Listener Feedback #195

Description: Leo and I discuss the week's major security events and discuss questions and comments from listeners of previous episodes. We 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-470.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-470-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. He's going to talk about - sigh - the first, probably not the last, exploit based on Heartbleed, an actual break-in, and a whole lot more. Your questions, Steve's answers, too. And what's wrong with PGP? We'll find out next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 470, recorded August 26th, 2014: Your questions, Steve's answers, #195.

It's time for Security Now!, the show that protects you, your loved ones, and your privacy online. It's like a giant button on your Internet, protecting you, with Steve's face on it. Hey, Steve Gibson.

Steve Gibson: And more and more there's sort of a "Keep calm and carry on" philosophy. It's like the press just seems to just be having a field day lately on all of these overhyped, I mean, that's their job, I guess, is to drive traffic. But it's just crazy how I've noticed that, in general, sort of the background theme that I've been carrying the last few months has been, okay, now, that's not quite as bad as it sounds. Or, okay, yes, the headlines are a little overwrought. So, yeah. It's, you know, we want to be safe, but also want to try to keep breathing at a constant pace.

Leo: I knew you'd come around to that. At some point you just have to say, you know, there are so many threats out there that it would paralyze you if you took them all seriously. So just, you know what, the chance of somebody targeting you is small. Take the reasonable precautions, good passwords, be careful, social engineering, et cetera.

Steve: Yup. There's a Microsoft research paper that I've still got, it just keeps getting pushed down in my notes. It's something that I have always been planning to dissect on the podcast. It's something titled like "Users' Rational Disregard of Security Advice."

Leo: I love it.

Steve: Which - isn't that great? I just love the title. It's like, "They are ignoring us, and that's rational." So...

Leo: You always have to. I mean, don't ignore people, but don't go all crazy, either.

Steve: Well, because, I mean, everyone wants to find their balance, wherever that is. And certainly you could really be belt and suspenders and superglue and epoxy and, I mean, just have a really difficult time removing your trousers at the end of the day kind of person; or you could just, if they're looking like they're about to fall off, it's like, eh, I'm not worrying about it. So everybody has a different balance point where it's the right place for them. And we've never been about absolutely crazy kneejerk over the top. We've been about, okay, here's what we think are the facts, and you can decide.

Leo: But of course, if you listened, it would be easy to get a little paralyzed by - it's the same thing as watching TV news, I find. The job of the news is to find all the bad things that are happening. And now with global news networks and the ability to communicate globally, pretty much there's always something bad going on somewhere. And you would start to think the world's falling apart.

Steve: Yes. It's definitely the case that you cannot fear what you don't know about. So first of all...

Leo: Yeah. Ignorance is bliss.

Steve: So, yeah, exactly. So if you have no idea that anything is going on, well, okay, yeah, how can you be upset? If you're informed, then you've got some responsibility to decide, okay, wait a minute, does that sound bad, or does that sound bad? So certainly the less you know, the less opportunity you have for being upset. The more you know, the more choice you have.

Leo: I think that most people who listen to the show are in the business or professionals. They need to know this information. And they have the wherewithal to weigh it and act appropriately and not go crazy.

Steve: Yeah. And clearly we're news and technology. So last week was steeped in the technology of routing.

Leo: Right, that was great.

Steve: And network addresses and masks and all that. And so because that's really where I come from, I'm looking at the stuff we cover from that angle. We had a very slow week, Leo. I went digging around for stuff to talk about because normally what happens is I kind of keep an eye on my Twitter feed during the week, and there's always enough stuff. I make notes of articles and issues and stories as I run across them or as I see people making sure that I know about something. Pretty much nothing happened.

Leo: Isn't that funny. You would think, now, this is also a slow week for tech news in general. In fact, for news in general. It's the last week of August. Everybody's gone. We're waiting for Labor Day. In the tech news world we're waiting for all the new phones and new gadgets from IFA and Apple's announcements, et cetera. And so it's very slow. We were talking about this on MacBreak Weekly. This is a dead time in general. But I find it funny that it's also a dead time for security. So apparently hackers take the week off, too.

Steve: Either that, or the reporters. I'm not really sure.

Leo: Yeah, hackers are still working, we just don't know it.

Steve: Exactly.

Leo: Oh, I get it.

Steve: Maybe we just have a little lull in the reporting, in which case we'll get caught up next week.

Leo: Everybody in McLean, Virginia is on the beach right now, not working.

Steve: Yeah. So we know that Sony's PlayStation network was attacked. There's a new guy in charge of U.S. Cybersecurity who has boasted that he knows nothing about cybersecurity.

Leo: Yeah, I thought that was great.

Steve: I did, too.

Leo: How is that an advantage? Please, really.

Steve: We actually have the first confirmed serious attack as a consequence of the

Heartbleed vulnerability that of course we talked about so much. And then the question is, would you rather be autonomous or anonymous, and how I tripped over my tongue last week. So that's what we'll talk about. And then of course we've got 10 great questions and discussion points from our users.

Leo: You caught yourself with the autonomous/anonymous. I was about to interrupt, and you finally fixed it, so I just left it alone.

Steve: Oh, good, because I know the difference. But of course I'm so focused on anonymity that, if I'm not - if I don't make sure I say "autonomous," then I just automatically say "anonymous." So, yeah.

Leo: Steve Gibson, Leo Laporte. We're talking security.

Steve: So just for the record, for those people who noticed I was saying "anonymous," I meant "autonomous." They are autonomous systems and autonomous system numbers, ASN numbers.

Leo: I translated in my head. I knew exactly what you - I didn't even think about it, or I would have stopped you.

Steve: Yeah, and I didn't even hear myself saying "anonymous" because...

Leo: You eventually - you said "autonomous" eventually, so it became clear.

Steve: Well, I hope so.

