SECURITY NOW!

Transcript of Episode #383

Listener Feedback #157

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-383.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-383-lq.mp3

SHOW TEASE: It's the last Security Now! of 2012, and we've got a bunch of good questions for Steve Gibson. He'll talk about a brand new version of Java, too. Does it address the security concerns previous versions have? We'll find out next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 383, recorded December 19th, 2012: Your questions, Steve's answers, #157.

It's time for Security Now!, the last official version or episode of 2012. With us, of course, our Explainer in Chief, Steve Gibson, the man in charge of security here at the TWiT Brick House. Hi, Steve.

Steve Gibson: Hey, Leo. I have to apologize in advance...

Leo: Oh, no.

Steve: ...if any Yabba Dabba Doos are heard in the background. I changed my whole environment around and changed AV receivers. And I used to have a remote control set up so that I could just easily mute the monitor of the servers at GRC whenever I want to. And this morning, when I pressed the remote control button, the remote itself is no longer emitting the IR signal that my system receives in order to mute. So I pressed it, like, a few times. It actually started to act up yesterday. And so I think it's just dying finally because I've been pressing that a lot for many years. So we've got Fred not muted, and there may be a Yabba Dabba Doo that we hear in the background.

Leo: Steve, you're missing a great opportunity here. If anybody would like to hear Yabba Dabba Doo, all you need to do is purchase a copy of SpinRite from GRC.com.

Steve: It is in real time.

Leo: Is that what Fred does? He's signaling a credit card purchase.

Steve: Precisely, the transaction with the merchant that moves the funds from a purchaser's credit card into our merchant account.

Leo: Well, you would go Yabba Dabba Doo. It's here. The money came.

Steve: Always good news.

Leo: So this is our last episode of 2012. Very fitting, we're going to do a Q&A episode. We should let you know, we will have a new show next week, but it is not new content. In fact, it's pretty stale.

Steve: Well, I can't remember whether we talked about it on air, so to speak.

Leo: I think we did. I think we did, a couple of weeks ago.

Steve: During the recording last week, I think so.

Leo: Yeah, yeah.

Steve: So our regular listeners already know that they're going to get a wacky special Christmas Security Now! episode, a video recording made on analog tape, the Sony Hi8 format, back before we had DV or anything digital, 22 years ago, when I had black hair and lots of it. And it's really entertaining. I will say again, although I said this at the beginning of the little chunk that we just recorded for that, you really need to see this. So unfortunately, 22 years ago, I didn't know we'd be doing an audio podcast, and so I make a lot of use of waving my arms around. And if you're just listening to it, you won't know why they're all laughing at me. And, that is, the audience of this.

Leo: Oh, yes, they will. Oh, they'll have an idea.

Steve: Yeah. So anyway, if you can, over the holidays, track down the video from Leo and watch it because I only have the audio.

Leo: How did you convert it? Did you have to buy something to convert it with?

Steve: Yeah. I had the original camcorder that I used, a Sony Hi8 camcorder. So the first thing I did was put them back into the same device that originally recorded them. I got nothing. And so I thought, okay, either we overwrote these - and it's very possible that we would have put the lens cap on and hit record and wiped them out in order to clean the tapes, get them ready for something else. So I was worried about that. Then I remembered that when my dad died, he had a Hi8 deck which I had grabbed. And so that was in the garage because I never throw anything away if it might be useful someday. So I pulled it out. And it sucked the cartridge in, but it failed to go to the next phase and wrap the tape around the helical scan head. So I tried that for a while, and I said, okay, that's dead, too. So now at least I can discard two devices that I didn't know were dead. So then I went to Amazon, thinking - or maybe it was eBay. I think I went to eBay first, and then Amazon, and I found a used Hi8 camcorder in, they promised me, like-new condition for $199. So...

Leo: Yeah, it better be like new for that price. Holy cow.

Steve: Well, I figured this was for a good cause. So I purchased it. It arrived. I put the tape in, and, oh, there - well, I don't know that I was blessed with seeing my image from 22 years ago, but at least there I was. So then I have a - I can't remember the name of the company. There's a really good, well-known - oh, Canopus.

Leo: Oh, Canopus, yeah.

Steve: I have a Canopus...

Leo: Yeah, the ADVC. We use those, yeah.

Steve: Yup. I've got a couple of those. And so I ran the analog video from that through the Canopus to turn it into DV, digitized it to hard drive. Then I used my old version of Pinnacle Studio that I have kept for years because they ruined it. And this was when it was lightweight and fast and everything. And I put a little title on the front, and trimmed it, and then digitized it, and then I ran it through TPMG, the Pegasus Inc. encoder...

Leo: Gosh, I forgot about that, yeah.

Steve: Yup, still there.

Leo: You've got some old stuff there.

Steve: Really a good one. And that converted it to a relatively high-bandwidth MP4. I think it was 700MB. It's about 45 minutes long. And then I shipped that up via Skype, of all things, to John at your studio. So you guys have the content.

Leo: That's fantastic. Well, that's for next week. This week we've got a Q&A, our 157th.

Steve: Interesting news and great feedback from our listeners, as always.

Leo: Well, why don't we get into the industry happenings, and we'll get to the Q&A in a little bit.

Steve: So, huge news, at least that's what you would imagine from the industry's reaction to it. I'm a little less impressed. And that is that Oracle late last week updated Java 7 to update 10. Now, 6 is still there. And they're doing security enhancements to 6 and 7 sort of synchronously. This is a change only to 7. And I got a kick out of seeing a comment, I think it was Adam Gowdiak - I think his first name is Adam, I remember it's Gowdiak - who is a Java security expert whom we've spoken of in the podcast before, who has found all kinds of problems over time in Java. His comment was, well, okay, you're still probably better off staying with 6 because Java 7 is so ripe with security flaws that even this recent change probably isn't going to help you. So here's what they did, and it is amazing. They have - oop, I just heard the cash register sound, so we're going to - yeah, there's Fred.

What Oracle did is, for the first time ever, in Java natively, in itself, under the security settings of the Java Control Panel - which, for example, Windows users can get to, under the Control Panel, there's a Java Control Panel applet. If you've got Java installed, you, right there, can completely disable it from your browser, from all access to your browser.

Now, we've been talking about how to do this the hard way and the easy way and various ways. Various people have posted how-to's on their websites or their blogs and pages, how to disable only your browser's access to Java because, as a runtime engine, as a virtual machine, Java gives you cross-platform. There are many things to appreciate about the flexibility that it provides, especially as a corporate development language. But the problem is, normally when you install it in the system, your browsers get it, too. So Oracle has themselves finally stepped up and said we will let you turn off browser access.

Now, the reason I'm a little less impressed is, first of all, it's not clear that blanket disabling it, I mean, while that's best for security, if you do have a need for it in a particular app, for example, I keep hearing, whenever we talk about this, people in Sweden talk about how their banks all require a Java applet in order to do online banking. Ugh, okay, well, but that's the way it is. Or many people will say, oh, all of our corporate middleware that our programmers do is not only in Java, but is hosted by the browser instead of an external container of some sort. So there are instances where you have to have it on the browser.

