SECURITY NOW!

Transcript of Episode #144

Listener Feedback Q&A #41

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-144.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-144-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 144 for May 15, 2008: Question & Answer 41. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now! with Steve Gibson, everybody's favorite kind of fatherly uncle-y security guru.

Steve Gibson: I'm not sure what that means.

Leo: Uncle-y.

Steve: Uncle Steve.

Leo: I think the word is "avuncular" that I was looking for.

Steve: Avuncular, that's good.

Leo: Yeah, you're the avuncular security guy. And every week we talk about the latest in security on the web, on your networks, on WiFi, all that stuff. Good to talk to you again, Steve. I hear you have your triple venti latte?

Steve: It's a quad, and it's my third quad. So...

Leo: Whoa, wait a minute. You're running on 12 shots of espresso right now?

Steve: Well, it's at the beginning of the third Americana. So that would be shots, what, 9, 10, 11, and 12.

Leo: I need one. I need one badly.

Steve: And actually Starbucks has, like, been - they're trying to reinvent themselves with the return of Howard Schultz, who is back and sort of trying to pull them back into more high-end espresso coffee mode. One of the things they did was they lengthened the length of the shots, meaning that the machines pull longer shots now.

Leo: Well, that's not good, is it?

Steve: And it really made it bad. I mean, I had, like, a week of hell before I...

Leo: You want short pull. So you ask for short pull now?

Steve: That's exactly what I do. I have them do - I do quad, half shots. And so I get the first, like the good half of the espresso. And it's funny, too, 'cause they're not used to that. So it's like, pull down, pull it down, get it out of the machine, let's go [indiscernible].

Leo: I don't want the rest.

Steve: Are you sure you need more caffeine, Gibson.

Leo: You crack me up. The good news is, for people who are thinking he's had, like, the equivalent of 12 cups of coffee, I'm told espresso shots are not as caffeinated as drip coffee.

Steve: Absolutely true. The roasting process, which is longer for espresso than it is for regular coffee, it burns off caffeine. So it's a stronger taste, but it's actually less caffeinated. I mean, and the commercial coffees, like Yuban and Maxwell House, they amp up the caffeine in order to increase the addiction factor.

Leo: Oh, that's interesting. I didn't know that.

Steve: That office coffee is like, oh, that'll give you the jitters.

Leo: It does. It does. Well, that's good to know. So we have a lot to talk about. I think we should really launch right in. This is our...

Steve: One of these days, yes.

Leo: Yeah, one of these days. This is our even week, even show, question-and-answer session. So we're going to get to your questions. Got some really good ones, I see them here. But you have some news?

Steve: A bunch of news. A lot of stuff happened in this last week. One of the things that happened is I sort of wrapped up my YubiKey/Yubico coverage, as you know, with last week's episode. And I thought, okay, I'm going to take all this correspondence - because I had a whole bunch of correspondence with the Yubico folks, Stina and Simon and Paul and those guys. And I thought, I'm just going to stick them all in a folder. So I did a email-wide search on the term "YubiKey," I think, or maybe it was "Yubico." And it uncovered - so I just had to give a heads-up. It uncovered two early mentions of this from our listeners. And Eric Roller wrote to me back in October of '07, early October, on the 6th. And the subject was "Security token with a key that is valid for one second." And he said, "Hi, Steve. In case you haven't heard about this new idea from a company spun out of Cypak, http://www.Yubico.com. The idea is that their token, a thin USB stick with one button, acts like a USB keyboard and sends a 128-bit authorization key which is only valid for one second. There's no battery, and hence no clock on the token."

Well, this was October of '07, and our listeners already knew about it. And unfortunately I get so many submissions at the GRC.com/feedback page, I never saw this, obviously. And then this year, in February, Torkel Hasle looks like is the way I pronounce his name, it says "Smart security dongle" with a similar note. So I just wanted to give a heads-up and shout-out to those guys and say - I mean, and imagine, they must have been, here I am all coming back from RSA, jumping up and down about the YubiKey. And these guys must have been thinking, hey, we told you about that months ago.

Leo: Yeah, yeah.

Steve: So thank you, guys, and I'm sorry that I didn't get your message. I just wanted to acknowledge that you were certainly ahead of the game.

Leo: We get a lot of mail. You can't see it all. Sometimes stuff slips through the cracks.

Steve: Also, since - actually I think it was the day that our podcast went public last week, that is to say, last Thursday, Service Pack 3 was finally released for Windows XP.

So I just wanted to mention that to our listeners. As it happens, I did a setup of a brand new XP. It was a reinstall, actually, for the manager of my local California Pizza Kitchen. He's a good guy. He's been bugging me for about a year. And it's good for me every so often to see how the rest of the world uses...

Leo: The other half.

Steve: Oh, not half, the other 99.9. His system had 85 processes running. It never really did finish booting because it ran out of memory before it got booted. He was using 574MB just because I don't think there's ever been a software offer to which he has said no. When IE no longer worked because it had so many toolbars installed that there was about a one-inch space at the bottom where you could scroll the web page. Oh. Anyway, I had fun with him, saying...

Leo: That's pretty funny. But you're right, I think this is normal.

Steve: Yeah, and he didn't understand that, I mean, he didn't understand that everything you install, especially nowadays because everything wants to be running, they want to have some little thing in the tray, they want to be checking for updates, they want to - he had something called Ding. I said, what's Ding? He says, oh, that's Southwest Airlines' flight notifier. I said, do you need that? He says, well, no, but I didn't - oh, and get this, Leo. He did not know how to remove software.

Leo: Well, clearly not.

Steve: I mean, he says, I don't know how to get rid of anything. So it all just kind of piled up. And I said, oh, baby, did it. So anyway, now his machine is beautiful. But I had an opportunity to reinstall XP from scratch. And you need either Service Pack 1 or Service Pack 2 in order to install Service Pack 3. So of course I've got from Microsoft, the most recent XP incorporates Service Pack 2 because it's been so long since Service Pack 2. So I put Service Pack 3 on top of Service Pack 2. It worked great with no updates. I did want to caution people if they haven't heard, though, that there's problems, I'm sure you know this, Leo, with AMD chips. There are some people who then get into a Blue Screen of Death reboot loop if they install Service Pack 3 - which is, by the way, an upgrade that Microsoft will be offering. So you'll want to say no to Service Pack 3 unless you're sure that it's going to work for you and you've got AMD chips. If you do get into this trouble, you can boot into Safe mode. And Safe mode will not give you the Blue Screen of Death. Then go to Add/Remove Programs and back out of and remove Service Pack 3 from your system.

Leo: Oh, so there is an uninstall for it. That's good news.

