it's pretty obvious - so just for those who don't know, this is an app for the Mac and for the iPhone. You put it on the iPhone, and you put it on your Mac. It uses low-energy Bluetooth, Bluetooth LE. And when I approach my Mac, it senses my phone. That happens anyway. And now the app on the iPhone, if I knock on the iPhone twice, unlocks the Macintosh, it says on here. And of course the only authentication you're using is the fact that you have the phone.

Now, I will give you a real-world issue that came up for me. I set it up here in the studio. Unfortunately, Sarah also has it on her phone. And for reasons I'll never understand, both times I set it up, it set up to work with Sarah's phone, not mine.

Steve: Oooh, boy.

Leo: Even though I was sitting right next to it. It doesn't obviously care where you are. In fact, it was within range of two phones. It chose Sarah's twice. And she's currently still set up to knock-knock unlock my laptop.

Steve: Okay. So that's disturbing in the extreme.

Leo: Oh, but there's no way to reject another Bluetooth LE. It doesn't give you a choice. It just - it does it.

Steve: So that's a bad implementation.

Leo: Yeah, they should give you a choice.

Steve: Yes. It should absolutely, you know, we talked once about the only vulnerability of Bluetooth being the moment of pairing, and that somebody who was really concerned should go walk into the middle of an empty parking lot, maybe like a stadium or shopping center sometime where no one is within 30 feet of them, the typical Bluetooth range, and do their pairing then. Because it's only in that instant that there's any vulnerability.

Leo: Well, and Bluetooth LE has a hundred feet. I mean, it has a much larger range. Sarah Cake 5s is the phone that can unlock my...

Steve: Unbelievable.

Leo: And it never gave me that choice. It never says whose phone do you want to use?

Steve: That's disturbing. So...

Leo: Gosh, when you pair a Bluetooth thing, these things jump through hoops. Oh, make sure the pairing number's the same. Are you sure you're seeing it? Nothing.

Steve: Yeah, well, these guys, I'm disappointed. What I was responding to was the crypto architecture, not the implementation. And several other people also said that they were worried because, for example, they didn't even have to knock their phone twice. They could bump into the counter, and it would unlock their machine. So again, I wanted to follow up and explain that I wasn't thinking that this was, like, good security. This was...

Leo: Interesting.

Steve: ...good, this was correct crypto. But obviously these guys have huge implementation problems. We've always talked about security and convenience being at odds. I'm shocked that they didn't do a "enter a code on each end" so we can figure out which is your phone. That's just crazy.

Leo: Too much trouble [laughing].

Steve: Wow. That's disappointing.

Leo: That is sad, isn't it. And by the way, you could do this with Bluetooth. There's an article here on Lifehacker from last June on unlocking your computer just by sensing the Bluetooth, in a variety of apps that do this, as you walk into the room. This is Windows or Macintosh.

Steve: And actually that's Question No. 5 we have following up.

Leo: Well, there we go. I'm already ahead of you. All right. Let's move on now, then, to - thank you, Kyle. Thank you for the kind words, too.

Stuart Ward in Maidenhead, U.K. - you're big in the British Isles - notices that Bluetooth unlocking is nothing new. Oh. Linux users have had this for a number of years. Yup. Have a look at BlueProximity. It's a SourceForge project. There's no function on the phone, so any device that will accept a Bluetooth connection can be used. The security is based on Bluetooth pairing, so you have to pair the device to your computer for it to work. I've used this for a few years. The only caution I would make is if you're away from your computer, but still close enough to make a Bluetooth connection, this can drain your phone battery more quickly because the phone will need to transmit at full power. When near, the dynamic power of Bluetooth means that the ping connection is not a significant battery drain. So if you're close, it's not a problem. It's only if you're kind of right at the edge of the 10 meters.

Steve: Well, and that's one of the reasons that these guys who did Knock chose...

Leo: LE.

Steve: ...to use Bluetooth LE, yes. It's far - they brought the bandwidth of the connection down and deliberately used the low-energy variant that's in Bluetooth v4.0. What happens with Bluetooth, similarly to cell phones, is they dynamically change their transmission power based on a report they get from the other end about the received signal strength. So as you stretch out the length of your connection, the receive signal strength that is reported from the other end drops, and so they put more juice into transmitting in order to keep the signal strength up. So LE solves that problem to a much greater degree. And I just wanted to say, yes, there have been other Bluetooth connection suggestions. Hopefully they have been done, well, with more security in mind, with more actual practical application security, rather than just the low-level crypto, which is sort of free because Bluetooth gives it to you.