So if all you have is an all or nothing, then you're back to this problem of, well, if you turn it on to use it, then you've got to remember to turn it off when you don't want it and so forth. And my point is that something like NoScript in Firefox already does that. NoScript won't let Java run unless you explicitly give it permission to do so. And then you of course can train NoScript to always allow your Intranet to run Java where the Internet would not. And you could, if you had sites on the Internet that you go to, like your banking sites, you might, with that granularity, stickily, persistently enable them to run

Java, but generally not anything else. So that's still probably the right way to go. But this represents a step forward.

The other thing that unimpresses me is that this normal control, you are able to do blanket, all or nothing. But they also provide sort of a four-step security, like low, medium, middle or something, I don't remember what the third one was, and high, where you're able to choose different sort of scales of settings from the control panel, but that only applies to unsigned Java applets. That is, anything signed or even self-signed is permitted to run unencumbered.

So the problem there is that, if this caught on, and if this became significant, then Java exploit malware would simply be signed. It would be self-signed. And so right now it's not because no one bothers because it's an additional headache. But we've already seen instances where malware is using stolen certificates. It wouldn't even need to be stolen. They could just be digitally self-signed, and this would pass right through. And of course Oracle is not by default going to use the kinds of settings we would suggest. They don't want to suddenly have a release that breaks things.

So these are - that's the other problem, of course, is as I coined the term "the tyranny of the default," is while all this is here, and it's better that it's here than not, because security-conscious users will be able to turn these things on, crank up the security to high setting, and/or use a third-party tool in our browser to give us more granular control, all of that only happens for people who make those changes. Unlike, for example, what Facebook is now doing, of moving people to SSL by default, even if they've never made the change themselves, which is really nice. Of course, that's solving a different problem. This is a serious problem.

And, of course, all of this is only because Java is a security catastrophe. I mean, it's just like the No. 1 exploited add-on, across-platform add-on, that malware authors go after because it just has - it's so powerful, so complex, there are side effects to the way it was designed that are, I imagine, Oracle's going to be chasing forever. And the fact that 7 is so much worse than 6 demonstrates the other rule that we've often spoken of, which is that new is not necessarily better from a security standpoint. New will give you more features, but every additional set of features is more opportunity for bugs to be hidden in there that can be leveraged and turned into vulnerabilities.

So I certainly wanted to cover this because it's been in the news. It's a nice step forward for Oracle, and I hope they're spending as much time just trying to make it more secure, rather than acknowledging the fact that it isn't. I mean, it's a big acknowledgment that they're saying we're going to allow you to disable it from your browsers. It must have come from corporate pressure. I mean, it's not we little end users that they're worrying about.

Leo: Well, it's a little embarrassing for Oracle.

Steve: Yeah.

Leo: I mean, that could be some of the pressure, too.

Steve: Speaking of embarrassing, Samsung, it was revealed over this past weekend by a nice little hacker, had essentially a deliberate kernel bug which was found which affects their more popular smartphones, the Galaxy Note 2, the Galaxy S2 and S3, those based on the - and I don't even know how to pronounce this, the...

Leo: Exynos.

Steve: Exynos, that's what I would have guessed, or something like that, the Exynos processor and chipset.

Leo: I don't know if you could blame Samsung, though. It sounds like it was an Exynos bug. It's a kernel bug.

Steve: Well, it's in the kernel. But apparently it involves the graphics portions, the aspects of the kernel or the add-ons that want access to graphics memory of various sorts, the camera and HDMI subsystem and so forth. In the UNIX world, they've done something that was really nice and clever, which was all of the resources appear to be in the common hierarchical file system. So, for example, you've got your regular drives and subdirectories and files. Those are in the hierarchical file system. But something, even things that weren't actual objects, like random numbers, the random number generator is you access it as if it were a device, an object in the same unified hierarchical file system. And Linux, being a functional clone of UNIX, took that same concept. So that exists in the Linux world, too, and thus in the Google-derived Linux core smartphone technology.

Anyway, there's an access to physical main memory, which is /dev/mem. But of course that is so powerful because anything that opened that device could have access to all physical memory. So it is locked down tight so that only root privilege devices can do that. Only other kernel-level and sufficiently privileged processes are able to open the /dev/mem pseudo device to give them visibility, read/write access to main memory.

Well, what this hacker "alephzain" found and he posted, it was kind of cute. English is not his first language. He said, "Hi. Recently discover a way to obtain root on S3 without Odin flashing," Odin being the Norse god, the main Norse deity. And Odin is the No. 1 popular means for rooting these devices. He said, "The security hole is in kernel, exactly with the device /dev/exynos-mem. This device is R/W" - meaning full read/write access - "by all users and give access to all physical memory ... what's wrong with Samsung? It's like /dev/mem but for all."

And then he enumerates the libraries that he has seen that are accessing that device. And he says, "Many devices are concerned" - and I'm thinking, and many users, as well - "Samsung Galaxy S2, Samsung Galaxy Note 2, Meizu MX" - whatever that is - "potentially all devices who embed exynos processor which use Samsung kernel sources." Now, he sums up his post, "The good news is we can easily obtain root on these devices, and the bad is there is no control over it."

Leo: Yeah, it even works on root-locked Galaxies from Verizon.

Steve: It's a complete short circuit.

Leo: Unfortunately, this guy published this proof-of-concept code, the code to do it, without letting anybody know at Samsung. So the good news is Samsung responded right away, and I'm sure that we'll have a patch soon.

Steve: Yes.

Leo: I have one of the affected phones. You know what's interesting, though? He's right. I now have a - there's a very easy download root, which I ran, and it rooted my phone. And by the way, the root exploit has a feature to turn off this kernel exploit.

Steve: Yes, yes.

Leo: So it's one way to secure your phone, if you trust these guys.

Steve: Yes. There are already public patches to fix this because, I mean, it is just a mistake. And you'd have to go back through and do a forensic analysis of the development path, whether the developer quickly created this, intended to lock it down so that only the sufficiently privileged devices or processes had access, and just forgot? I mean, that has to be the case. So it's just one of those things that is lurking in the Samsung phones ever since this chipset was introduced, and apparently having to do with graphics access, and, whoops.

Leo: Ooh, hello. I got this from Chainfire. I've bought some of his software before. It's on the Play store, so I kind of trust him. And it's nice because it means you can root all of these phones by just running an application, and it has a little checkmark to disable the exploit. So you can protect yourself that way. Probably, though, most people will want to wait until Samsung issues a patch.

Steve: And for what it's worth, they're on it big-time. I mean, as we have just seen, this is a trivial fix. So as quickly as a company with the bureaucracy that they have, and their needs to verify they don't break something else, and it's done right and so forth, as quickly as they could move, they will. But you're right. For our listeners who want to - the overall take I've seen, the consensus seems to be, if you don't download sketchy apps, you're okay. And certainly since this became known on the weekend, there's no doubt that sketchy app land is going overtime right now to incorporate this and put stuff out in order to try to get access to as many phones as they can before this gets locked down.

Leo: Probably the smart thing to do would be not download any new apps, from Play store or anywhere else, until there's a patch. And that way you're probably all right.