Leo: Yeah, you did.

Steve: Because I meant "autonomous" every single time. As far as I know, there was no instance last week...

Leo: No anonymity.

Steve: ...where I actually meant - there was no anonymity in these autonomous systems. They were not anonymous, they were autonomous.

Leo: Thank you.

Steve: So just to correct the record.

Leo: Hey, by the way, I wanted to thank you. I don't know if this is - I don't see this in your notes. But we got an email from your friends at DigiCert. I know you use them for your certs.

Steve: Oh, and I, I mean, I've - for years now. And they're just - they're my company. I'm so happy. I finally - I don't change easily. I'm one of those people...

Leo: Oh, I know. You're a loyal man.

Steve: I need, like, some reason. And so I'm still over at Network Solutions for my domains...

Leo: We'll fix that, yeah.

Steve: ...and I have no idea why. But finally I just had to leave VeriSign because there was just too much pain. And what it was, was it was noticing that Facebook was using DigiCert. And I thought, okay. I was nervous about that there would be - someone wouldn't like the DigiCert cert, which was completely, it turns out, misplaced concern. And so when I saw that Facebook was using DigiCert, I said, oh, well, if it's good enough for Facebook, I mean, clearly everyone's going to accept that certificate. So I went over. And oh, my god, has it been a great experience.

Leo: And this all comes from the story we had that Google was ranking a little higher secure sites, sites that were using HTTPS. And you and I had the conversation, well, why does TWiT need to be secure, and then the issue of, well, man-in-the-middle attacks, for one. And so, thanks to you, the folks at DigiCert contacted us and said, "We'll give you a free cert if you want to do an EV cert." That's the fancy one; right? The green bar.

Steve: Yeah, oh, it is. And, I mean, of course we know that there's a method to their madness. This gets you...

Leo: They got a free plug right now.

Steve: It gets you hooked on their certificates.

Leo: And next year I'm sure - yeah. First one's free.

Steve: You will then be renewing in three years or two years.

Leo: I think they're fans, also, and I think it was a generous thing to do.

Steve: They are. They listen to the podcast. And it was very generous. And I'm delighted that this will happen. And I guess so the way to sum this up is that a site with a great reputation, and a reputation that it wants to enhance and maintain, is just - it's better off offering secure connections to its users. My position was, well, if you're not doing anything interactive, if you're just displaying passive content, there's not such a big problem.

But people argue correctly that you're still subject to various sorts of injection attacks. And so, for example, TWiT.tv being a high-reputation, popular site could be targeted for injection attacks, that is, taking advantage of the fact that people trust TWiT.tv to abuse the nonsecure connection. So your having a certificate then allows people to connect to you securely. And so you're sort of extending your shield of security from around your server all the way out and enclosing the connection all the way to their browser. So it's sort of a - it's arguably a good thing to do.

Leo: Well, and I deferred to our sysadmin, Mike Taylor, "Bear," we call him, because if it was hard to implement or whatever, I didn't think it was so important that we would do it. But he jumped at it. He said, "Oh, I'd love to get all of TWiT behind a cert." So that was enough for me. So it's not there yet, but I understand he's working on it now. So pretty soon, when you come to TWiT.tv, you will see a green bar and HTTPS.

Steve: Nice.

Leo: Yeah. So that's - thank you. I appreciate that. And thank you, DigiCert, for doing that.

Steve: Yeah. So we don't know much about the DDoS attack that knocked the Sony PlayStation network down. It was weird, though. There was like a real-world component to it, too, because at the same time the president of Sony Online's flight was rerouted and grounded because American Airlines received a tweet from Lizard Squad, they call themselves.

Leo: Oh, please.

Steve: That was a bomb threat for the flight. And they put the flight down. I think this was...

Leo: That's a felony. That's just horrible.

Steve: Yeah. I think it was in - I think they grounded them in Phoenix and got them off the plane, and the feds were there and so forth. So that was all sort of synchronized. And this same Lizard Squad group apparently had attacked Blizzard Entertainment, of course famous for World of Warcraft, and Riot Games, that does League of Legends. So these are guys that, for whatever reason, like to take game networks off the 'Net and harass John Smedley, who's the president of Sony Online. Do you know what's, I mean, is Sony doing something controversial or bad or anything?

Leo: Well, Sony's been widely hated for a while because of, well, the security breach that they had and other, I mean, and they put, you remember, I mean, it's gone on and on. They put DRM on their games that actually turned out to be a rootkit, you remember that. But don't give these guys credit. These guys are jerks, whoever's doing this. And it may be one person, by the way.

Steve: You mean don't glamorize them.

Leo: Don't glamorize them. They're not acting out of any righteous political anger. This is just...

Steve: Just a random attack.

Leo: These kids are a-holes. And I hope they get caught. That's just - that's bad stuff to do that.

Steve: Yeah, well, we can't have people tweeting bomb threats and grounding...

Leo: That's really wrong.

Steve: That's really - that's really a problem for our society.

Leo: Yeah.

Steve: So I got a lot of tweets because the tech industry took great umbrage to Michael Daniel, who is the recently announced appointee. Barack Obama, of course our illustrious President of the U.S., appointed Michael Daniel to head the U.S. Cybersecurity. He's the cybersecurity "czar," which is the term we all now use. And in an interview that Information Security Media Group did, he said that: "Being too down in the weeds," as he put it, "at the technical level could actually be a little bit of a distraction."

And he said: "You can get enamored with the very detailed aspects of some of the technical solutions. And particularly here at the White House, the real issue is to look at the broad, strategic picture and the impact that technology will have." And so he explained that he plans to focus on the economics and psychology of cybersecurity.

Leo: Moron.

Steve: Which I guess are like the parts that he knows.

Leo: Yeah, because he's not - he has no background in this field. Not that he

doesn't...

Steve: Yeah, exactly.