Steve: Yes. Yes. Also many, many, many listeners, as I was going through my mailbag for pulling the questions for today, everyone's worried about this news that just recently came out, although Microsoft's been doing it for some time, this COFEE, COFEE with one "F," stands for Computer Online Forensic Evidence Extractor. Unfortunately, the online reports exaggerate what this is. And, I mean, literally, I think it was even Ars Technica, that I normally have a high opinion of, said that it bypasses PC security. What this is, this is a USB thumb drive Microsoft has prepared, one of Microsoft's security guys who's been with company for four years, prepared this thumb drive that they've been giving out to law enforcement. And it's like a forensic, well, obviously a forensic evidence extractor for Windows. And so the concern is that this is, like, some secret backdoor. I've seen the words "backdoor," "bypasses PC security," you know, "decrypts BitLocker drives." Okay, none of that is the case. So I wanted to, for everyone who wrote in wanting to get some feedback about this, all it is is a command-packed set of tools that are otherwise freely available. It's got about 150 different commands to make it, you know, basically Microsoft's pulled all this together to help law enforcement. But it doesn't do anything that you wouldn't be able to do otherwise. So there's no secret backdoor it's accessing or anything. It's just a really neat toolkit. And of course the bad news is that, when you give it to the good guys, the bad guys'll get it, too, ultimately.

Leo: So that's Microsoft COFEE.

Steve: With one "F," COFEE. And it's just a USB thumb drive loaded with Windows evidence extraction tools that are freely available. You may remember we talked last February about the sort of mysterious Adobe patch where they released a bunch of fixes but didn't tell anyone even afterwards what it was they were fixing. They've since made that public. And they now acknowledge that it fixed eight flaws, six of which were allowing remote code execution, and most of which were flaws in their JavaScript interpreter in the Adobe products. And some are being actively exploited. So I did want to mention - probably by now, you know, they've mentioned this, by now everyone who is using older versions of Acrobat, for example, hopefully will have upgraded. I think it's 8.1.something is the current one. So if you're back on 6 and 7, it is the case that there are malicious PDFs that can literally take over your computer when you view them. So you want to make sure you're using the latest Adobe. And...

Leo: That's the free reader you're talking about.

Steve: Yes, Acrobat Reader. And it is the case that today is, well, actually while we're recording this, we're recording on Tuesday the 13th, which is Microsoft's second Tuesday of the week [sic], Patch Tuesday.

Leo: Patch Tuesday. I should run my Windows Update.

Steve: Well, yes, exactly. There are some important things. So by the time our listeners are hearing this on Thursday, they will probably have already received that. I did want to encourage people, as always, to keep themselves patched. There are three critical remote code execution vulnerabilities, two in Office and one in Windows, and then one moderate vulnerability that actually occurs in Microsoft's antimalware products. So...

Leo: I love it. And there's a special irony when security software has malware in it, or exploits.

Steve: And actually, yes, we're seeing that more and more. It's a problem because they're complex software. And any antimalware, any contemporary antimalware is in the loop. It's a filter that's putting itself between your machine and the Internet, which means anything coming in hits it first. Well, if there are any buffer overruns there, it's ripe for exploitation. So those being vulnerable are a problem. One of the SANS editors, of SANS Security, Dr. Eric Cole, had a little editorial note that I thought was really interesting. He said he was encouraging people to apply patches in general as quickly as possible, and Microsoft's specifically. And he said, "We're now seeing 'Patch Tuesday' followed by 'Exploit Thursday'."

Leo: Oh, great.

Steve: So, I mean, the point being that this window of opportunity, I mean, exploits are being developed from the patches, as we talked about last week. And people may have only a couple days before they start getting - before exploits for what's been patched go live on the 'Net. So it is increasingly important to move that up.

Leo: I like that you call it - in your notes you call this, today, "Exploit Thursday."

Steve: Exactly.

Leo: You've got Patch Tuesday, two days later Exploit Thursday. So patch fast as you can.

Steve: Yeah. And I just wanted...

Leo: To raise this issue, typically corporations do not apply patches right away. They want to test them. What do you do if you feel like you should test these things before you install them? You don't have a chance, I guess.

Steve: Well, that is really a problem because in the past corporations have been hurt by patches which...

Leo: Well, individuals, too. It's not just corporations.

Steve: Yeah, although for example a corporation may need to run this stuff against their own internal proprietary software. So, for example, Microsoft tests it against sort of the native generic Windows OS. But there have been instances where patches disabled critical infrastructure systems inside of corporations. And so now they're much more skeptical about it.

Leo: Yeah. But I can remember a number of times where patches have caused big slowdowns or had an incompatibility with one drive or another. And this has been end-users, as well. So I talk to end-users all the time, especially after Service Pack 2 and that fiasco, who are very loathe to - you know, most of them say, oh, I wait a week to see if there's any big problem with that patch. You can't do that anymore.

Steve: Right, it's becoming, yeah, that window of opportunity has really closed. Over on the sci-fi side - as we know, that's a passion of mine. I wanted to remind our listeners that this weekend is the miniseries of "Andromeda Strain" [S/B Monday, May 26, 2008] on the A&E network that Ridley Scott has produced. And the trailers look really good. In fact, I saw an extended trailer for it earlier, I guess it was early last week when I was out in the theaters to see "Iron Man," which I loved, Leo.

Leo: Everybody loved "Iron Man."

Steve: Oh, it is so good. So I just wanted to toss that in, too. I loved the movie "Iron Man." And this weekend is A&E's production of the miniseries "Andromeda Strain."

Leo: So if you get A&E on your cable system you want to check that out.

Steve: Yup. And it will be released on DVD next month, in June of '08.

Leo: Oh, that's unusual they do it so fast. That's good news. That's great.

Steve: Yeah, that'll be coming out shortly thereafter. And I finished the first patent work, the first patent for CryptoLink, my forthcoming VPN-ish product, has been submitted and is now pending. So...

Leo: Let me ask you about that. A lot of software authors do not use patents because one of the parts, one of the things that's part of the patent process is don't you have to expose your source code?

Steve: No, you don't have to expose your source code. You do need to, I mean, the whole idea of a patent is that the, I mean, the concept, the original concept was that the government wants to encourage people not to keep things trade secret, but rather to make them public so that other people can build on those inventions. So the idea is that once the patent is issued, it is a publicly available document. In return for publishing the technology, the inventor of the technology receives a multiyear exclusivity on the use of that. I believe it's 17 years at the moment. So my interest is sort of in claiming the intellectual rights. I mean, I've come up with something that's very cool.

One of the security notes that I saw when I was researching news for the week was that apparently SSH password guessing is dramatically on the rise. SSH we've talked about, it's the secure shell log-in. It's a service that runs on port 22. And so apparently people who run SSH are seeing a distressing amount of activity, meaning that malicious people, even apparently some botnets, are now - they're looking at port 22. If you accept a connection on 22, they will then perform a brute force password guess, trying to get in. And of course, if they do, I mean, that's really bad. They've got access to root, essentially, secure shell.

Well, what this first CryptoLink patent does, since I'll be running a service also, I've come up with a way of doing, essentially, stealthing an open TCP port so that it's not open. That is, nobody except a matching authenticated CryptoLink client is able to see the port to connect to it, even though it's TCP. So it's a way of stealthing open ports that would prevent all of this kind of problem.

Leo: Oh, that's interesting. Very clever idea. So when are we going to see CryptoLink on the market?

Steve: Well, I've got to start working on it first.

Leo: Oh, you've patented it, but you don't have any code written.

Steve: No. I haven't even...

Leo: So the patent just has to say your kind of basic algorithm, your fundamental premise of it? It doesn't have to...