Steve: And if you have to, then fix it yourself, as you just said.

Leo: Yeah. If you go to XDA Developers, the code to root it is easy. I mean, that's the side effect, it's great, is it's a one-click root now for all of those phones, the Exynos 4-based phones. That's easy.

Steve: Yeah. You might want to bring this link up, Leo, while we talk about it.

Leo: Sure.

Steve: Under the category of YAC, which stands for Yet Another CAPTCHA, we have MintEye, at Minteye.com.

Leo: This is hard.

Steve: And, well, okay. So it's kind of clever. What their pitch is...

Leo: Oh, I get it, I get it.

Steve: ...that you just have a slider, and the slider changes a distortion, like a single-point sort of sinkhole gravity spiral distortion of an image. And as you slide the slider back and forth, it winds this distortion one way or the other. And your goal as the "prove you are a human and not a computer" is, looking at the image, we can instantly tell what our slider is doing. And but the clever part is they're suggesting that sites that want to protect themselves with CAPTCHAs also tie into advertising networks.

Leo: That's what's interesting about this is these are ads, once you solve it.

Steve: Yes. And so it's also clearly got your eye on the ad so you don't glaze over and don't focus on it. Basically you're resolving an advertisement yourself, and you have to in order to move forward. Now, the thing that doesn't impress me about it is that the slider has only 30 settings. And 30 is not a big number, as we know, which means that something that was just trying to brute-force post on a forum that was protected by this could just choose a random setting for the slider, and one 30th of the time it's going to succeed. That's the problem with this solution, as opposed to - and they talk about the impossible-to-solve CAPTCHAs that we have all encountered. I mean, some of these things, they make you feel like it's your fault that you cannot possibly figure out what this heavily distorted string of characters is supposed to be.

And they quote some statistics, like a failure rate of 75 percent by people and a success rate of 30 percent by computers for old-style CAPTCHAs, the distorted text CAPTCHAs. And they talk about a 98 percent success for people of their untwist-the-twister, the twisted-up ad approach. So anyway, I wanted to bring it to our listeners' attention because it's kind of cute. I also do think that this would not be difficult for a generic image algorithm-based solver to find. And there does also seem to be sort of a dead spot on the proper solution. As I was moving the slider back and forth, it unwound, but it seemed to kind of like the correct setting more than the other ones.

Leo: It's stupid. This is just a way to put an ad on the page. And we know that anything a human can solve can be solved because you just redirect the CAPTCHA to a human and let them solve it.

Steve: Yeah, and actually this one would be really quick to solve.

Leo: Yeah, it'd be fast.

Steve: You'd be real good at unspinning the thing.

Leo: Truck through these, yeah.

Steve: While going through our mailbag yesterday for our Q&A, I found a note from Bryan in Carlsbad, California. And I liked this because it was a follow-up on remember that we talked about FreeBSD having discovered that their servers had been - I think two of their servers had been compromised, and they were very worried over anyone who downloaded FreeBSD between two dates could have been subjected to an unknown exploit because they had not yet had a chance to figure out what was going on.

So he wrote, "Hi, Steve. Regarding the news of intrusion at FreeBSD servers you reported in Security Now! 379, I shared with a colleague who reported back to me with a November 22 update" - which I had missed, which is why I wanted to share it with our listeners - "stating: 'Verification of CTM-sourced trees has been completed against the Subversion tree, confirming that there are no differences between the two. Our experimental Git repository has been similarly verified.'" So it looks like that is okay. No one who did get FreeBSD during that time would have risked being in trouble.

I wanted to give a moment for an update on the Quiet Canine project. About a hundred of our listeners so far have reported problems with dogs and an interest and willingness and in some cases, I mean, they're, like, to their wit's end. They've bought all the other devices available. None of them work. They're, like, on the verge of moving because the neighbor's barking dog problem is so bad. There's one person who's being harassed by Chihuahuas that, like, run around him, and he's sure that, if he didn't keep his eye on them, they would nip him. And having read all these, I found that my feeling about the problem has evolved.

I mean, I don't have a dog problem. As we know, my best friend Mark does, and we solved it. I was telling you before we began recording, Leo, that he's only had to use that megablaster unit that I first built for him a month ago three times. But when he does, and it's just with the merest little blip that he sounds it, these two little collies, he said it's like the Keystone Cops with them, like, crawling all over each other, trying to squeeze both of them at the same time back through the doggie door that only has room for one of them. And he says it's pretty funny because, I mean, they just - they absolutely want to leave the area.

Leo: We should underscore this isn't harmful to the dogs or even distressing to the dogs, it's just like shouting at them.

Steve: Yes. Well...

Leo: And it surprises them.

Steve: I think it's better than shouting because shouting will anger them and upset them. This is alien. This is like nothing in their experience. It's completely foreign. And so it's the surprise value. It's the "What the heck is that?" And so they just want to get away. I mean, yes, he's doing it from his second-floor window down to the ground floor, so it's not at all harmful. And believe me, they don't stick around.

So where I am at the moment is we had a huge breakthrough this weekend. The design no longer uses or needs a microcontroller at all. It's self-oscillating rather than needing to program a microcontroller and use that as the oscillator. The parts cost is now less than $5, including the tweeter. It costs more for shipping than it does for the parts. And people are building them. I'm seeing pictures now. One guy built one into a flashlight form factor that he calls the "Canine Flashlight," I think. Or I think that's what he called it. But it's still in flux.

I've seen some complaints from people who talk about how disorganized the group seems, and he just wants to get a parts list. Now, Leo, I put some links here in the show notes. You can bring them up for people who are looking at the video. You can see that I have the wave forms that it produces that I was staring at last night, and I managed to reduce its power consumption by a third so that it will last 50 percent longer than it would have before. The schematic exists and the parts list and so forth. But it's still in flux.

http://www.GRC.com/tqc/TQC_v2.1.png

http://www.GRC.com/tqc/TQC_Waveforms.png

http://www.GRC.com/tqc/TQC_v2.1_Schematic.pdf

So for everyone who is interested, I mean, I've seen some neat mail. There are some parents who, because this is so simple, think it would be a great project to work on with their kids to sort of introduce them to electronics and electricity and so forth. And it would be because it is so simple, and it does something.

All of this will end up being organized and living at GRC. So the Google Group only really makes sense for people who are actively following the postings. You can't just sort of come by and, like, have everything laid out for you. I will be doing that at GRC as soon as this settles down. But I'm still making changes. Just yesterday, as I said, I reduced its power consumption by a third. So it's too soon. For people who want to be on the bleeding edge, people are building these things and providing feedback. But there will be some blood. So, I mean, if you poke yourself with a resistor lead.

Leo: The dogs will not bleed. I just want to emphasize this.

Steve: No, no.

Leo: There's no bleeding dogs in this.

Steve: No. So anyway, I'm really, when I'm listening to people who are being bitten, and we have mail carriers who are really being harassed, and people who, I mean, their life is being ruined by a next-door neighbor dog who is out in the backyard all day long. Sometimes someone lets their dog out at 2:30 in the morning, and it starts barking. They've got newborns that cannot sleep that are being awakened at all hours by dogs barking. I mean, it's just - I really developed a much better sense for that we're the victims, unfortunately, or oddly, in this. Which seems so counterintuitive. But it's just dog barking is a huge problem for people.