Leo: Okay, maybe he doesn't know how to write PHP. He doesn't have any background in this field.

Steve: None.

Leo: He's a policy wonk.

Steve: Well, yes, exactly. And he says: "At a very fundamental level, cybersecurity isn't just about the technology, but it's also about the economics of cybersecurity. Intruders get in through those holes," as he puts it, "that we know about..."

Leo: Moron. I'm sorry.

Steve: Yeah, "that we could fix. The question is, 'Why don't we fix them?' That clearly leads me," he says, "to the conclusion that we really don't understand all of those economics and psychology situations well enough."

Now, okay. The guy is certainly no dummy. He's got his bachelor's in public policy from Princeton, then two masters, one in public policy from the Harvard Kennedy School of Government, and the second master's in National Resource Planning from the National Defense University.

Leo: Oh, that should be useful.

Steve: But it's true, nothing in cybersecurity. So what I saw on the 'Net was, first of all, people just making sure that I knew that this guy had said this. But there was a lot of techies, sort of academic techies, who were upset that this is the person who was appointed. I mean, he's clearly 100% bureaucrat.

Leo: It's political crap. It's political crap.

Steve: But the fact - yeah. And the fact is, Leo, neither of us could do that job. I'd just shoot myself. Because, I mean, at that level, there's nothing technical going on. But you really would like someone more like we had, what, Howard, was it Howard Schulz or Schmidt, can't remember [Schmidt], who was the previous cybersecurity guy. And he was fabulous. I mean, he understood cybersecurity enough to be able to know what made sense and what didn't. And you've got to wonder just how far removed from that is the right place to be. And this guy is as far away, as far removed as you could get.

Leo: It's political cronyism, and it's just shameful. I'm just...

Steve: Yeah, it is disappointing.

Leo: This is not the time to appoint somebody that doesn't know anything about security to a cybersecurity position.

Steve: And then who boasts that...

Leo: And then boasts.

Steve: And then who boasts that, well, it's the psychology that we're trying to understand.

Leo: It's not. It's not. And he should go to DEFCON. This is just more of the same.

Steve: So we found, we have the first confirmed major breach caused by Heartbleed. It was reported a week ago that - there was a major breach reported. I didn't pick up on it and talk about it then because it's like, okay, another breach. It's getting to be the point now where that's just not very - it's not very exciting if there isn't anything to back it up. Well, there is something to back it up.

So it's a little more than a week ago it was announced that the nation's, the U.S.'s second largest for-profit hospital chain, called Community Health Systems - and they've got hospitals that they manage, I think for some reason I'm remembering 18 states, like 18 states throughout the Southeast I think is sort of where they're centered. I kind of think, again, a lot of this just ran past me. I think maybe they're based in Tennessee. I'm not sure. But they had a major breach. The names, addresses, and Social Security numbers at least - again, that hasn't been exactly specified - of 4.5 million patients.

Now, of course this is arguably more sensitive data, this is a medical records breach, than if it was just your PayPal account or something. What is significant, and what just was revealed, and even now this is still not through confirmed sources, they're keeping a lid on it during the investigation, but what has been determined through trusted inside sources is that the breach was made by hackers in China who used Heartbleed to continually probe the servers. And in this case it was a Juniper VPN server that still had the vulnerable OpenSSL on its Internet-facing VPN server that allowed them to obtain VPN credentials from some high-placed network administrator.

So those VPN credentials were captured in through this well-understood now Heartbleed buffer overrun that is able to, as we've talked about it when we did our podcast on Heartbleed, to take a snapshot of RAM that should not be available publicly. They found, through who knows how many persistent snapshots, they found VPN credentials, then were able to use those to log in as this highly placed network admin as them, and then got access into the internal network of Community Health Systems, and through that then exfiltrated this 4.5 million patients' medical records back to China.

So, and that is, interestingly enough, I mean, what we had to date was confirmed theoretical vulnerabilities. And even then, I mean, when this was first announced, there were people reluctant to say that you could actually do this. And, famously, there was a challenge put up, and credentials were stolen. And those were the security certificates of the servers were stolen, which arguably was one level of problem, although remember that the argument there was, even if you had the security credentials, you would still need to perform other - you would still need to do other things like a DNS highjack in order to get people to go to the wrong IP in order to believe they were at the site whose stolen credentials were being used. It's not enough just to have the credentials.

Well, here, I mean, if you're able to exfiltrate VPN credentials, as this attack on Community Health Systems demonstrates, you're in. You've got a major attack against, not visitors to a public server, but into their internal network. So for what it's worth, this is sort of a - this would have been remote attackers identifying a persistently vulnerable Heartbleed-vulnerable server, who just sat there patiently performing the Heartbleed buffer overrun, pulling buffers of 64K of data over and over and over and looking at it.

So if anybody is still running - and we do know in fact that, last I heard, many, many months after this was publicly known, the number that I have in mind that I remember seeing was 330,000 publicly facing servers are still vulnerable to Heartbleed. And they're things like this, machines in the closet that nobody really thinks about that are vulnerable. So, yikes.

Leo: Yeah. And it's kind of also a proof of concept, right, because the real question about Heartbleed was, well, could you really get anything of value by polling again and again and again? Well, yeah, apparently so.

Steve: Yeah. And many people who did it just got noise.

Leo: Right.

Steve: They thought, well, there's nothing here. It's like, well, no, try again. Ask again. Knock on the door again.

Leo: It did take them a while. And I bet you this has been going on since the original, like they just kind of, let's get some more, let's get some more.

Steve: Exactly. That's, I mean, that's what you would do if you were determined, in the so-called "advanced persistent threat" sort of model, where you're determined to get in, and so you just trickle. You don't want to do too much because you don't want anything to appear in logs. And one would hope that intrusion prevention or detection systems would be now looking for this very visible intrusion. This is something that any sort of IDS (Intrusion Detection System) could easily be primed to detect and block further connections from that IP and sound alarms.