Leo: Right, right. Moving along to another tweet, this one from Economic Mayhem, probably thinking of the fact that the folks at TrueCrypt are about to undergo a security audit, wants to know: Shouldn't you advocate audits before getting 100% behind a product like Threema or OTR?

Steve: And I saw this, and I thought, okay. Let's talk about this for a minute because in a perfect world, yes, we would like to have everything audited.

Leo: But look how long we've been using TrueCrypt without an audit.

Steve: Yes. And the fact, I mean, people say, well, I'm not using anything that I don't know exactly what it does. Well, but you're using a processor chip. You're using an operating system you did not write yourself from scratch.

Leo: Yeah, all the time, yeah.

Steve: You want to have your eyes open, certainly. And look at the people that just lost tons of bitcoins because they were using some bitcoin exchange that they had no direct personal knowledge or control over. So all we can do is have our eyes open and use our best judgment. Does everything we see from the people of Threema look right? And I'd say yes. Their FAQ and the details they provide all look correct, and nothing raises a red flag to me. And they want a dollar for their device, to use their product so that they can pay for the infrastructure that they have to create.

In the case of OTR, the Off The Record protocol, that's been heavily cryptanalyzed by people to understand how it works, and it's been well vetted now, so we know we can use it. My problem with BitTorrent Sync, all of their words they're using sound good, but they're really being vague about what they do. And it's like, okay, wait a minute. Is it open source? Is it open protocol? What are they going to open? And we just don't know. But I would imagine that they did security right. They understand security.

So there are clearly situations where we can look at what we're told, like when we did the review of cloud storage providers. About half of them were wrong, and we could say, okay, this is not TNO. This is clearly not correct. In the case of Apple, for example, with iMessage, they've said, and we know, that they did not do the protocol correctly, and it's closed. So we can say, well, they have good intentions, but they're not telling us what they're doing in detail, so it's hard for us to trust them completely. So unfortunately, security requires absolute knowledge to have absolute security. And we're not going to have absolute knowledge unless we go make our own chips and write our own operating systems and write all the applications that run on it, which no one is able to do now.

Leo: Yeah, so we have to just live in a world where we trust people. But I would say you can trust open source a little bit better because at least in theory it's on display.

Steve: Yes. Well, and look at the intent; look at the background of the people; look at what their goals are. For example, I will be writing an SQRL client for implementing that protocol in assembly language. And talking about the protocol, it'll be open. We'll be using open libraries. And everyone will understand that I have no ulterior motive other than creating the most secure implementation I am capable of creating. And I believe people will trust me.

Leo: Yeah. And if they don't, they don't have to.

Steve: And if you put your coinage in a Chinese...

Leo: BitLocker...

Steve: ...bitcoin exchange, and it turns out they're fraudulent, well, gee, maybe that wasn't the right place to put the money.

Leo: But to be fair, you coined the term Trust No One, TNO.

Steve: Yes, TNO.

Leo: But that wasn't a call to action. That was a description of a certain kind of thing.

Steve: Yes. It was an acknowledgment, an explicit acknowledgment that we have the technology. That's the key. We can do TNO. And in fact that leads nicely into the next question.

Leo: No. 7, from Steve Davidson in Eastern Massachusetts. He wants to know what you think of iCloud Keychain, the new feature Apple's offering in Mavericks, OS X 10.9.

Steve: And in general in iOS 7, too; right?

Leo: It comes with 7 and Mavericks, that's right. He says it looks to be a lot like LastPass for the rest of us. I use LastPass, but I'm a listener to Security Now!, so I can't be called normal on the geeky scale. LastPass requires a bit of technical skill to use, and the willingness to use a special browser on an iPad. I'd really like for my octogenarian father and other non-technical relatives to have a good, easy-to-use password vault. iCloud Keychain does seem to be the right thing. Or is it? What does Steve think of the security model? Of the one or two setup options, which makes the most sense to our guru and advisor Steve Gibson? I'm not as worried about NSA snoops as I am about protecting them should Apple ever be compromised. Could you please weigh in on this? Thank you. Steve Davidson.