So anyway, I don't know how this is going to develop, where this is going to go. I don't really want to be in the hardware manufacturing business. I was there once with the light pen, and I did that. And I don't think that's where I want to be. So I'll play this by ear. I'm committed to building some prototypes for our listeners because I want to find out whether this is effective. That's the next step. So I'm just sort of taking this one step at a time. I want to see, like, do dogs get used to it? Is it initially startling but not after a week or two? Can dogs be trained? People want to - I would say it's about 50/50 neighbors' dogs and people's own dogs who have some behavior that they want curtailed. So I just don't know yet, but that's the nature of research and development is we'll just go one step at a time.

Leo: Awesome.

Steve: You and I discussed, before we began recording, but I wanted to for our listeners, that you finished Season 2 of Homeland.

Leo: Yeah. We're not going to spoil anything here.

Steve: Which you could have only done on Sunday because I put this note in the show notes because Season 2 just finished, and I wanted to say, at no point was this a disappointment.

Leo: What a great show. What a great show.

Steve: Yeah. So I'm sure there will be...

Leo: That's all we can say.

Steve: I'm sure there will be a Season 3.

Leo: There is going to be a Season 3 because they did a little piece at the end with the showrunners. This is on the Showtime Network. Showtime has a showrunner show. And he talked about next season and what might happen.

Steve: Oh, I've got to go find that. I didn't see that, Leo.

Leo: It's on the on-demand portion. Yeah, he said, basically - no, I'm not going to say anything.

Steve: Okay.

Leo: Because you shouldn't watch it because it does - it is a little spoiler-y.

Steve: I have heard through Twitter and through email, many people who have been induced to see it are thanking us for bringing it to their attention. They're really, really liking it. So for what it's worth, I think it's an entertaining program.

Leo: Yeah, quite...

Steve: Speaking of entertaining.

Leo: Yes.

Steve: I did run across a note I wanted to share because it ties into sci-fi and one of TWiT's sponsors, Audible. James Tisdale in Waterloo, Ontario, Canada wrote. The subject was "David Weber's Honor Harrington Books - Blessing or Curse." And of course that subject got my attention. He sent this on the 12th of December. He said, "Hi, Steve. I've finally gotten around to taking your suggestion to," he has in quotes "read," he says, parens, "(I listen to the audio books) David Weber's Honor Harrington books. I've gone through the first three books so far, and each one has me wanting more. As I am 'reading,'" in quotes, "them, I am as happy as a treecat with celery," which Honor Harrington readers will know what that means, "but I have to curse you at the end of each book as I have to then wait the rest of the month for my next Audible credits so that I can get the next book. Though I wouldn't want it any other way. I have to say that I think this series is one of the best works that Audible Frontiers has done and would suggest that anyone wanting to read these books think about going the Audible.com way. From this long-time Audible user, these audio books are five stars all the way."

Leo: Great. Great.

Steve: And just on the topic of "reading," I also saw Preston in Silicon Valley. He wrote, subject, "I'm reading, no, enjoying a great book." He said, "Hi, Steve. A super quick note about audio books. When I started 'reading' audio books, I would say to my wife, 'I just started reading (insert book title here),' and she would jokingly complain, 'You're not reading it, you're listening to it.' We debated the topic, and finally I said, 'Fine, I'm enjoying a new book.'"

Leo: Good word. Good word.

Steve: "Ever since, I use the term 'enjoying,' and every time we both laugh a little. Love the show, including the sci-fi, Hush Puppy, and other talk. Preston."

Leo: I like it. "Enjoying."

Steve: And I asked you last week about the iPad Mini. I found myself near an Apple store, so I went in. And I haven't changed my decision, which we sort of - you and I came to, which is they are sure to increase the resolution, so why buy one now? But I just wanted to say that what struck me more than the size was its weight, which is light. It is, I mean, I'm an iPad - I've owned multiples of every version. And they're not light. This is really light. As I was holding it, I was thinking, oh, my god, this is - here's everything that the iPad is, and it doesn't weigh much. So I was very impressed with that. I would love to have it get, boy, if it could get the pixel resolution of the regular-size iPad in that size, so that it was super retina, that would be something.

Leo: Well, I think it will be retina. In fact, now, and this will really peeve people off if this is true, we're starting to hear rumors that Apple may rev the iPad Mini sooner than later, like sooner than September. And if they do put out a retina, like in May or June, there are going to be some angry people. Angry people.

Steve: Not me.

Leo: Angry.

Steve: Now, the note I have...

Leo: Yeah, because you didn't buy one. I mean the ones who did.

Steve: Yeah, so I know what you mean.

Leo: Angry.

Steve: The note that I have that would normally talk about SpinRite is about everybody. And I just liked it. The subject was "Nothing but love." Now, I didn't know what this was about. This was in the mailbag from Jason in Pennsylvania. He says, "Nothing but love." And he said, "Hey, Steve, GRC gang, Leo, Tom, et cetera. I know that this is technically the wrong feedback form for mentioning the podcast. But I'd like to address everyone, and I figured this might be a good way to do it.

"SpinRite has saved my data more times than I kinda care to admit. I do have backups now, but there is simply nothing like the speed of a SpinRite recovery compared to the daunting download task of getting those backups back from my cloud provider. Even a SpinRite run that's extended saves time. Also, the podcast has been AWESOME," he has in all caps. "I'm quite addicted and really look forward to listening on my horrible commute or during my workouts. It is clear to me that Steve, Leo, Tom, and the rest of the gang at GRC and TWiT are making this world a better place to live in. Seriously. I'd rank your efforts high among the great things that make life worth living."

Leo: Oh, wow.

Steve: "And before you write me off as nuts, stop and think about that. Isn't it always the small things that matter the most?"

Leo: True.

Steve: "When we recognize these kinds of things. If I wasn't fed, sheltered, and clothed, my opinion might change. But that would be because of my perspective. From where I sit now, joy comes from different places. Anyway, I felt the need to express thanks to everyone listed above. You have all made a big difference, and it is much appreciated. Please keep up the good work, never stop, et cetera, et cetera. Also I'm a proud SpinRite owner, ready to cram money in your pocket for any upgrades or new products you create. I'm also a slave to buying everything advertised on TWiT, so please tell Leo to take it easy. I do have my limits. If you read this on-air or post this someplace, please don't reveal my email." Of course not.

Leo: No, we would never do that.

Steve: So thank you, Jason. That was a very nice, neat, holiday-spirited note that I know we all appreciate.

Leo: You know your blinking lights have stopped.

Steve: Oh, you're right. We had...

Leo: You have a PDP crash?

Steve: No, no, we had another little brief power failure a couple nights ago, and I had to go around and reset all the clocks. And I just forgot my blinking lights. So I'll...

Leo: What is that you've got there? Is that a tuba?