But in this instance there was some VPN server in the back room that nobody thought about, nobody was worried about, and it was enough to get people in. So, yeah. It's definitely, as you said, a perfect demonstration of a theoretical vulnerability. This is where, oh, yeah, this maybe could happen. Well, bang, you know, big-time.

Leo: Amazing.

Steve: And I did get a tweet, even though Harry's is not on the sponsoring of this week...

Leo: I shaved on MacBreak Weekly. I don't know if you caught it, but I shaved with Harry's this morning on MacBreak Weekly.

Steve: Nice.

Leo: Smooth.

Steve: We have a listener, Todd Eddy, said that his first shave with Harry's after never - oh, he tweeted on the 23rd, "First shave with Harry's after never using a razor" in his life. So this was his virginity of an actual straight-edge razor. He's only used electric. And he said, "This is as close, if not closer, and no cuts." He did follow-on tweet that apparently he shaves his head. And he says, "For that I'm still using electric." And I said I think that's probably a good...

Leo: Did you ever use an electric razor?

Steve: No.

Leo: I've tried them.

Steve: I don't think I ever did.

Leo: They're not very close.

Steve: No.

Leo: I would love for them to work, but it's just not the same.

Steve: Yeah. I grew up in a household with a dad using a straight-edge, and that's how, you know, he says, "Let me show you how this works." And that's how I was - I just grew up that way.

Leo: Yup.

Steve: I mean, the convenience of it, sometimes when I'm driving to breakfast I'll see somebody shaving in his car [imitating electric razor] on the way. It's like, well, that's sort of...

Leo: That's convenient.

Steve: That's multitasking. Yeah, yeah. That's better than women trying to put makeup on when they're driving. It's like, ooh, that requires a little too much concentration.

Leo: That's funny.

Steve: So that's our news.

Leo: All right. Do you want to do a little - I'm done with ads. If you want to talk about SpinRite, I've got the questions for you.

Steve: Actually, I talked so much about it last week, and I got a lot of great feedback from people who really did like hearing all about it, and there are a couple questions relating to that in our Q&A, so let's just get into the questions.

Leo: Let's get into it, then. Stephen Collins, Thomasville, Alabama. He's worried about copper. What?

Steve: Yeah, several people.

Leo: First of all, love the show. I've been with you since Episode 1, he says. In the Episode 468 you gave advice to a listener asking about wiring his home network who wanted to connect the LAN in his new home to his parents' home some 400 feet away. You mentioned the cost advantage of CAT6 versus fiber and even suggested he use CAT6 inside a conduit to connect the two locations, the conduit being for upgrade purposes. Speaking from experience, I can tell you this is a terrible idea. The reason? Ground potential differences. Any time you run copper - well, this is interesting. I didn't know this.

Any time you run copper wire between buildings with separate electrical power systems, there's a problem due to difference between the voltage of ground in the two buildings. In addition to carrying data, the copper wire will connect the ground systems of the two buildings. When there's a difference, a ground current flows on the data line. Eugh. I've personally witnessed the results of this type of setup. I've seen fried Ethernet ports, fried motherboards, even sparks flying from expensive Cisco switches during a thunderstorm.

The only solution is to connect the two homes with non-conductive media like fiber. It may be more expensive initially; but in the long term only fiber, or maybe wireless, will provide a safe, high-speed, non-conductive path. That is great advice.

And I'm glad...

Steve: Yes. And we got it from several people. Now, I was a little confused because the question that I remember from two weeks ago was the Q&A guy asking, he said, it turns out that fiber is so inexpensive that I'm thinking of using that because why not. And then I think that we, in our discussion, we sort of switched into talking about plumbing inside a home, and I think I remember talking about Mark Thompson, wiring his whole house for CAT5 before even moving in and how convenient it was to have outlets wherever you thought you might need them and so forth. So I don't know, I got a feeling like we were talking about so much, but I absolutely wanted to mention this.

Now, the only way this technology works at all is so-called "differential signaling," that is, even CAT5 with 10Base-100 or 10Base-T, you've got a "twisted pair," as it's called, one going in each direction. And the idea is that the wires are twisted around each other continuously so that any interference, electromagnetic interference, that one wire picks up, the other wire picks up. That is, they are a pair that are deliberately twisted in order to sort of balance any interference that they pick up.

And the idea then is that, at the transmitting end, the signal is made by moving the voltage on the wires in opposite directions, so it's called "differential." And then at the other end there's a differential receiver that ignores the so-called "common mode," which is to say it looks at the difference between the signal, not the absolute voltage on the lines, which is the key to all this working. If you just had, like, just one wire going along, you'd have a very difficult time over any distance not picking up an incredible amount of noise on the line. USB is not differential. It's so-called "single-ended." But it's dependent upon being grounded and shielded. And its length is deliberately limited. You're not getting nearly the same kind of length as you can get with a CAT5, which uses this differential signaling.

So it's definitely the case that Stephen and the others who wrote about this are correct. You can't have each end at large voltage differences because you are then going to get some potentially destructive current flow which actually results in a voltage difference. It's the voltage, the pressure that breaks down the semiconductor and causes it to deteriorate and cause problems. So if the differential is small, as often exists even within a house, the system is designed to handle it. But the further apart you are, and exactly as he says, especially if you've got separate electrical systems, then using a nonconductive bridge like fiber absolutely makes sense. And as our original questioner said, hey, it turns out fiber's not expensive any longer, so why not use it? And so the lesson here is absolutely, especially when you're connecting things that are distant from each other.