Steve: Oh, no, a patent doesn't have code. But the idea is you must disclose such that anyone who is well informed, who is trained in the art that the patent covers, would be able to reproduce your work. So, I mean, it is a guidebook to how to do this. And this is - I've got it probably to three or four things which are brand new that I've invented for CryptoLink. I'm still busy working on getting ready to start working on the CryptoLink R&D. So I'm still plenty ways a way.

Leo: You're a wise man. You're not going to make any promises about delivery dates.

Steve: Oh, god, I have no idea.

Leo: Okay. Good to know.

Steve: You wouldn't believe the rat hole I'm down in at the moment. I'm still messing around with third-party cookies, although it's become phenomenally comprehensive. So, and we found bugs in every Windows browser as a consequence of this work.

Leo: Oh, interesting. Oh, that's very interesting.

Steve: Yes, the browsers are leaking privacy, and no one knows it. So we'll be going public with that here shortly.

Leo: Oh, that's very interesting. I can't wait. So we're going to do some questions in just a little bit. I know you have a SpinRite letter. I have an Audible book to recommend. Why don't you tell us about your SpinRite letter first, then I'll tell us about the...

Steve: Well, this is a short little fun story that I got a kick out of. Again, I look for things that are sort of interesting. This says "SpinRite Saves an Artwork." And I thought, huh? Anyway, Gregory Mills wrote, saying, "Steve." Oh, he's a sculptor and an IT manager. That's an interesting combination. He says, "Steve. I just ran Panda's new active scan" - oh, no, I'm sorry, he was talking about getting a false positive on DCOMbobulator, which is not uncommon because my freeware sometimes has the same code that the malware has in it in order to do what it does. So anyway, he said, "I also thought you might like to know that SpinRite recently saved an artwork in the museum I work in. We currently have an exhibit with a digital artwork running in one of our galleries. The artwork is actually running on a laptop hidden in a pedestal. The artwork stopped one day, and the computer would not boot. Needing to get the exhibit up and running, I quickly bought a copy of SpinRite and was able to burn it to a disk within just a few minutes, thanks to your easy checkout and download procedure. I let SpinRite work its magic, and about an hour later the laptop booted back up. I got the exhibit up and running with about 30 seconds to spare before a group of 50 fifth-graders came in for their tour. I listen to Security Now! every week and really appreciate all the work you do to educate us on computer security. Say hi to Leo and thank him for his hard work, too."

Leo: Oh, that's great, that's great. Well, SpinRite does it again. GRC.com is the place to go to get SpinRite. I want to mention also before we get into our questions - we've got, as usual, we've got a dozen great questions. But we have the Winning Kick Ass Revelation of the Week and the Astute Observation of the Week and the Great Quip of the Week. So you've got some winners in here.

Steve: You know, Leo, I'm watching you as we're doing this. And you're flailing around with your hands.

Leo: Well, I'm a programmer.

Steve: Well, I'm the same way. And I'm realizing that, when I get a microphone like yours, then I would feel different about being on camera. Because, I mean, here I am, I'm hunched over my Heil, kind of like I'm some old-time newscaster. Well, let's see, "Robb in Orlando, Florida, asks" - and so that would make a big difference.

Leo: We're going to get Countryman for everybody. I mean, I think this is the key. I'm wearing a little headset mic. And I didn't, you know, I was wearing it last week, and it was very echo-y because the room is very live that I'm in. But we've, you know, there's stuff. The room is a lot more full than it was last week, and it's getting fuller still, and I think it's not nearly so echo-y. So good news. And for those who are watching at home, I just want to point out the reason you're only seeing me right now - Doug Kaye just sent me a note saying you ought to get a teleprompter so you don't have to look off-camera for the chat. Good point, I am looking off camera for the chat. But remember, I'm always on camera right now, where eventually we'll be able to see Steve, and I'll switch to Steve, and then I'll read the chat, then I'll switch back. So the reason you see me look off camera a lot is because I'm on camera all the time. We want to see Steve. We want to see everybody. So that's going to happen. So you think you'll be able to send video?

Steve: I think that sounds like fun.

Leo: We'll get you one of these mics...

Steve: Yeah, I think that sounds like fun. I mean, there's not much to see here. But at least both of us are gray now, so...

Leo: Yeah, exactly. Are you gray? You're not gray.

Steve: Oh, my goodness, am I.

Leo: When did you go gray? You weren't gray the last time I saw you. You were a little salt-and-pepper.

Steve: Well, there's more salt now than pepper.

Leo: We'll get you a camera. And then the other thing I really want to do for you is get some sort of virtual whiteboard we could put on the website so you can draw. Because I know you like to draw.

Steve: Oh, yeah. I don't have enough going on right now.

Leo: All right. So we are going to get to our questions now. We have a good dozen of them, and I'll start with number one. This is Mitchell, who listens to us in London. Hello, London. He worries about Google Mail cracking his 128-bit AES encryption. How did they do it? He says: Hi, Steve and Leo. I'm a big fan of the show, long-time listener. Steve, I'm a SpinRite user. And although I have no incredible stories to report, I find it to be an invaluable part of my toolbox. If he has no incredible stories, it means he hasn't had any hard drive failures yet, so he's a lucky man.

He says: I have a question which I hope you can answer. I recently rebuilt my Firefox profile from a clean installation of Firefox. I had accumulated way too much junk from all the plug-ins and so forth. I had installed - if ever there was a needed piece of software, it would be for a Firefox profile cleaner. You can actually, I think, just throw out the profile, can't you, and start over? Anyway, he says, I zipped up my new clean profile, which by the way was now 2MB down from 12MB, and attempted to email it to myself at home. He says he used WinZip, and he used the built-in WinZip encryption, which is 256-bit AES encryption. He used a 26-character password. He attached it to an email in his Gmail account, and he sent it. After a long think about it, Gmail decided to come back and said it had detected an executable and couldn't send the file. So now I want to know, how did it detect an executable? Is it able to look into my 256-bit encrypted file? That's a good question. Maybe it just says a zip is an executable.

Steve: Well, no. What's happening is - I've noticed this myself. I can't remember, I was sending a JPEG to someone through Gmail. And when I went over to Gmail it said it was checking it for viruses. So it's filtering attachments.

Leo: As it should.

Steve: As it should, which is a good thing for...

Leo: As all ISPs should do.

Steve: Yup. And what's happening is, I'm sure in this case it's looking at the file header that he's attached Maybe it recognizes as a WinZip. I don't even know, and I know nothing about the container that this 256-bit encryption is in. It'd be nice, for example, if there was no header. But if WinZip encrypted the entire thing so the whole blob looks like random noise...

Leo: Yeah. I'm sure it doesn't because it has to see it as a WinZip file and then ask for your password and unencrypt it.

Steve: Probably good enough, then. But in this case I'm sure, I mean, either Gmail recognized it was a zip, or it looked at the header and didn't recognize it as something that it was able to interpret because normally the way these AV systems work is they'll look at the header, and they'll say, oh, you know, this is a JPEG image. So it then knows how to parse the header and check the image for any inconsistencies and, for example, if the JPEG might be carrying a virus that's taking advantage of some image processing vulnerability, which we have had in the past.

Leo: Now, I've seen in our chatroom a number of people say unless you specifically obfuscate the directory, even though the files are encrypted in the zip, WinZip does send a directory of files. So it can see the names of the files in that bundle.

Steve: Ah, interesting. So, oh, even the names of the files?