Steve: This just came in the mail. The doorbell rang as you were starting your Ford commercial. This is the neatest company. I don't know if people know about it. The company, I think they're in Minneapolis, is Digi-Key. They are a fabulous online electronics parts supplier that can ship overnight, or I finally got myself under control because I was spending way too much money on overnight shipping because I was wanting the stuff immediately. But all of the parts for the Quiet Canine Dog Whistle project will be sourced from this one company.

Leo: Oh. This is just like a toy store.

Steve: Oh, my god, Leo. Everything you can imagine, massive inventory, quantity discounts, I mean, I would imagine major companies might be sourcing stuff from them. But so you're able just to go through, use an online ordering process, tell them how much you want, they put it all together, you tell them how you want it shipped, and they're just fabulous. In fact, something I asked for it turned out they didn't have by the time they were trying to pick it. They phoned me and said, "Steve, this is Digi-Key. We just wanted to let you know that or hope that this wasn't a critical component that you needed because we don't have it. But we'll ship everything else. And if there's a replacement that we can use, give us a call, and we'll get it to you immediately." So they're just - they're an amazing company, DigiKey.com. And so when I finally put together the whole bill of materials for people who want to build these themselves, it'll just be a parts list from Digi-Key. You go there, put it in, and you'll end up essentially with a kit just arriving at your doorstep.

Leo: This is awesome. Look at this.

Steve: Yeah, I mean, anything you can imagine. I put in "n-channel enhancement mode MOSFET," and bang, there's, like, all the ones they have. You're able to, like, then, winnow down a huge array based on characteristics. You can sort the columns. It's just - there's also Mouser.com. They're sort of the - Digi-Key and Mouser are the two distributors that have really built themselves a beautiful online presence for doing this kind of thing.

Leo: You did not just learn about this company, somebody in the chat says, obviously. I think...

Steve: Oh, no.

Leo: I think you've known about them for a while.

Steve: No, it's why I can talk about - I can state their reliability and reputation is that, I mean, they're my go-to place when I need a particular widget. Well, and we no longer really have electronics stores around. Radio Shacks are kind of cheesy, and they've pretty much always been a little too consumer-ish. We happen, because we're in a particular location in Southern California, there's one store called MarVac in Costa Mesa that I do drive to when I want something, and I'm willing to go half an hour both ways to get it. But again, they've got limited inventory, nothing like Digi-Key.

So what I ended up doing is, if I order by - they're so good that they will accept orders up to, I think it's 8:00 p.m. central time. So even late in the day. But I know that if I order, for example, the stuff that just came now, I ordered Monday morning. So they got it in - and this was by mail. So this is Priority Mail, which is the least expensive way to ship it, it's like $5.00. And they ship it Monday, I get it in California on Wednesday at noon. So, anyway, love them.

Leo: That's cool. You're such a geek. Shall we get - you're such a geek. Shall we get to the questions?

Steve: Yeah, we'll do as many as we can. We've had a lot of fun up to now on the podcast, so...

Leo: We've got 20 minutes left. That'll be enough time.

Steve: We'll do what we can.

Leo: Yeah. All right. Let me see here. This is...

Steve: Oh, actually, No. 1 is just so funny. Oh, Leo.

Leo: All right. Scrolling down. Where are the questions?

Steve: They're on a different PDF.

Leo: Ah, there you go.

Steve: That would explain it.

Leo: That would explain it because I have the long Oracle Java notes that you sent.

Steve: Oh, I decided not to drag everybody through that.

Leo: Thank you. Thank you. They can read those on their own. We don't need to read those to them. Let's see. Q&A show notes, questions. There it is. Let's open that sucker up.

Steve: Oh, goodness.

Leo: Oh, I did open it. I already had it. Why don't I see it?

Steve: These computers are so confusing.

Leo: Question 1. Yes, it is. I can't figure out how to use a computer. This is a "Listener-Driven Potpourri," according to Steve. Wes in Indianapolis inadvertently interfered in his family dog's "business." Hmm. Hi, Steve. I'm a big fan and was just listening to the Security Now! episode on DTLS when I heard you mention how old CRT TVs produced a certain very high-pitched whine while they were operating. It reminded me of when I was younger, and we had an ancient-looking CRT television in the living room. It was the kind with customizable buttons that you had to dial in to the station you wanted to watch - or the cell phone conversation you wanted to hear, but that's another matter - although thankfully it came with a handy three-button, count 'em, remote.

One Sunday morning I was playing Super Mario World. My dog came into the room to perform some lewd acts with the furniture. I told him to stop, but he wouldn't do it. I even threw a toy to him to try to distract him, but he was rather focused and engaged, I wonder why, in a lovely piece of couch. In a fit of exasperated acceptance, I pointed the remote at him and pressed the power button, prepared to dryly complain to no one in particular about how the remote was broken, and at the very least entertain myself.

However, oddly enough, the remote wasn't broken at all. After I pressed the button he jumped backwards and looked around as if he were stung by something. I tried it again with the same result. Then, to my dog's chagrin, I did some further youthful experiments. In short, the effect was reliable up to 10 feet while the remote was pointed at him and, to a lesser extent, when pointed at him through a wall. I decided not to do it again because it obviously upset him.

But maybe you could find use for this in building a more compact version of your PDK. I figure with a bit of amplification you could rig up a pocketable device with a decent range for dealing with aggressive dogs out on the streets. You could sell it to mailmen all over the country. Unfortunately, I don't recall the brand of the TV, and I don't know how standardized remote control technology was in the '90s. But maybe there's something here. Thanks for the great podcast. Wes. That is bizarre. It must have been an audio remote.

Steve: Well, do you remember - yes. First of all, I thought maybe we need to rename this the Canine Coitus Interruptus box. So the original remote controls had three or four big stiff buttons. And when you pushed it, a striker hit a steel bar that emitted an ultrasonic tone.

Leo: Oh, my goodness.

Steve: And so there was a receiver in the TVs with four tuned circuits, each one that would respond to a different tone. So one was like alternate action on/off. Or maybe it was like channel up, channel down. I mean, one was channel up; one was channel down; one was volume up; one was volume down. But you would kind of go clunk, clunk, clunk,

clunk, and the TV would respond each time because you were banging this bar, and it would send out a very high-pitched tone. And clearly what we had was a very, very - he arguably was the originator of the Quiet Canine Dog Whistle. It was exactly that effect, which I just got a kick out of.

Leo: I hope this won't throw you. But Zinga tells me that there is on Amazon something called the Pet-Agree Dog Training Ultrasonic Aid. Also use in training cats, it says.

Steve: It doesn't upset me at all. And in fact it's one of the reasons I want to thoroughly beta test this because many of our listeners, being techie people by nature, have already bought every one of these things. They sent me links to things that I've seen. And remember that I mentioned I had bought a whole bunch of these things for Mark because I'd just rather buy something for him than have to go through inventing and building one.

Leo: Right.

Steve: But none of them work. And all of our listeners report nothing, nothing has ever worked for them.

Leo: They just aren't willing to put enough power behind it.

Steve: I really think that's the case. The other thing they do is they pitch them much too high. There was something Mark had called a "Dazer" that actually I got for him.