Steve: So here we have a problem, and that is that Apple doesn't document their stuff. Apple is easy to use and gives us nice little switches that we can turn on and off. And we have to take them at their word. Now, again, I tend to be trusting. That is, if someone says this is what we're doing, for me it's like, okay. The consequence of them not doing it, of Apple lying to us about what they have deliberately engineered for iCloud, would be catastrophic. And we know, for example, that Apple has now, what was it, their canary policy, where they're going to preemptively tell us periodically that they have not been served with a letter from the NSA because they're unable to tell us when they have been, which is sort of clever. It's like, okay, they're sounding like their heart's in the right place.

So what do we know from Apple, what has Apple stated about iCloud Keychain? They have said that it is encrypted, the keychain data, encrypted in transit and when stored on their server. They've said they use 256-bit AES encryption. Now, remember that the AES encryption is a block cipher whose block length is not changeable. It's always 128 bits. But the key is what is changeable. So when we say 128-bit AES, we mean a key of 128 bits. Theirs is double that.

Now, here we are. That's my favorite new number, 256. 256-bit is the new black. And so they're using this level of encryption which is a trillion trillion trillion billion times stronger than the chance of us all being wiped off the earth in the next second. So we're fine. So long as that's the only - so long as brute-force guessing is the only vulnerability. So they're using that encryption to store and transmit passwords and credit card information. They also use elliptic curve asymmetric crypto and key wrapping. So they're sounding like they're doing all the right things. They have written that iCloud Keychain encryption keys are created on our devices. So this is the model where - this is TNO. This is the model where an asymmetric key, they're saying they're using elliptic curve asymmetric crypto, as am I, for example, with SQRL, because that's the right one now.

Now, we don't know which, but there aren't known problems with elliptic curves, even if you use the standardized elliptic curves. As far as we know, they're okay. I'm using Dan Bernstein's curve because I'm just a little afraid of NIST and their past affiliation with the

NSA. But still, Apple's doing the right thing. TNO. So the keys are created on our devices, and Apple can't access those keys. Only encrypted keychain data passes through Apple's servers. And Apple cannot access any of the key material that could be used to decrypt that data. So they're saying that the private key stays on the device, and the public key, presumably, is what's encrypted and exchanged. Maybe.

I mean, again, unfortunately, we don't know what the architecture is. They do, they continue to say only trusted devices that you approved can access your iCloud Keychain. They say advanced settings allow you to choose an iCloud security code longer than four digits - oh, and my goodness, please do - or have your device generate one for you. And they said you can choose to disable keychain recovery, which means that iCloud Keychain is kept up to date across your approved devices, but the encrypted data is not stored with Apple and cannot be recovered if all of your devices are lost.

So if we reverse-engineer this, this says that, if you allow Apple to store your iCloud Keychain data on their servers, and you lost all of your devices, so that you didn't have your own local database, then you could go to their web page, or maybe get another iCloud device, put in the same security code, and it would download it and then decrypt it locally on your device. So that says they do have the keys, that is, all the keys, including - again, we don't know what they're doing with asymmetric crypto. This is what's so frustrating about not having any protocol documentation is that we have to, like, from what they say, kind of guess and reverse-engineer.

But they are saying, I guess, that if they store a copy of your iCloud data, that you can recover it with your encryption code, whatever they call that somewhere here, even if you lost all your devices. So you want that to be very good. Otherwise - because that's what you're relying on. And for safety you probably don't want them - you want to disable what they're calling, what was it, keychain recovery. So disable keychain recovery, then they're not storing a copy on their servers. Because to me that does not seem safe. If they're storing it, it must be that it's only protected by your password, and that doesn't seem safe. So disable keychain recovery, they don't keep a copy, but then it's up to you to make sure you don't lose all your devices. And again, that's the best we can do with what little we know.

Leo: Yeah. If you're going to give it to an octogenarian parent, the default settings need to be sufficiently adequate. Are they? Yes, you can make it more secure. But it sounds like the default settings aren't the best.

Steve: Oh, no. Their default is the four-digit code, which is insane. No, I can't...

Leo: And storing it for recovery. So to really, to answer his question, he's saying, look, is this for the rest of us? If you're smart, you're using LastPass. Is this good enough for the rest of us? And to me that means using the defaults because the rest of us...

Steve: I'm using iCloud Keychain with an insanely strong password and no keychain recovery.

Leo: Right. And that's the right way to use it.

Steve: To synchronize - yes. And that's the way I'm using it.

Leo: But most people will not use it that way.

Steve: And I am trusting Apple.

Leo: Right. You're still trusting Apple. But most people will not use it that way.