Leo: Well, I don't know. I'm looking at the chatroom. But a number of people have confirmed that. And apparently there is a setting in WinZip that says you can obfuscate the directory. So if you don't do that, it might know that you have executables in there.

Steve: Wow. Well, we talked about a really cool encryption program called AxCrypt. That's what I would recommend. I mean, if this is the case, there's a lot of information leaking out of WinZip's encryption. And so it would make much more sense. AxCrypt is a beautiful, well-behaved little standalone encryption program that would have been able to take that profile and turn the entire thing into noise. And it would be interesting to see whether then Gmail would say, oh, I don't know what this is, but I don't see any viruses in here, and it may well have been able to go through in that case.

Leo: It may just reject blobs of random binary, be thinking, well, there must be something here.

Steve: It well could.

Leo: Yeah. And you know what he didn't say, but maybe, you know, you can save a zip file as a self-extracting executable. If he did that it would be an EXE file.

Steve: He's a Security Now! listener, though.

Leo: He's a smart guy, he wouldn't...

Steve: He's on the ball.

Leo: He wouldn't do that. Robb in Orlando, Florida is asking about something that just came out in the news this week, quantum computer cracking crypto: Hey, Steve, I'm curious. Will today's encryption stand up to quantum computing? I can't say that I completely understand the ins and outs of quantum computing - very few people do, don't worry. But I do know it will enable PCs to be millions of times more powerful than they are now, at least that's the advertising. How will our current encryption algorithms stand up to that kind of power? Will we just need to come up with something better? I'd assume that the government will be among the first to have such computers. Will encryption become trivial for them to break before those quantum processors are in widespread use? I'm not at all mathematically inclined, but you have such a great talent for putting this stuff in terms that even I and Leo can understand. Thanks for that. "And Leo." And in fact there was a story, but I'll get to that after you talk. But there was a story about quantum crypto in fact being cracked. I thought that's what he was going to ask about. But let's talk about the fact that this is the promise that quantum - in fact, this is actually something that in the advertising for quantum computing they often mention can crack even strong crypto in minutes instead of millennia.

Steve: Well, as it happens, I took the opportunity to ask the guys who invented crypto while I was at the RSA conference.

Leo: Excellent.

Steve: The crypto panel did a Q&A afterwards, and I had known Diffie and Martin Hellman when they were working at the AI lab at Stanford back in '73 when I was there. And I said, so guys, what's the story with crypto and quantum computing? Is this just all over now? And what they said was really interesting. And I can paraphrase what they said. I'm going to spend some time looking into this so that Robb and our listeners can get whatever ability I'm able to find to explain exactly what the story is with quantum crypto.

Leo: I'd love a - you want to do a whole show on it? That would be a great subject, yeah.

Steve: Yes, I'm going to do that. What they said was really interesting. They said it's not at all clear that what it is that quantum computers are good at will mean that they're at all good at cracking crypto.

Leo: Oh, really.

Steve: Meaning that essentially the idea being that normal computers the bit is either zero or one, and with a quantum computer it's both. It doesn't have to choose.

Leo: And you have multiple states.

Steve: Exactly, it's multiple state. And one way to look at this is that it may very well be that the problem set that quantum computing can be applied to is completely different than this step-by-step algorithmic process that crypto cracking is today, which isn't to say that there may not be a way to crack crypto from a quantum computing angle. But if so, it'll be completely different from the way we would go about brute force cracking crypto now. So the idea that quantum computers are super powerful and strong and fast and whatever they are, and multi-state, it doesn't - it wasn't clear to these guys that that was going to create any weakness in contemporary cryptography. Which I thought was, you know, really interesting and telling.

Leo: Okay. That's very interesting. Yeah, because I know that we interviewed some quantum computing folks up in Vancouver there. That's where supposedly they've created the first working prototype, doesn't do very much. And they always use this as an example. Oh, we'll be able to factor prime so fast that we'll be able to break public key cryptography.

Steve: Yeah, well, the guys who - certainly the people at RSA have a stake in that not being the case. But they, I mean, the way they phrase it, I'll try to understand this better so I can explain it to our listeners in a way that even convinces me.

Leo: Good. I look forward to that. Now, there was a news story, there is also quantum cryptography which uses laser beams and kind of uncertain states to create crypto. And they were having trouble with the authentication part of it. But they've since gone on to, I think, fix that. So I...

Steve: Well, the cool thing in quantum communication, the quantum crypto communications, is that we're all familiar with the Schrdinger's cat deal where, you know...

Leo: Why don't you - I don't if everybody is. That's a great, I guess it's a mental exercise or mental experiment, as Schrdinger and Einstein used to perform these thought experiments. They call them...

Steve: Yeah, the idea - well, the idea is with quantum uncertainty is that the act of observing the state of something forces it to assume one state or the other. That is, so it's - and the idea with the cat is you could have a cat in a box. And the question is, is the cat alive or not? And it's...

Leo: It's both.

Steve: Exactly. The idea is, well, it doesn't have to decide until you open the box and look in.

Leo: Until you observe it, it could be either.

Steve: Right. And so they have actually - the physicists have actually figured out how to create a quantum mechanical link such that the act of observing it breaks it. Meaning that it is provably unsnoopable. You cannot snoop on it. You cannot inter...

Leo: But how would you get on...

Steve: ...[indiscernible] man in the middle.

Leo: How would you then decrypt it? Wouldn't that break it? I guess decryption is not considered observation.

Steve: Exactly. And the idea is that it wants to be, you know, it's like the - somebody wants to set up super secure optical links between two points where there's no way that a cat can be put into it that would allow it to be eavesdropped on. And the physicists can say we absolutely can guarantee you that nobody can intercept this or it just - it won't work. It'll completely break.

Leo: Makes sense.

Steve: Yeah.

Leo: Greg Christopher in the San Jose area, just down a little piece from me, is with Adobe on this one. He says: Hi, Steve. I was behind on listening to your podcast due to a busy work schedule, but was listening to your show on the whole disk encryption when I heard your comment regarding the turf fight between InDesign and TrueCrypt. My first thought was, little do they know someone on the quality engineering staff from Adobe listens regularly and has the ability to do something about this. Wow, that's great, Greg. That's exciting. You guessed correctly as to the root source of the problem - pun intended - and you guessed correctly that we licensed the technology, as it turns out, from Acresso. These guys, I loathe these guys, they're Macrovision. Right?

Steve: Yup.

Leo: That's me saying I loathe them. Greg didn't say that. But we've had, I mean, Macrovision has caused all sorts of problems. You also guessed correctly, it doesn't just affect InDesign. I'll give you the bad news first. First, all the Adobe Creative Suite 3 products, Acrobat 8 products, and many other products are affected. He sent us a whole list. The good news is that Adobe is changing the licensing code to avoid using track zero, and the next set of Adobe products will ship without using track zero for license compliance. Yay.

Steve: Yay.