Leo: Yeah, that's this. The Dog Dazer II Ultrasonic Dog Deterrent.

Steve: Yes. Now, the problem is that's at 25KHz. I've measured it. And that is way too high. Dog hearing actually peaks down around 5 to 10KHz, and then it does extend to, like, 15 and 20. But it then begins to drop off very quickly. Many of these companies pitched theirs much too high. Just, I don't know if they didn't do their research or what. But so that's why I'm deliberately at about 15KHz is to definitely stay down where I'm sure we have a sensitive receptor.

Leo: There's a review by a postal carrier of the Dog Dazer II. It says it works only on four out of the thousand dogs he's tested it on. It stops about half of all dogs from barking for a few seconds, about 30 percent of dogs from barking as long as I hold the button. It quiets my day, but I'd only use it as a primary defense if I have a can of mace as backup.

Steve: And we do have a few postal carrier listeners who have asked for and will receive a beta device.

Leo: Postal carriers, we should point out, do carry mace for this.

Steve: No kidding.

Leo: Yeah. So if they're attacked by dogs they have something to spray them with. This would be more humane than macing a dog.

Steve: Oh, my goodness, yes. I mean, if it's effective. And the other thing, too, is that I've been considering using a microcontroller so that it only generates a short burst. There is no need to, like, spray anything with this. I mean, my intention is to have it be so loud that you want a shock value, a startle value, not to hurt anything. You just want to say, okay, knock it off.

Leo: Right. And here...

Steve: And something brief is better than that.

Leo: ...thanks to Eric Duckman and Wikipedia, is the Zenith Space Command Remote Control, with four buttons.

Steve: Oh, there it is, yes.

Leo: Each of which strike a bar, make a tone that you can't hear.

Steve: And you know that I took mine apart, and my family was not happy.

Leo: Of course you did. Moving along to Question 2, John Hughan in Austin, Texas: Why not start with TCP and just switch to UDP when you're using DTLS? Given that one of the design goals of DTLS was to reinvent as little as possible, why couldn't the design have been to perform the standard SSL/TLS handshake - I'm getting the acronym hiccups - over TCP the way we always have, and then use the symmetric key negotiated in that session for the UDP session? To me that would seem to require the least change of all since there'd be no need for the mini-TCP tweaks to UDP. And for applications like VoIP, I can't imagine that the extra time required to complete a TCP handshake upfront to negotiate a key rather than doing everything over UDP would be significant.

Is there some issue with the way connections are handled by operating systems and/or firewalls that would prevent switching over from TCP to a UDP session while retaining the symmetric key negotiated over TCP that way? And, for that matter, if UDP is only now gaining the benefits of SSL/TLS, how has Skype been providing encrypted conversations for so long? Are they running a proprietary encryption scheme? Thanks for providing such a consistently fantastic show. This email from the one listener who understands this show. Because I don't understand the email.

Steve: I was very impressed with John's question.

Leo: Interesting question. But can I boil it down to, basically, we don't negotiate a new key, we use the key we've already negotiated, the symmetric key? Is that right?

Steve: Well, he was exactly right that the guys that were trying to do essentially SSL over UDP, they ended up trying to reuse all of the existing good technology and proven that was designed, that was developed for SSL over TCP. But doing that does, because TCP offers a reliable transport, they had to add things to UDP, specially during the setup handshake, to sort of simulate the reliability of TCP in the ways that I described in that podcast [SN-380]. And so John is - it's a very interesting proposition. That is, if their goal was to not reinvent the wheel, why not just negotiate a TCP connection, then take the context, the SSL context which you negotiate from that and move it over to a UDP session? So you let TCP do what it's best at, which is the reliability that you need during the SSL negotiation, then take the information both endpoints obtain, which is used for the subsequent crypto, and move that over to UDP.

I actually had a different solution that I would probably argue was better than any of those, I mean, even better than DTLS, that I'll talk about in a second. But John is right when he suggests that maybe is it something about operating systems or firewalls or something. And the reason that you can't move context between flows, between endpoints, is that many systems are behind load balancers. There'll be like a firewall load balancer which receives the incoming traffic and then redirects it to a given server behind. Sometimes those are based on the instantaneous load that all of the servers behind them have, or the load that they're under, so that this switch will, in like a Google or an Amazon or any big datacenter, there's normally a load balancer. So it will choose which server is going to get this, is going to handle this connection, and then remember that statefully. So it's very possible that one server might get the TCP negotiation, and then when you establish another connection, that ends up going to a different server. There's normally no reason why that wouldn't be okay. So that's one of the problems.

The other way these things work is sometimes that they will, rather than using dynamic load balancing, they're just trying to evenly spread the traffic across a set of servers that are behind sort of this deconcentrating switch. What they do is they'll take the source IP and source port and often the protocol, and they will mix them together and essentially hash them and end up with, like, a one of 10 or one of eight, and then that determines which one of the eight ports the traffic is emitted from going to one of eight servers that are behind there. That way sort of statistically all the users on all the different ports all over the Internet end up randomly spreading themselves between servers. And the beauty is any one user always gets assigned to the same server, that is, for a connection.

But when we allocate TCP and UDP connections from our operating system - we talked about this years ago - we sort of march up through the available ports. So port 2468 will be used, then 2469, then 2470 and 2471. So the point is that there isn't a way for the application to say I really need to be on the same port that I was on TCP under UDP. That's done by the TCP/IP stack in the kernel, and the application layer doesn't have any control over it. So, yes, that's why they didn't make that change.

The thought that I had was that an interesting modification to TCP could easily be made, which is to tell TCP to shut down all of its reliability nonsense. That is, you establish a TCP connection, and then you say, I want to go asynchronous. And essentially you turn the existing TCP connection into a UDP connection by telling both ends, okay, don't care about buffering packets, don't care about lost packets, don't care about out of order arrival. We just want a clean, unencumbered, unbuffered, unpatched-up pipe between endpoints. And that would actually be something pretty simple to do. So maybe someone will do that, which would be cool.

Leo: Bruce Barnett, Albany, New York writes: Here's two great low-cost items for the home user who wants a "data diode" from GreatScottGadgets.com, the "Ethernet Throwing Star." And you can Google "Ethernet throwing star" if you want. It's a LAN Tap that looks kind of like a ninja throwing star, actually. He says there's a kit for $15 and a fully assembled version for $40. It's great for network sniffers, intrusion detection systems, et cetera. It splits two-way traffic into the original two-way and two additional one-way connections that have to be merged to fully decode protocols. This is a preferred solution because programs like Wireshark can have buffer overflows, and they run as a privileged process. A malformed packet can compromise a sniffer, but the diode prevents that machine from interfering with the monitored network. Keep up the good work, Steve. We enjoy the show. There it is, the Throwing Star LAN Tap.

Steve: Yeah, I liked this because essentially I've been very impressed with the technical level of our listeners. I mean, they've jumped on, for example, the Quiet Canine project, and a bunch of them are building these things, even though the design isn't finished. They don't mind being on the bleeding edge. I remember when I talked about this a year ago and found that cool little Xpresso LX board, our listeners kept buying out the supplier. And I thought, wow, we've got a lot of techie, hardware-capable, interesting, experimenting oriented people.