Leo: Question 2 comes from Michael Renyard in Pennsylvania. He's already tried the "I'm recording you, too" experiment. Two months ago I had to call Wells Fargo about an issue that needed to be resolved. After being greeted by the all-too-common recording, "This call may be recorded, blah blah blah," a representative answered. I informed the rep, I, too, am recording the call. I was promptly placed on hold and then informed they did not authorize me to record the call. Thereafter the statement was repeated approximately every 30 seconds. I had to laugh. I feel what's good for the goose is - well, great show, guys. Keep it up. They didn't want the call to be recorded.

Steve: I thought that was interesting. Because we were talking about this and the whole issue of, well, just respond that you're recording it, too. And I didn't know that there were organizations like this who are prepared for people saying that. Obviously this is not the first time they've been told that, or they wouldn't have a button to press that immediately drops the person into a procedure for dealing with someone who's recording the call. And the only reason they would be repeating that statement every 30 seconds is so that it's going onto the record of the recording which is being made by the person. So I thought that was just - I thank Michael for...

Leo: So at that point you have only one choice, do business with some other company. Just say, hey, thank you, I'm taking my business elsewhere. And that's the real bottom line issue problem with Comcast and today's Internet service providers. They're monopolies. There is nowhere else to go.

Steve: Right.

Leo: You can't take your business elsewhere.

Steve: Right.

Leo: Joseph in Los Angeles reports that American Express has issued him a chip-and-signature card? Although my current Amex card doesn't expire till the end of 2015, I just got a new chip-and-signature card. The old and new cards are identical except for the chip on the front of the card. The card also has a 2019 expiration date. Prior Amex cards were generally only good for three or four years. My guess is they did the five-year cycle as the cards are more expensive. Unfortunately, there is still a mag strip on the card. Maybe the replacement card that comes in 2019 will be mag strip free. Yeah, I mentioned that I got a chip and - I don't know if it's chip-and-pin, chip-and-signature. I'm not sure what. But I got a card, finally for the first time got a card with a chip in it.

Steve: Yeah, I think we're going to begin to see that incrementally over time.

Leo: Well, we know it's required, right, by the end of next year.

Steve: Right. And I just wanted to say I have not yet done the deep dive into this that I plan to for the podcast. But in general, what the chip allows is an active response to a query. So that's what makes it different from just the mag stripe, which is necessarily passive. The mag stripe is fixed information which can be read, whereas the chip allows whether it's in conjunction with a PIN or not, it allows a challenge response, meaning that, for example, it can have secret information on it which is itself never made available.

And so that's the fundamental difference on a card that has an electrical contact-facing faade is eventually we'll put it in something; and if that something queries the card, it can challenge it for something the card knows which it never discloses, but it generates a response that's a function of the challenge. And so if you set up a one-time challenge,

then you get a one-time response, and that prevents replay attacks. And so fundamentally the problem with anything passive like the mag stripe is it's basically completely prone to any kind of replay because all you have to do is get your credit card number stolen, and so a, quote, "replay attack" is just reusing that number.

Which is why I'm having to change my card every few years is that websites that I use - less and less so now, I'll say, since more and more sites are supporting PayPal, which I really appreciate when a site allows me to use that, especially little mom-and-pop hokey sites. It's like, I'm just not going to give them my credit card information. Or Chinese sites or something. It's just, like I'm just not going to give it to them. I just can't. But if they say, oh, it supports PayPal, it's like oh, okay, good. That works.

Leo: I think it's now - of course it's going to be required. But that doesn't mean you don't have the mag strip. I imagine they'll do both for a while for just compatibility; right?

Steve: Yes. And in fact I'm glad you said that because I meant to bring that up. That's exactly the case is in order to allow us to phase over, right now nothing supports chip in the U.S.

Leo: Unless you travel, yeah. I'll be taking that chip-and-pin card with me to England at the end of next month because I'll need it. You go to a gas station in Italy, you can't buy gas if you don't have one because it's an unattended pump.

Steve: It really is weird, isn't it, that we're just so far behind in the U.S. It's another place where technology, we have a lot of belief in ourselves as the great source of all technology, but we do seem to move slowly.

Leo: Did you see that - and of course this is part of the issue Coin is going to have. Did you see they've delayed now their release for another few months?

Steve: And you know - yes. I have to say I'm interested in the technology. I ordered two because I want to take one, I want to delaminate one, take it apart, and I'll hold it up to the camera on the podcast.

Leo: I think it has an Arduino in it. I think.

Steve: But, I mean, it was very clear to me that the well-intended guy who was doing it, I mean, he was, like, learning to solder in the beginning of this. And it's like, okay, you know. And he was, like, wrapping coils around, I mean, he had a long way to go from having an idea and bringing it to fruition.

Leo: But I don't feel sorry for him because he got more than 20,000 people to send him 50 bucks.

Steve: No. I'm not feeling sorry for him.

Leo: And in fact, I feel like this is a little bit of - well, okay. But I was, you remember, I was very deeply skeptical of the whole thing.

Steve: Well, and I have to say of Kickstarter in general, I'm noticing...

Leo: This wasn't even a Kickstarter project. This was just a webpage that said "Send us $50. One of these days we might send you something."

Steve: Yeah, yeah. And again, for people who've never created a commercial product, there is far more to it than they expect. I'm getting email, and I'm sure you are, too, from the guys who are doing the Temperfect Mug. And they're, you know, we're still...

Leo: Yeah, I never got that.

Steve: We're waiting for it. And there's emails coming in. It's like, okay, well, here's what we've got now. And, oh, look, it's raining, so we had to put a new roof on the shack where we're doing the blah blah blah. It's like, okay. I mean, again, this is all a bit of a crap shoot. So I think ultimately I'll probably get something. And as a person who has brought many commercial products to market, I understand there is much more to it than anyone who hasn't done that before appreciates. So I'm very patient. And I recognize, too, it's like, okay, well, maybe it'll happen.