Leo: I'm sorry that some of your very astute listener audience who are wise enough to use whole disk encryption have bumped up against this problem. See, he's saying really it's great that you use TrueCrypt, and we're sorry that this is causing a problem with our products. We try to make the process as painless and as invisible as possible, but no test plan is perfect. I can't speak for the company about anything related to software anti-piracy efforts. However, I think you might find it interesting that only a fraction of the Adobe software in use is actually paid for. These losses can obviously add up, resulting in fewer people available to create and test the products. My personal feeling is we do a pretty good job given our constraints. Big thank you to those who take software licensing seriously and realize that that is money that keeps the new and interesting stuff rolling out of Adobe. And of course if everyone did that, this problem would likely never have happened. Love the show. Keep up the great work. So he's giving a rationalization which I hotly debate, but I won't do it here, for why they use copy protection on there.

Steve: Yes. And the good news...

Leo: And I had that hot debate, by the way, with Adobe people, so I don't need to have it with you guys here.

Steve: Yeah. And the good news is they're going to be moving away from it. So that's...

Leo: Well, they're going to move away from that. They're going to change how they do it. I guarantee you they're not moving away from anti-piracy.

Steve: Oh, no, no, I'm sorry, you're right. I meant that they're going to be moving away from track zero that was colliding with TrueCrypt. And remember that 5.0 we immediately got feedback from our listeners saying, hey. They installed some Macromedia thing, I guess InDesign was what in this case the guy was talking about. And suddenly he couldn't log onto his TrueCrypt volume anymore. And of course 5.1 fixed that by making the track zero data redundant, so that it would tolerate having Adobe there sharing track zero with it.

Leo: The real problem is, and I don't care what they go to, ultimately DRM always causes problems. It breaks something no matter what. And it's always the honest guy who suffers from it; right? That's what really gets me. Pirates just take it out.

Craig Cuttner in Connecticut has a need for speed. He says: Love the podcast - loads of great information with just the right amount of geek speak. He must have a high tolerance for geek speak. In SN-140 Steve mentioned a media encoder, MPEG/H.264, he's not sure, that effectively used multicore resources. Many of the professional encoders that are available just call some stock Microsoft DLL and do a mediocre job. So what brand of encoder is Steve talking about? What's the one he likes? What's the one that uses multiple processors? Thanks, and keep up the good work. We should mention this was when you were talking about your monster quad core and how that very little software took advantage of it except for this one encoding program. What was it?

Steve: Yeah. Well, I've been a media guy, as you well know, Leo, for years. I just - I love doing stuff with media. And I watch movies on my Palm Pilot by encoding them. There is a company that I can recommend absolutely without reservation whose products I've been using for many, many years. Their very first MPEG-2 encoder had a horrible name. It was TMPGEnc. It stands for Tsunami MPEG Encoder. And it then sort of - it went from shareware to commercial and continued to do very well. Anyway, this is - it's Pegasys-Inc.com, with a hyphen. Pegasys-Inc.com. And they've got English and Japanese versions of their website and maybe, I hope, I think, a couple other languages, too. I use all of their stuff. They've got a fantastic encoder that does do MPEG 1, 2, and 4, which is the H.264 encoding. And they've got a very nice, simple DVD authoring tool.

When you compress the media into MPEG-2, which is what DVD requires, then you've got an MPEG-2 file. Oh, it also does AC3 compression, which is rare to find in a media encoder. And that's really the audio compression that you want for DVD because you either have to, for domestic DVD, it's either going to be non-compressed audio or AC3. European DVD understands MP3, but domestic DVD players won't decode MP3. So you can only compress with AC3, which is the Dolby Digital compression. But when you have that file, that's all you've got. You still need to author that onto a DVD if you want it to be playable in a DVD player. They've got something that does that. And you can set up either a no-menu DVD where you just put the DVD in and it just kicks off and plays, or you can - they've got full menuing editing abilities, so you can do, like, multi-episode DVDs and make them yourself.

Anyway, I recommend their stuff. I have never had a problem with it. It's very mature. And, I mean, the only thing I have found that just soaks this quad core machine. And boy, I mean, this quad core machine with the Tsunami products, the Pegasys-Inc.com products - I still call them Tsunami because that's what they always were for me. It's unbelievably fast.

Leo: Makes a big difference to have all those processors, yeah.

Steve: Oh, a huge difference with this machine.

Leo: I think that that's one thing we've often said, which is it is really things like that, like transcoding, or encoding in the first place, that really multicore processors make a big difference. Most of the stuff you do, you don't need four cores to do word processing, to balance your checkbook, to surf the 'Net. But you do need it where there's CPU-intensive stuff. But that's not a lot of what you do, I think that was the point you made.

Steve: Right.

Leo: I think, you know, I'm looking on the Mac side, I think that there are quite a few now that are multicore-enabled, partly because OS X just kind of makes it so easy to do that. And the development tools make it so easy to do that. And that's a case of, again, developers relying on libraries. And if Microsoft's libraries don't do it, they're not going to do it. And if Apple's libraries do, they will do it.

Steve: And I have to say, Leo, I'm unimpressed so far with Mac's compression. I've tried, I've got a bunch of Macs, and I own the DVD Studio and the standalone Compressor product...

Leo: [Indiscernible] that stuff. You don't like Compressor?

Steve: I hate it.

Leo: Really.

Steve: I do not. Unh-unh. I don't - I want more control. And it's all generic.

Leo: Ah, yeah. Yeah, QuickTime Pro, surprisingly, gives you a lot of control, if you get into the settings deep enough. I think that's what Alex uses. I'll have to ask him tomorrow when he comes with MacBreak Weekly. Because a lot of people talk about Compressor and like it. I don't, I don't usually use it. We might have to start doing it, now that we're going to start doing some video.

Ken Juenke in Sparks, Nevada wants to "Yubi-Logon" to Windows: Steve, thanks for taking the time and effort to introduce us to this great product, YubiKey. That was our last episode. I, too, feel it's revolutionary. I'm going to follow its introduction to the marketplace with great interest. As I listened to the last podcast, I was hoping you would discuss the use of YubiKey with regard to authenticating a user's Windows session. I'd really love to give all my users a YubiKey to use when they log onto their computers. What a good idea that is. I've emailed Yubico about this topic and received a reply telling me this functionality is coming. Can you please keep this on your list of what you'll be discussing in future episodes about the YubiKey? Thank you so much, keep up the great work.

Steve: Well, this is sort of - I wanted to put this question in because so many of our listeners asked about, I mean, they were interested in the YubiKey and enchanted by it. But because support for it is not yet widespread, they were like, okay, well, I want one, what can I do with it? And then they're looking around for something to plug it into. And, I mean, figuratively, like what can they do? And so let's merge this with the next question because I'll cover both sort of at once. From a technical standpoint it's got sort of the same answer to it.

Leo: Okay. Okay. The next one's from Daniel Ernst. He's in West Bloomfield, Michigan. He wants to use YubiKey for TrueCrypt, another very good idea, I think: Steve, I was so intrigued with the YubiKey at your first mention of it in Episode 141 I ordered it immediately when the price was still in euros. What, do they sell it now in dollars? I just got it today, and I love playing with it. I wish I had some practical use for it. Again.

Steve: He keeps touching it and spitting out random-looking character strings. Hey, isn't that cool, that's all crypto. Wish there was something I could do with it.

Leo: All right. Seems like there would be some way - I guess when a website asks you for a password you could do that, but you'd have to have some way of remembering it, maybe RoboForm or something.

Steve: We're going to talk about that as we go through.