We talked about the idea of modifying Ethernet cables, but this has done it in a very simple way. You may be wondering why they used the term "throwing star" until you see this thing because the PC board is in a wacky sort of four-pointed star shape. And then with the little kit you just get the Ethernet connectors which you mount on the four points of the star. And two of them are a passthrough, and the other two monitor the traffic in each of those two directions.

So anyway, the point was that, if anyone was interested in the notion of sniffing Ethernet in a one-way direction - the so-called "data diode," as the term was used by that company we talked about a couple weeks ago who'd done that at the protocol level - if you're interested in doing it at the hardware level, this does it for you for 15 bucks if you have a soldering iron, or 40 if you don't.

Leo: They sell it at the Hak5 store. Darren Kitchen and Shannon Morse have a video on it and everything. And they sell the kit for 15 bucks, not very expensive, and the assembled version is $40 if you don't want to take soldering iron in hand. That's neat. Kinda cool.

Jim Sauber, Minneapolis, Minnesota has a suggestion about show links: Steve and Leo, listener for several years, insert usual stuff here. Steve brings up many interesting websites during the show and refers listeners to his Twitter feeds for the links. Since often people listen to the show or read the notes weeks or years later, relying on Twitter for the many links seems to leave us with the task of searching through your Twitter feed for the right dates. Also, if Twitter someday disappears or decides to truncate your old tweets, these will be lost forever. For the sake of at least posterity, I request that you include the links in your show notes or copy and post your relevant tweets on your site so they will live forever as we know your notes will. Looking forward to many more years of Security Now! and other great TWiT shows. Thanks for everything.

Steve: And you know, I had not thought about that, but he's completely right. Twitter is inherently recency based. And I'm always saying, and I'm thinking, to people who listen to the podcast in the next few days, since I'm not typically frantically tweeting, the things that I post for the show won't have been pushed far back into my Twitter history. But on the other hand, we're also encouraging people constantly who just joined the podcast and find out about it, we're saying, hey, and by the way, all 380 prior episodes are over here. But it's certainly the case that on all those times a year later that I refer to things, there's just no way to find that on Twitter.

So I'm going to ask Elaine if she would grab the links at the time that she's doing the transcription of the podcast and just embed them in the podcast. I don't think that would be a problem for her, I'm paying her by the hour, and it shouldn't delay her very much. That would capture them at the time. Now, we still have the problem of the links themselves becoming stale over time, but that's - at least we've done everything we can. So I'm going to, when I send this off to her, I mean, she's hearing this right now...

Leo: Oh, you want me to do that, Steve? Okay.

Steve: ...because she's transcribing this. So I would like her to do that. I don't have any this week, but in the future - I know that she's a little bandwidth constrained, but pulling up my Twitter feed takes no bandwidth. And that would be great. So thank you, Jim, for the suggestion. That's an improvement we will incorporate. And thank you, Elaine, for doing that.

Leo: Do you send Elaine what you send me, the show notes before each show?

Steve: Yes. She gets that all, too.

Leo: Because the links are in there, too.

Steve: Oh, good point, yes.

Leo: She doesn't have to go anywhere. She's already got them. Question 5, R. Morton in Round Rock, Texas - home of Dell Microcomputers, I think that's about all that's there - wonders about Google and SSL certificates up the wazoo. Steve, as you suggested, I have Certificate Patrol installed in Firefox, and I have a Gmail account. Lately I've been spending an enormous amount of time in China - he does work for Dell - and as such I keep a very tight rein on Internet usage. Within the last six to nine months, it seems every time I visit Gmail, Certificate Patrol warns me of a slew of changed certificates which I ignore while in China.

But then today, after checking Gmail at home in the U.S., I receive an alert that Google is now a Certificate Authority, having replaced Thawte and issuing their own certificate that expires three months sooner than the Thawte certificate. What am I to believe? Is Google going rogue, or is someone trying to spoof them? Please, what's going on?

Steve: So that certainly was news to me, so I established an SSL connection to Google. And what I saw was a little different than what our listener was seeing. However, I should mention I was a fan of Certificate Patrol. I loved it. And in fact it's through Certificate Patrol that I found DigiCert, that is now my certificate provider. I really love them. And it was by seeing all of, like, Facebook uses DigiCert, so I can, too. And I'm so happy that I left VeriSign for this because it just - VeriSign was becoming increasingly difficult to deal with.

However, I was forced to stop using Certificate Patrol because of Google. Google is synthesizing certificates at an insane rate. So much so that, exactly as our listener reports, Certificate Patrol was popping up all the time. And there is an ability or a checkbox to say "Ignore further notices from this provider." But whatever Google was doing was still upsetting Certificate Patrol. So I just said, I mean, I put up with it for quite a while, and finally I just said, okay, I've got all the information I'm going to.

What Google is, is an intermediate authority. Equifax is the root. And so what R. Morton said made me curious to see whether Google had in fact quietly become a root authority in our browsers, but that's not the case. And I'm kind of glad because that's a little heavy-handed, and a lot of responsibility, too. Instead, they are an intermediate authority. Their certificate, the Google Certificate Authority, yeah, I think it's called Google Internet Authority, is signed by Equifax, that is a longtime, old-school certificate authority, a root CA. And then this Google Internet Authority is just - they must have an electronic certificate generator, I mean, it spews things out. So it's constantly changing, different servers, different IPs, I mean, just basically these are - it's very much dynamic.

So I don't think it means anything bad that Certificate Patrol is being driven crazy by Google. It's just the security model Google has, for whatever reason, is they do not have static certs. They're being dynamically generated and signed by their own intermediate authority that is in turn signed by Equifax. And he mentioned Thawte being replaced or reissued or I don't know. So maybe the chain, certificate authority chain, changed recently. But at this point - because I do remember Thawte being around there. But at this point it's just certificate to Google Internet Authority to the Equifax root, is what I saw yesterday.

Leo: All right. Chris Lewis, Jonesboro, Arkansas, found a really nice Chrome tree-style tabs. We know Steve loves tree-style tabs. A new Chrome extension just came through my G+ stream, says Chris, that provides the tree-style tabs you say you love. It's a long URL, so just search for "sidewise tree style tabs," I guess, in the Google Chrome store.

Steve: Yes, I meant to mention that, and I forgot to. It looks very nice. It's sort of like a sidecar that you dock along the side of the browser. And from looking at the page, I have not installed it or tried it yet, it looks yummy. So if there's anybody who, like I am a side tab addict over on Firefox, this is beginning to get there. And I noticed there were some other utilities that were doing the same sort of thing. So we're beginning to see - we're waiting for Google to come up with their official solution because they recognize there are tabaholics who organize themselves with their browser this way, and that tabs across the top just don't do it. So I just wanted to point this out for other people who feel as I do.