Leo: It's a little bit of a risk, that's all.

Steve: Yeah.

Leo: I'm still waiting for the NFC ring. I'm still wait- I have so many Kickstarter projects that have just never really been baked.

Steve: Yeah.

Leo: I forgot about that mug. I ordered one of those, too.

Steve: Yeah, I know. We both did. We ordered the good one, the one that was, like, extra, I don't know, it was black anodized or something fancy. Or maybe I did. I don't remember. But, and I love the idea that it does thermal storage; that when you put coffee in it that's too hot to drink, it immediately cools that off by absorbing the heat, but then it holds the heat so it keeps the coffee at that now-drinkable temperature for a long time. So it changes the temperature time curve in a way that we want. Love the idea. Would love to have one.

Leo: Some day.

Steve: We'll see. Look at that, a quarter of a million dollars. Well, they've got a lot to work with, at least. So now their shack has a new roof.

Leo: Yeah.

Steve: Yeah.

Leo: Corby in Reno, Nevada has now encountered a gas pump that asked for a zip code. I get that every day, or every time I...

Steve: I don't - yeah, I was so surprised. I think this is the first time he's seen that. And I'm thinking, wow, I've been doing that for years.

Leo: Yeah. I just used my credit card at a gas pump. It asked me for my zip code. This seems a very simple, reasonable method for two-factor authentication. Well, actually I guess it's really single-factor, which is still one more factor than most point-of-sale systems require. Why don't other point-of-sale systems ask for a zip code? Obviously, it's not perfect, but it sure seems much, much better than zero factors. It's two-factor. You have the card, that's one factor, and the zip, that's the second.

Steve: Right. There is a formal flag, as someone who implemented an eCommerce system, as I did for GRC, it's called "card not present," which a purely electronic transaction has to acknowledge, versus a physical "card present" transaction. So as you say, you have to have the physical card. Of course the zip code request is the card could be stolen, and the thief wouldn't know the zip code of the owner, presumably.

The reason I chose this question was this is a nice place to note that the reason this doesn't provide fabulous protection, and the reason point-of-sale systems, for example, where you do enter a PIN still have a problem, is that where the acknowledgment or the verification occurs, if you are upstream of that point, then your second factor doesn't provide you any protection. So, for example, there have been gas pumps that have been compromised, where the gas pump itself is spying on the user. So the gas pump just waits for the zip code to be entered and then bundles that up with the credit card information and sends that off to the bad guys.

So I guess my point is that the further back in the system you're able to authenticate, the further away from the user the better. So multifactors is good. But if the bad guys can catch and intercept all of the factors, then it really doesn't provide you much protection.

Leo: Yeah. Bart Busschots in Maynooth, Ireland - I'm sure I'm saying his name wrong.

Steve: Looks good.

Leo: B-U-S-S-C-H-O-T-S. I bet you got a billion of these already, but you made a wee booboo when describing free certs from StartSSL.com. They are not "no better than self-signed certs," and they most certainly are recognized and trusted by browsers. The validation is a standard email loop. You have to prove you control the domain before they'll issue you a cert. So you mean if I use my Yahoo.com email address, I can get a cert for Yahoo.com? There are some important asterisks to the StartSSL free certs though: non-commercial use only; all free certs are for 1 year so you have to renew them annoyingly often; all free certs contain exactly one SAN name.

In other words, the cert is good for your domain, and your domain with the www prefix, but you cannot specify other service alternative names like, say, images.twit.tv. For people running charitable sites or personal websites, this is a good option. A lot of these sites use CMSes like WordPress and Drupal and Joomla, which means there are usernames and passwords whizzing around in the clear needlessly. If Google helps push these kinds of sites towards free SSL certs, that's a good thing, in my opinion. Also, with the death of Windows XP, or the death of IE6 to be more precise, all versions of IE now support multiple SSL VHosts on a single IP address, so the days of having to pay for a dedicated IP address to enable SSL are over at last. So the timing is good.

Keep up the good work. And every time I hear you plug SpinRite, I remember that it got me a bottle of very good single malt Irish whiskey - he didn't share that with you, Steve - as a thank-you for using my licensed copy to rescue a conference at the 11th hour, smiley face. That's sweet.

Steve: So I went back, and I cannot find where I saw the note that I referred to when I apparently incorrectly disparaged StartSSL certs. First of all, I called them STARTTLS, which that was a problem because we know STARTTLS is the protocol used for protecting email. I corrected that a couple weeks ago. So I appreciated Bart's note about StartSSL, and a number of other listeners wrote about it also. And I, again, for the life of me I can't find what it was that I saw, that I'm sure I saw, but maybe it was older. I did find some 2011 notes about Android 2.1 not supporting StartSSL. And there was a problem back in the past with Mozilla and Firefox. But nothing contemporary.

So I want to fix that because for people for whom this makes sense, as far as I can tell, as Bart says, StartSSL browser support is universal. I looked at StartSSL.com, the site where you can get these, and they advertise absolutely universal browser support. What you need to do in terms of an email loop is you need to demonstrate domain management, typically by being able to respond to webmaster@yourdomain.com. And so it would be difficult for you to get webmaster@yahoo.com, we hope. We hope that email address is actually in use by the actual webmaster of Yahoo.com. But that's the way that the process operates.

And in some cases, if you are unable to, for whatever reason, control the email for your domain, they can provide you something which you put on your site, which you then give them the URL to. So again, you demonstrate that you have a means of controlling the content on that domain, which then essentially allows you to qualify for a cert.

So noncommercial use, you have to do it annual. But if you don't want to pay anything, everybody recognizes these certs, and so it is, for the slight overhead of dealing with it

every year, it's so far as I can tell 100% useful. Although, again, you couldn't protect email.domain.com. As he says, only domain.com and www.domain.com. But for your typical website, that's enough. So thank you, Bart. And I want to thank everybody for giving me the opportunity to correct that because I incorrectly stated that there were some people who did not handle them, and I can't find that now.