Leo: Ah, okay. I know it's meant to provide authentication via the web, but could it also be used locally to provide authentication for an application running on my local machine, something like TrueCrypt? I use pretty strong passwords when using my two favorite security apps, TrueCrypt and Password Safe, a great password program originally written by Bruce Schneier. But it's not easy memorizing strong passwords, then typing them in without error. I'd love it if I could plug in my YubiKey, touch the button, and be in. Is it possible to incorporate code into an app so that it can authenticate a YubiKey locally? Oh, now you got me going. I'm intrigued. TrueCrypt and Password Safe are both open source, so I assume it's permissible. That's what you need to do.

Steve: Okay. So let's talk about the idea of local authentication because it's a mixed blessing. The way, as both of our listeners understand it, is that the normal way you would use the YubiKey is much as VeriSign works with their VIP system, where you have a - somewhere is a remote server which knows all of the YubiKeys it's responsible for, and one or more relying parties, as the jargon goes, someone who wants to rely on somebody's authenticity will accept the YubiKey token from that person as they're logging on, then turn around and ask the central authentication server is this valid. That has a couple reasons why that's being done.

First, the relying party does not need to know anything about the YubiKey, that is, it does not need to have its secret 128-bit AES key. It simply forwards the string that it received to the authenticating server and says, is this correct. The other thing is that the authenticating server is able to maintain the knowledge of the most recent count which is part of the YubiKey token once it's decrypted it. So it has the YubiKey's key, and it knows which is the most recent password it has seen. Well, that's important because it prevents a replay attack. If you were having multiple authenticators, then someone could catch a YubiKey string going by to one authenticating server and feed that to another authenticating server that wouldn't know that the first one had already seen that. So that's why you need to have centralization of this in order to prevent replay attacks. So that's the normal network model for authentication.

Now, both these guys, and many of our listeners, I mean, I saw many questions about TrueCrypt, many questions about Windows log-on. The catch here is that we would be authenticating locally, meaning that the - presumably the system that you are trying to authenticate to would need to know your YubiKey's 128-bit AES key. And that's dangerous because it could get away from it. It could get out of its control. The beauty of using a third party is that they're super security, super trusted. They've got big guard dogs, you know, barking at people who approach too close to the building and so forth. So nobody has a chance to compromise the key store. Okay. But I thought about this for a while because it would be cool to be able to use the YubiKey, for example, at boot time to authenticate to TrueCrypt. And...

Leo: I should say that the problem you're talking about is exactly why you can't make a DVD that's uncrackable. Because the key has to be stored in the player. Right?

Steve: That's exactly the case, yes. That's a good analogy, Leo. And we've talked about this, I mean, why it's fundamentally impossible because any technology that you have total access to, you have total access to.

Leo: Right. And if the authentication code is in there, you're going to see it. You're going to see it whether you store it in memory or - that was that whole thing we were talking about with freezing memory is because the key's in memory.

Steve: So the TrueCrypt is interesting because it is open source, and it would certainly be possible for someone to modify the boot screen, given open sourcedness, to be

YubiKey compatible, if that made sense. And in the Windows case, Windows has a modular log-on system...

Leo: It's got a hook, yeah.

Steve: Yeah, GINA, G-I-N-A, is the dll that does log-on, sort of the log-on experience. And that is replaceable.

Leo: Sure. That's why you can use a thumb-recognizing or a fingerprint-recognizing, yeah.

Steve: Exactly, exactly. So, okay. So let's take a look at the TrueCrypt example. So we've got the YubiKey. Now, there's stuff that's changing all the time that we would not be able to use, or wouldn't necessarily be able to use. The idea being we want to associate a YubiKey with a laptop, for example. There is information which is not changing, though. Remember that the first 12 characters of the string is in the clear, that is, it's cleartext. It is just the YubiKey's sort of public ID. So 12 characters, and they use this mod hex encoding which is very much like hex except they don't use 0 through 9 and A through F. They use a set of alphabetic characters that are in a uniform position on all keyboards. So it looks more crypto than it really is. And they're storing four bits per character.

So that 12-character preamble on the front of the YubiKey is 48 bits of data. That is, it's six bytes, 48 bits. Well, that's a lot of bits. I mean, it's not 128 bits. But 48 binary bits gives you 281 trillion possibilities. Actually it's 281 trillion, 474 billion, 976 million, 710 thousand, blah blah blah. So it's a bunch. So one interesting possibility is just to use the first 12 characters of the YubiKey. It's going to save you from having to type those. It's never going to change. And brute forcing it, although not impossible - again, it's not 128 bits. But 281 trillion, that's a lot of combinations. And they do appear to be highly random, pseudorandom tokens on the front of the key.

Now, if you knew the 128-bit secret AES key, then you could decrypt the balance of the YubiKey data. And that would give you another unchanging six bytes. Remember that the first six bytes of the YubiKey is its secret ID. So if you were willing to have the system know your 128-bit YubiKey AES key, then - and that represents some vulnerability because it could get away. But if you were willing to have the system know that, then it could decrypt the balance of the 128 bits and get another 48 bits that never changes. And that would give you 96 bits. Well, now we're talking serious strength because that's that 281 trillion, 281 trillion times. So that's, I don't know what big number that is. But, I mean, that's big.

So one interesting possibility would be, first of all, you might say okay, I'm only going to use this YubiKey for authenticating my various laptops, that is, for running with TrueCrypt. So if I'm only going to use it for that, I don't care of the 128-bit key gets loose because I'm not going to use it anywhere else, and nobody else can do anything with it. Anyway, it is going to be in the laptop.

Now, one way to prevent it from getting loose is the TPM, the Trusted Platform Module, which laptops are now generally shipping with, because the TPM is able, I mean, this is exactly what it was designed for. It performs AES encryption, and it stores keys. So you could put your 128-bit AES key from the YubiKey into it. Doing so represents no vulnerability because it can never come out. And you then give it the YubiKey's ASCII string, convert that back into binary, ask the TPM to decrypt it for you, and that would give you the other six bytes. So if you put those together you've got 12 bytes, 96 bits, and a ton of security. Basically that would then allow you to use that as the passphrase to hand to TrueCrypt to decrypt your drive. And you'd have something that was extremely robust.

Leo: But of course you're relying on some way of storing these keys on the laptop that is secure, and that's why you're relying on TPM. And I'm always, you know, I mean, look what's happened with DVDs. I guess if there's an incentive for people to crack these things, they can.

Steve: Well, okay. Here's the point, though, is that without the YubiKey available, presumably someone's going to take your laptop and not going to have your YubiKey and crack it. So they're in bad shape. You've got a 96-bit, high-entropy, I mean, essentially completely random set of bits. That's 281 trillion trillion, or 281 squared trillion trillion, possibilities. Now, they could get your YubiKey's 128-bit key. That doesn't help them, though, because they need a string from your YubiKey in order to catch the first six bytes from the unencrypted preamble and the second six bytes from the decrypted internal in order to get all 96 bits. Well, so we're assuming they're going to have your laptop but not your YubiKey. So, I mean, and that's the whole point of multifactor authentication.