Steve: Well, I'm trusting Apple's description. I'm trusting that what they've told me is true. If I turn off keychain recovery, they're not storing a copy on their servers, in which case we're only linking across devices, and they have no copy of it.

Leo: Would you say that LastPass's implementation is preferable?

Steve: Not for the octogenarians.

Leo: But again, I think octogenarians are going to stick with the defaults - four-digit codes and letting Apple recover it for them.

Steve: Well, yeah. They'll die before anyone decrypts their data.

Leo: Well, I'm just saying the tyranny of the default. I didn't know that there was an option not to use a four-digit code. I'm going to have to look into that. I have a four-digit code on it because I didn't know there was an option not to. They don't expose that information.

Steve: Yeah, the tyranny of the default, as you say.

Leo: Right. So I'm using Keychain in an insecure fashion, just because I didn't even know there was an option. Finally, Peter Chase in Columbus, Ohio wonders whether he can drop NoScript if he's using Sandboxie. We talked about Sandboxie last week: I reinstalled Firefox on my wife's laptop - it's a Windows 8.1 device - as part of the process of getting rid of some AVG toolbar she'd inadvertently installed and that was causing serious havoc, by the way. NoScript does not cooperate with Firefox Sync, so I have to laboriously re-approve all of our commonly used websites for NoScript. I've written to NoScript asking if they would consider having NoScript work with Firefox Sync so I wouldn't have to do this. He's approved certain sites, or she's approved certain sites, and Sync doesn't sync those sites. You have to enter it each time.

Steve: Right, exactly, right.

Leo: My wife's laptop is getting all of its bookmarks and add-ons restored from my main machine via Firefox Sync. NoScript never responded to his email. After hearing last week's episode of Security Now!, I took this as an excellent time to install Sandboxie. Hence my question. If some scripting mischief occurs, wouldn't it all stay within the sandbox? Our e-mail is web-based, so sandboxing the browser should help things a lot. Your thoughts, please. Thank you. Listener since No. 1, dittos, et cetera, SpinRite owner. Thank you for your service to humankind.

Steve: Yeah, I'm glad we talked about Sandboxie last week. Sandboxie is very mature. It really works well. And if you're using web-based email, by all means put your browser in Sandboxie. And for someone like your wife, I mean, I like the control that NoScript offers. But for a less technical user, wrapping Sandboxie around your browser makes absolute sense. It's necessary, then, it's a little trickier, you have to, like, drag things out of the sandbox if you download a file that you want to keep because that'll be stored in the sandbox. You need to manually drag it out of the sandbox. But for someone just using webmail in this current world where something like CryptoLocker is such a threat, again, I think Sandboxie is a terrific solution for someone using web-based email, or even just email. You can certainly run Sandboxie, not on just a browser, but you can Sandboxie your email client, as well, so it doesn't have to be web-based. Yes, yes, yes.

Leo: Yes, yes, yes.

Steve: I think Sandboxie deserves another look for those who looked at it once and haven't looked at it since.

Leo: Isn't it compatible with 64-bit now? Somebody wanted to know.

Steve: Don't know for sure, but it must be because it's still cranking away. It's cranking away...

Leo: Yeah, I don't think you can - I don't think there is a 32-bit version of Windows lying around. My friend, Steve Gibson, the time has come for us to say goodbye. You have answered all the questions I have in our little box here. It's empty now. Thank you, Steve. We do this show every Wednesday afternoon, 11:00 a.m. Pacific, that's 2:00 p.m. Eastern time, 19:00 UTC, on TWiT.tv. Please tune in and watch live, if you can. If you can't, though, on-demand audio and video is always available. Steve has 16Kb audio for the bandwidth-impaired and handwritten, personally crafted by Elaine Farris, transcripts so you can read along as you listen.

All that's at GRC.com along with SpinRite, the world's best hard drive maintenance and recovery utility, and all the great freebies Steve offers. GRC, Gibson Research Corporation, dotcom. You can also follow Steve, @SGgrc on Twitter. You'll get lots of links throughout the week by doing that. And of course we have full-quality audio and video at our site, TWiT.tv/sn. Or you could subscribe because this is everywhere. This is one of the oldest podcasts in the world. And so that means it's on every list, everywhere. Hey, Steve. Thanks so much.

Steve: Thanks, Leo.

Leo: See you next time on Security Now!.

Copyright (c) 2012 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

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