Leo: Richard in Calgary, Alberta wonders whether we're concerned about password strength. Listening to...

Steve: Confused, confused.

Leo: Confused, I mean, yes. Listening to the discussion on password strength in the last episode, it occurred to me you've never distinguished between online and offline attacks. The password protecting an encrypted file should be much stronger than the password protecting the login for an account. I think you discussed the distinction in an earlier episode, but the distinction seems to have been forgotten. Just my two cents. Did you forget?

Steve: No. So here's the problem. In order to move things along, in order not to have to describe essentially the underpinnings of everything we talk about whenever we do, I sort of have to assume some knowledge is in evidence.

Leo: Yes.

Steve: And for what it's worth, I am never, never talking about online login password strength, that is to say, the idea of someone guessing your online login by successively entering passwords in the browser, because that's just not practical. I mean, anybody could, I mean, most sites are going to have some sort of a lockout. If you guess wrong 10 times, they're finally going to say, okay, look, call us, or do something. Obviously, I mean, and that's where they've got the little "I forgot my password" link. All of our discussion, even in the context of online passwords, is about the theft of their database, which is the problem that these sites all seem to have sooner or later is they lose control of their password database, which is then an offline, high-speed attack against that database.

So I apologize, Richard, and to anyone else who was confused, if I'm not clear about that. But that's sort of the background behind this is nowhere are we talking any longer about the idea of someone sitting there trying to guess someone's password by successively trying to log in. Normally you get locked out after some period of time. And even if you don't, just the turnaround time of how long it takes to produce a guess and be declined makes it completely prohibitive of, like, doing a brute-force attack on their account. It's generally that you have found that database offline, and then you just blast at it with an offline attack.

Leo: Or to say it more simply, we always use the worst-case scenario, not the best-case scenario.

Steve: Right.

Leo: Which in security is probably the right thing to do. Hey, if everything goes well, you'll be fine.

Steve: But if no one - and in fact just use the password "monkey." And if no one tries...

Leo: You're great. You're good.

Steve: You probably will be fine.

Leo: I think that's just - we use the worst-case scenario when we talk, and we just assume....

Steve: Well, and that's, I mean, security, as we have often said, is about the security of the weakest link. So that's what that's about is the strength of the chain is which link is going to break when you put it under stress. So, yes.

Leo: Babak in Dubai makes a very good point about password change policies. Long-time listener to the show. Thanks for the great podcast. Episode 468 you discussed - we dismissed, I will say...

Steve: Yes.

Leo: ...password change policies. But I think you forget about the most important benefit they provide: They protect the user from someone else accessing their accounts over an extended period of time without their knowledge. And this is a good point.

Steve: Yes.

Leo: Your credentials could become compromised once; then the person who obtained them will continue to be able to access and read your emails and transactions for many years to come. A password change policy is not completely pointless and limits this risk.

Steve: Yeah, I actually was put in mind of this of my mom, who's had the same password protecting her, air quotes on "protecting," forever. And she's given it to pretty much all the various members of the family at one time or another when she needed them to do something. And so if any of them have any interest about anything going on in her life at any time, they can just log in as her. And that just, you know, just makes me close my eyes and think, oh, goodness.

But if Mom were changing her password ever, then she would be shedding those other members of the extended family who may very well be poking around and seeing what's going on, to my great dread. So I think Babak makes a very valid point. This of course is in the context of the policies which require people to change their passwords periodically. So, yeah, thank you.

Leo: Yeah. This is from Martin in Frankfurt, Germany: I'm an on-and-off listener to Security Now!, recently purchased SpinRite just to try it out - have had no problems, knock on wood - and of course to support the work you do. I've run it on all my drives on Level 2, and to my great surprise it did not report any problems. Lucky me, I guess. But the actual question is about how running SpinRite on Level 2 fixes people's problems. I might have missed the explanation in one of the podcasts I haven't listened to, so maybe you can explain it again, please. I understand Level 2 is a scan of the drive, look but don't touch. So how could it possibly fix anything? Which piece have I missed to understand how running SpinRite on "only" Level 2 helps with problems? If Level 2 already fixes issues, what are the benefits of Level 3 and 4? Good question.

Steve: So I didn't talk about that last week, so I appreciated Martin's question. The look-but-don't-touch Level 2, it does several things. First of all, in the IDE specification, there is lots of control over sort of maintenance-level modes over things you can tell the drive not to do. You can tell it not to retry before it reports an error. So that makes it much more sensitive to trouble. You can tell it, first of all, obviously, not to cache, and so that prevents it from reading data ahead. So there are a number of things that SpinRite does that increases the drive's sensitivity to problems.

And then the other thing is that, if the drive, when reading a sector, encounters an error which is becoming long enough to be worrisome, remember that error correction is able to correct problems up to a certain length. Contemporary drives do error correction as a matter of course now. The densities are so high that drives are just expecting to have problems reading the data all the time. So drives will ignore correctable errors up to a certain length. And then, if the error sort of grows over time, as errors are known to do, called a "grown defect," if you put grown, G-R-O-W-N, as opposed to G-R-O-A-N, "grown defect" into Google, you'll find, wow, the world knows all about this. The defects tend to increase in size.

So at some point, even when you're just doing a read scan, SpinRite allows the drive to fix these problems itself. This is exactly how it fixes flash drives and thumb drives, with the same technology, is just giving the drive the chance, when it's being told to be extra picky, don't do rereads in order to get a read which is good, but fail on a single read, and when you do that, fix the problem right then. So it's very possible, essentially, cranking up the drive's sensitivity to problems, which SpinRite does, then making a pass across the drive allows the drive to find problems which are nascent and growing and fix them before they get to a point where it's then going to have problems.