Leo: Right. If they had the YubiKey, they'd press the button. And then they wouldn't need the YubiKey. Right, that makes sense. Dave Rodgers, Green Bay, Wisconsin has been thinking about DNS. He says: Dear Steve, Windows XP allows you to change your DNS server settings to use the Netgear router's gateway IP as a DNS server, 192.168.0.1. Is this more secure or less secure than using your ISP's default DNS IPs? Unless the Netgear has a DNS server built into it...

Steve: Precisely. That was what I wanted to mention was that the consumer routers, these little plastic boxes, do not have a DNS server built in.

Leo: So what's it do? It goes, I don't know.

Steve: It turns around and just basically it does NAT on the DNS query and just sends the DNS query right back out, just like you do, to the ISP DNS which it has received from its DHCP query of the ISP's connection. It would certainly be possible for a higher end box, if somebody were running Linux or a UNIX machine as their gateway, it could be running a full copy of BIND, as I do on my own FreeBSD box here, in which case I have no ISP's DNS that I'm using, which is what I was talking about before. But you're right, Leo, one of the standard little consumer routers, they're not doing their own DNS lookup, they're merely forwarding the query that comes in to the ISP's DNS server.

Leo: The key is you've got to forward, you've got to use an actual DNS server for this thing to work, whether you set one up yourself, you use OpenDNS. I know people who use Verizon's DNS even though they're not customers. But whatever you're doing, you're going to use somebody else's. And the only way to protect yourself for privacy reasons is to run a DNS server, get SmoothWall or Astaro or something.

Tom Fenton and his classmates at CTU in Denver, Colorado - is that Colorado Tech? I think it is - wonder about Deep Packet Inspection: My classmates here in the Network Security Class at Colorado Tech University - oh, I got it - want to know what the deal is with deep packet inspection. We've read that this type of network analysis will break encryption since it works all the way down to level two of the network stack. Are we wrong in this thinking?

Steve: Well, deep packet inspection is - essentially it's a fancy-sounding word for doing more than looking at the headers. Most firewalls, and NAT routers, for example, well, NAT routers is a little bit of an exception, which actually is a good example of this. But simple packet filters, they're not concerned at all about the content of the packet. They look at the headers, and that's where you find IP address and port number and protocol type and packet type, like if there's a SYN packet it's because it's got its SYN bit set. And so early packet filters, where you didn't want to allow incoming connections, all they did - they were sort of dumb. But they just looked at the header, and they would drop any packets who had a SYN bit set. Because if you do that, then no SYN packet can make it past them, and it becomes impossible for someone to access your servers.

Leo: Is that stateful inspection?

Steve: No, that's stateless inspection.

Leo: That's stateless. They don't care about what's going - what the conversation is. They're just looking for certain little things in there.

Steve: And for example, here that factors in perfectly because, for example, that would mean that if you sent ACK packets through, a firewall would allow those because they don't have the SYN bit set. So a stateless firewall that is not maintaining state, it would only drop SYN packets but allow, for example, ACK packets through.

Leo: Presuming a conversation is going on.

Steve: Exactly. But a stateful firewall, it would say, what's this ACK packet? I don't have a conversation happening now. And, for example, it would see a SYN packet going out, and that would tell it to expect a SYN/ACK coming back and then follow-on packets. So it would sort of be maintaining a state of what's going on. Now, NAT routers have to do a little deep packet inspection because some protocols, for example FTP, embeds in the FTP packets, for example, the port and IP number of the client because FTP involves two connections. That is, active FTP does. Passive does not. And so NAT routers that are FTP aware, they will actually see the FTP packet and reach in and modify the contents of the packet on its way out so that it's to adjust the IP and port number that the FTP server behind the firewall has suggested the client connect to it on. The NAT router needs to change that for active FTP connections to make it correct. So there's a little bit of deep packet inspection going on.

Now, what Tom is referring to, with his classmates at CTU, this deep packet inspection means looking at the actual contents of the packets beyond just their headers. And so the question is, does it break encryption? And the real - the answer is no. Encrypted traffic cannot be deep packet inspected. And in fact, using encryption is one way of thwarting and avoiding any packet inspection. People increasingly use it because ISPs are unfortunately becoming increasingly snoopy about people's traffic. And if you set up encrypted connections, nothing your ISP can do. There's no way for the ISP to intercept that traffic, as we've talked about, you know, on many occasions.

Leo: I bet what they're thinking about is a situation - since they're at a technical university, they're probably learning about networking - is a situation where a business is taking the SSL and doing it themselves. And in that case they have the ability to decrypt because it's their SSL certificate, not Amazon's or whoever.

Steve: Right. If the business is setting up an SSL proxy, then it's able to decrypt and reencrypt, and in the intervening time look at everything that's going on.

Leo: Then you could do a deep packet inspection that would actually be meaningful and revealing.

Steve: Right.

Leo: But we've talked about that before. That's another issue. Robert Berry in North Carolina doubts that his credit union knows how to factor: My credit union, he says, has recently, with much fanfare, rolled out what they call "multifactor security." But it turns out all they've done is to add additional prompts to the log-in process - don't get me started - asking security questions like your mother's maiden name or the name of your first pet. And they don't even ask these with every log-in, just once in a while. Is it even legitimate to call this "multifactor security" at all? Seems to me that it only serves to inconvenience customers while providing no actual protection against identity theft. They claim they're doing this to comply with a directive issued by the Federal Financial Institutions Examination Council. I have a hard time believing this satisfies any such requirement. Oh, oh yes, it does. I'd be interested to know if you have any recommendations on how I can convince my credit union to implement real multifactor security. I'm sure cost is a factor, but there has to be something they can do relatively cheaply that is better than this.

Steve: Well, what they could certainly do - well, okay, wait.

Leo: First of all, this does satisfy the FFIEC requirements because they're so pathetic.

Steve: It's really distressing, yes.

Leo: That's why the SiteKey happened.

Steve: Yup. So I would say in response to the question is this real multifactor security, no. As we know, multifactor means not just more of the same factor.

Leo: Not just more of something you know.

Steve: Yes, exactly. It's like, so tell me something more that you know doesn't solve the problem because, for example, it's completely prone to any kind of replay attack or keystroke logging or man-in-the-middle interception sort of things. I mean, that's why something you have is a different factor; or something you are, like a fingerprint, is yet another factor.

Leo: And I have to say my bank, a big bank, Bank of America, does exactly the same thing as his little credit union is doing. When we log in from a new computer it says, oh, you'd better answer these security questions. As if that's somehow making it more secure.

Steve: Yeah. I mean, it makes it - I guess the idea is it tricks the users into thinking it's more secure. I guess instead of multifactor, it's mobi factor.

Leo: Mobi?

Steve: Mobi factor as opposed to multifactor. But, yes, this really doesn't do it. And, I mean, the answer is to go with a common available technology. I mean, it would be very cool if banks were making YubiKeys available and providing those. We know they're not very expensive in volume. Or things like the PayPal football or the VIP security card. We're still at the beginning stages of this. But we know that authentication is the big problem that we need to solve. And we'll be doing that as we move forward, certainly.

Leo: You know, I wish - you know, I have the football here. But I wish that more banks would do what my - this is the funny thing. That little thing that BofA's doing with me with the extra questions is on my business account. For some reason, and maybe it's just because it's a business account or whatever, they haven't enabled the very real and, I think, good authentication they've enabled on my personal account, which is, if I'm new to the account, or I'm using it on a different computer, it says, okay, we're going to send an authentication code to your cell phone, which has previously validated my number, so I know they know it's my phone. And now that's something I have, right, it's that number that's come to my cell phone. That's real authentication.