Leo: Tabaholics. I like it. Greg in Washington, D.C. wonders about a company impersonating commercial root CAs: On show 381 you discussed how a person can tell if a company is snooping on their SSL traffic by examining the certificate's chain of trust. Most companies issue their employees the hardware. So what's stopping them from installing their own root certificates and naming them after the commercial providers? A casual inspection of the certificate's chain of trust would show no anomalies. You'd need to check the fingerprints for all the root CAs to uncover this problem. What am I missing? SpinRite owner/operator Greg.

Steve: And Greg is not wrong.

Leo: Really.

Steve: I don't know if the root store in our computers would allow two identically named certificates.

Leo: That's what I think is the problem; right?

Steve: Yeah. There might be a naming collision there. But I'm not even sure that's true because, with certificates, you can definitely have identically named certificates with different expirations because I've had that myself where I'm installing a new one, and the old one is still there. It's about to expire or expired. But I've seen them sitting side by side. So it might be very possible for a company to issue, to themselves create a certificate named Equifax CA and sign it and install it in people's machines right along with the normal Equifax certificate. And that might work. Then, when their browser - let's see. How would this work? When their browser would ask for the cert from a secure site, it would provide the certificate from the fake Equifax. And again, I don't know then how the matching works. Is it serial number matching, or is it name matching? So I don't really have an answer. But it's a great question, and I'll bet you that we've got some listeners who have drilled down in this area where I haven't yet and will probably provide me with some answer in our feedback. So I'll look for it and hopefully have an answer next time.

Leo: Cool. Here comes Question 8 from Matt. He's commuting somewhere near Chicago. He was listening to 381, as well: During episode 381, a listener expressed some concern about their company monitoring their SSL traffic; and, if it's actually monitored, are his LastPass passwords still secure? You are correct in that the blob of data LastPass uses is secure, even without any transport encryption. However, what you missed is when the password is decrypted and sent back to another server as part of the login process. If the listener's company is monitoring SSL traffic, then this password would be visible to corporate security software. In other words, you couldn't read all the person's passwords, but any of the passwords he uses you could. I always look forward to the drive home on Wednesday so I can listen to a new podcast. Please keep them coming.

Steve: So Matt and a number of our listeners caught me on this. I answered the question correctly. I assumed everyone understood Part 2.

Leo: All bets are off when you use the passwords.

Steve: I should have made it more explicit. So, yes, the question was, is my LastPass blob secure? My answer was yes, it is. And it is. But the person who asked the question certainly deserved me saying what our listeners have added, which is, but, when you use the individual passwords, they're not secure if your company is filtering your SSL and spoofing the provider.

Leo: Andrew Cooper's in my new favorite city, Sydney, Australia. He got a rude surprise: First, Steve, I want to say "blah, blah, blah." I was recently at a conference at a well-known museum here in Sydney. While there, I connected to their public WiFi in order to check my email, among other things. But when I connected to Gmail, Chrome gave me an alert about the SSL certificate being used. I checked, and sure enough, the museum was trying to intercept the SSL session. Needless to say, I immediately turned off my LAN WiFi radio and went without a connection for the day. Without the podcast this would have been much more confusing, and I would have been less sure exactly what it meant. As always, thanks for the great podcast. I never miss an episode. Andrew. Wow.

Steve: So I'm impressed. First of all, I thought, why would a museum do this? And then I thought, oh, yeah, of course.

Leo: Why?

Steve: They're wanting to filter. They're wanting to do...

Leo: Ah, no porn.

Steve: ...porn and bad content filtering. And so they bought some edgeBOX that's sitting on the edge of their network, and it just does this. It's like, that's what it's going to do. So, and I'm sure, a museum being sort of a little bit like a school, in the same way they're just wanting to do content filtering for their LAN. But I was impressed by Chrome. So tip of the hat to Chrome for noting that something is fishy here. You're trying to connect to Google, but you're not getting one of our certificates, so something's in the way. Very nice.

Leo: Wow. Wow Something to pay attention to.

Steve: And many people, by the way, I mean, this is - we're getting so many questions about this idea of am I really secure? Am I being spied on? Is my company filtering stuff? So that's why we just went through a bunch of these. It's representative of a cross-section of our listeners.

Leo: Yup. And Tyler Larson in Scottsdale, AZ suggests: Make key-stretching hardware-proof by burning memory. Okay. You're going to have to explain this one to me. You've already mentioned key-hardening algorithms such as PBKDF2 and bcrypt, which hash and rehash passwords thousands of times to slow down cracking attempts. But these approaches all have an inherent flaw: You can still build a cheap hardware device, or program an FPGA to dramatically speed up cracking. But someone solved this problem. By making your algorithm require huge amounts of RAM, you can massively increase the hardware cost of building a dedicated password-cracking device. CPU-speed memory is extremely expensive, which means that building an ASIC for password cracking would be too costly to warrant the effort. That's the idea behind scrypt, used by Tarsnap. Reportedly, a hardware device implementing scrypt would be 20,000 times more expensive than an equivalent one implementing PBKDF2. Your thoughts?

Steve: So this is our lead-in question for our next podcast after the Christmas Special.

Leo: Oh, joy.

Steve: We have talked - I've touched briefly on this. Attentive listeners with eidetic memories will remember the phrase "memory hard problems." That's the cryptographic jargon for this kind of deal. They're called "memory hard problems." They are problems which are deliberately memory hard, that is, not algorithm hard, but memory hard. Because Tyler and the author of Tarsnap, who designed scrypt - and, by the way, I'm very impressed. Scrypt, which just some random guy did, has now been adopted by the IETF and is heading towards RFC. So he did it right. And in fact there's even - I ran across - there's even a non-bitcoin currency, another currency, that is using this scrypt algorithm, this memory-hard algorithm, as proof of work. And remember, the proof of work is the whole concept behind bitcoin, which is doing something that is really hard, and you want hardness to be scalable and not something that you can easily get around by doing hashing fast.

And so everybody is correct. Hashes are designed for speed so that they're not burdensome for normal applications. We've sort of repurposed them for scrambling passwords. But they're really not appropriate because look at what we're seeing with [indiscernible] breaking records all the time in the speed at which they've been hacked. So the solution is somehow do something that is much harder, that is not just algorithmic, that takes it in a different dimension. And that dimension is memory, and that's our topic in two weeks: Memory Hard Problems.

Leo: Awesome. Wow. That is going to be a hard problem. We'll be back January 3rd, I think. No, the 2nd. January 2nd, the day after New Year's Day. And that will be a special return to the regular Security Now!. Next week, of course, we go back in time to 1990. And that'll be a lot of fun. Steve Gibson's at GRC.com. That's where you'll find 16Kb versions of the show and transcripts, as well, thanks to Elaine. GRC.com. You'll also find SpinRite there, the world's finest hard drive maintenance and recovery utility, and lots of freebies, as well. He's @SGgrc on Twitter, SGgrc on Twitter.

And of course you can get the show live here every Wednesday, 11:00 a.m. Pacific - not next week, but the week after - 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1900 UTC on TWiT.tv, or download audio and video after the fact at the same spot and wherever finer podcasts are stored. Thank you, Steverino. Have a great holiday.

Steve: Will do. Thank you. Great to be with you as always, Leo. And we've got years and years more of this.

Leo: See you next year, Steve.

Steve: Bye bye.