And as for the writing tests, it is also the case that defects interact with the data written on them. Say that you wrote a zero over a spot where there was a defect. Well, when you read it back, it would be a zero. So the drive wouldn't see that as a problem. But if you wrote a one over that spot and read it back and got a zero, now that's a problem. Which is to say that data interacts with defects. So what the higher levels of SpinRite do is they invert all of the zeroes and ones, write them, read them back, invert them again, write them and read them back, in order to make sure that all of the areas of the drive are able to hold both ones and zeroes.

That is an oversimplification because the data we write no longer really maps into the flux reversals that are stored on the disk. But at least this is something that sort of exercises the surface and verifies that not only the data we've written, but also the inversion of that, is able to be safely read and written on every spot of the drive, and then we move forward. So it takes a lot longer, but it sort of does a more thorough scrubbing and analysis of the surface. So that's how a look-but-don't-touch can provide benefit, and also what the deeper levels do.

Leo: From Matt Reyes in Tracy, California comes this question: I have several servers in our environment here, and I'm wondering how SpinRite can help us out. As expected, they are all in RAID arrays. Hmm. What's the best means of running SpinRite in a RAID environment? Will 6.1 support RAID?

Steve: Unfortunately, almost certainly not. And it's another thing I didn't touch on. I coined the term "thin RAID" to refer to the motherboard-based RAID that, for example, some of the Intel chipsets support, where you don't have a third-party RAID controller plugged into a slot. But you just have sort of RAID, typically 0, 1, and 5 are supported by the motherboard. And you'll have RAID drivers that are available. And so the idea is that basically those are just independent IDE, you know, SATA ports, which drives are plugged into. And then once the OS is booted, it runs a native driver that essentially does RAID in software.

SpinRite can see all of those separate drives with no problem at all. So you can run SpinRite individually on those drives, in a so-called thin RAID, and get all the benefits of SpinRite. But in any instance where you have a server which probably has a physical RAID controller, the drives are - and there's no visibility for, like, into the drives from the software or even from the hardware. That controller is pretending, it's got a processor on it, and typically cache, and its own RAID controller and buffer memory. And it typically costs a couple hundred dollars. And so that's a serious piece of equipment which is itself pretending to be a drive.

So from the first moment you plug this in, the motherboard, the BIOS, the OS, everybody sees this as a drive. And the OS probably has a driver to allow enhanced performance and to interact with the RAID controller and monitor the health of the RAID and the drives, which it's able to provide through additional interface. But SpinRite, from the outside, SpinRite sees it as a single drive. And frankly, it does no good to run SpinRite from that view of the drives behind the RAID. If there's a problem, and many people do have problems where the RAID breaks and they need to then run SpinRite, so people do this. But you have to unplug the drive from the RAID controller, plug it directly into the motherboard, where SpinRite can then see it and then run on it and repair it. And then of course put the drive back.

Leo: Yes. Ladies and gentlemen, our very last question - and this sets us up for next week, apparently - from John Andrade in New Port Richey, Florida. Steve, what are your thoughts on Matthew Green's statement on PGP? An article just published on the Hacker News website talks about Matthew Green, who's a famous cryptography dude, and his take on the future of PGP. Have you read his blog? I'm pasting a link to the article. I'd be very interested in what you think. It's in CryptographyEngineering.com. Perhaps you'll talk about this on an upcoming Q&A or a normal show. Thanks, Steve. By the way, proud owner of a copy of SpinRite 6, a real lifesaver. Stay true to your roots and never change or bend for anyone's

interests. We depend on you, Steve.

Steve: So this was on my radar. And I thought this was a perfect segue into next week's podcast. Matthew Green, whom we have spoken of often, he is a well-known cryptographer. Johns Hopkins, as I recall.

Leo: Yes, JHU, yes.

Steve: Yup. And he essentially raises the question: PGP was designed right, but is it time maybe to consider an upgrade? Many things have happened since, for example, the addition of elliptic curve cryptography with its very conveniently short keys. And PGP, beautifully designed, maybe it's time to take another look at it and ask if it's the best we can do today. And I think that would be a great topic for next week's podcast. So that's what we've got lined up for next week.

Leo: Good, yeah. I actually moved from PGP to S/MIME because PGP was confusing the heck out of people I sent email to.

Steve: Yeah.

Leo: It just - nobody could figure it out.

Steve: Yeah, and I really think S/MIME makes a lot of sense because it does have the advantage of being built into the underlying protocol and just being sort of supported natively more and more.

Leo: Right, right. Steve Gibson is at GRC.com. That's where he hangs his hat. It's called the Gibson Research Corporation because of it. You'll also find lots of cool stuff there, not just SpinRite, the world's best hard drive maintenance and recovery utility, but also a lot of freebies. Steve's giving away stuff all the time, including, yes, this show. He has 16Kb audio for the bandwidth impaired and full human written transcriptions so you can read along as you listen. That's at GRC.com. You can leave questions for Steve there, as well, GRC.com/feedback. And you'll find a lot of freebies, and it's a great site just to browse around. It's become more and more a compendium of interesting stuff that Steve likes.

We have full-quality audio and video at our site, TWiT.tv/sn. We put this on YouTube. You can share it with friends and family: YouTube.com/securitynow. And you know, if there's a little particular part of the show that you want to share, you know you can do that in YouTube. You scrub to the part you want, click the "Share" button, and then you can share by time. And they'll get a link that they just click, and it jumps right to that part. I don't know if people - if that's widely known. But that's very useful.

Steve: Yeah, very good point.

Leo: You can also subscribe to the show in all the different podcatchers. Just search for TWiT or Security Now!. You'll find it. That way you'll get it each and every week. Next week PGP, and what could be better? Thanks, Steve. We'll see you next time.

Steve: Thanks, Leo.