Steve: Yes. And you're right. So there's an example of a potentially zero cost...

Leo: Cheap, yeah.

Steve: Yes, yes. Although...

Leo: They don't have to send anything out, they just call my phone [indiscernible].

Steve: And the thing to do would be to not require it because you might have users that, for whatever reason, don't have a cell phone or...

Leo: That's exactly what they do, yeah. They offer it.

Steve: Exactly. And explain that this is - if you want enhanced log-on security, you can turn on cell phone loop authentication, and we'll make sure, we'll take the extra effort to prevent anybody from logging on as you.

Leo: And I did that. But for some reason I can't do that on this business account. But maybe they don't have it on all their accounts. I think it's a great idea.

All right. Are you ready, Steve, for the Quip of the Week? We've actually never had a Quip of the Week before. This is from Anonymous John in Oregon. And he says: Security Now! is costing me a fortune. So, he says, I just ordered a YubiKey. Let me tell you how that happened. I'm listening to the YubiKey Security Now! podcast. I figure I need a YubiKey (Security Now! influenced purchase) because it sounds so cool. So I fire up a portable version of Firefox from my IronKey (Security Now! influenced purchase), and I start up a secure session and head to Yubico.com to order the YubiKey, which I paid for via PayPal after securely authenticating my PayPal football - where is my football? Gotta hold it up whenever anybody says "football" - (my Security Now! influenced purchase), and finish the order. Really glad you guys don't talk about cars or private jets. Yeah, well, for that you have to listen to the Daily Giz Wiz. That'll make you buy other stuff. Sorry we're costing you money. But it's good stuff; right?

And then here's Tom Willwerth in Seabrook, New Hampshire. He has the Astute Observation of the Week. Now, this isn't the super astute one, this is the medium astute one.

Steve: This is not the Kick Ass Revelation.

Leo: I get confused. You know, as we do more and more video, I think we need graphics and music and stuff. It's the Astute Observation of the Week. Steve, I'm an avid listener of Security Now!, also a SpinRite customer. Yay. I've enjoyed your talks about EV certification in the past few episodes. That was that new high-end certification that we're saying you ought to do, even though it's more expensive. He has a quick tip of EV certificates in Internet Explorer 7 that may be good to share with the listeners. He says he tried to follow your example in checking out both

VeriSign and PayPal to see that neat green bar that we mentioned. That's what you get when you go to an EV certified site, as long as you're using the latest Internet Explorer. He says, the problem is I could never see it. After doing some trial and error, I found that in order for the green shading in the address bar and the company name display to appear, you have to turn on the phishing filter in IE7. That's funny because I turned off the phishing filter. I don't use it. He says, now, I'm a pro user, and I figured the phishing filter would slow down my machine, so I shut it off. I didn't relate it to the EV certification. He thought it was just, you know, a phishing filter. I would say that Microsoft's support for the EV certificate is part of their anti-phishing technology. Part of, this is an important distinction. Many users would just assume the green bar comes as part of the core certificate functionality of the browser. You know, I wonder because I...

Steve: I verified.

Leo: Is he right? You have to have it turned on?

Steve: He's absolutely right. And that is really annoying.

Leo: It is because I don't need to have - because the rest of that functionality is you go out and check a database. I don't need them to do that.

Steve: Well, exactly. And he's right that, you know, if there's some checking database turnaround time, and you're prevented from going to the site until Microsoft gives you the thumbs up, you could certainly see that that's going to slow down your access. So, but the idea that turning off the phishing filter turns off the EV certification display, I mean, that's nuts. It certainly doesn't have to. I mean, that's just some bozo at Microsoft decided, oh, let's, you know, if you're going to turn off the phishing filter, then we're not going to let you know if you're using an extra secure site. It's like, uh, yeah, that's a good idea.

Leo: Well, the good news is Firefox doesn't do that. So the green bar is there whether - and I don't think - actually do they have a - I don't even know if they have a phishing filter in Firefox. They probably do. For the alliteration alone.

Steve: I guarantee you they've got an add-on for it, if they don't...

Leo: Yeah, yeah. Tim Madison in Westchester County, New York, has the long-awaited Winning Kick Ass Revelation of the Week: Steve, you mentioned on the RSA 2008 episode - that was a few episodes ago - that your credit card information was stolen while most likely using a site that doesn't support PayPal and/or Google Checkout.

Steve: Yup.

Leo: While I may not be as paranoid as you are online, I do like to refuse many online retailers my information by making use of PayPal and Google Checkout. For sites that don't support these options, I use one-time use credit cards from PayPal, which is actually very cool. Actually I used one of these when I bought SpinRite, it worked just fine. And here's how you do it. Because you don't support PayPal on SpinRite.

Steve: Correct.

Leo: You need a credit card number.

Steve: Correct.

Leo: But you don't have to have a credit card if you've got PayPal. You log into PayPal. You click "PayPal Plug-in" under Tools.

Steve: And that's the only entry that's in the Tools menu at the moment.

Leo: Tool. You don't need to install the plug-in, by the way, you can use these cards just at the website. See, I'm glad to know that because I thought I had to install it. Click "Secure Cards." You can then generate a one-time use card funded through your PayPal account or a multi-use card that only works for a single vendor. So if I'm going to always use it at Amazon, I just always use it at Amazon. That way you could set up something that bills you monthly, but you never have to worry if it's getting stolen. All charges from any other merchant will be rejected. This is fantastic. You're right. This is a revelation.

Steve: It is fantastic, Leo. I tried, as I mentioned before many, many months ago, to get whatever it was I had to do on PayPal to get access to their little freebie thing. They had an app that you could download. But I had to get a PayPal credit card in order to enable that. And I tried to apply, but something about my credit reports threw it off. And when I got all my credit reports, there was one time where someone changed my residence information and was sending stuff to another state.

Leo: Oh, man.

Steve: It was a credit card scam. It was another, again, on my identity problem. And so I think that's forever thrown off my ability. So if you don't - if you can't use their automation to one-click credit card approval, and I can't, then I was completely blocked from doing anything like this. So what I loved was Tim brought it to my attention, and I want to make sure our listeners know. We know we've got a bunch of PayPal users because look how many footballs we're responsible for selling, at $5 for the PayPal football. So this means that PayPal will now issue you, without needing anything other than a PayPal account, one-use credit card numbers. And this is fantastic.

Leo: More reasons to use PayPal. Now, I have to ask you, though, Steve. Somebody called the radio show and said, I was listening to Security Now!, I heard your discussion of the fact that PayPal will log through DoubleClick. And he said that makes me want to stop using PayPal. Sounds like it hasn't discouraged you from using PayPal.

Steve: Well, and we have been critical of PayPal in the past. And I will continue to be. It's certainly the case, he's certainly right. Remember the time that we talked about all the different URLs, all the different links on PayPal's page that loop you through DoubleClick, even though they've got nothing to do with...

Leo: With no reason.

Steve: No, absolutely no reason. I mean, so as I have said before, I would love for PayPal to have some serious competitor come along. And Google Checkout, of course there's Google. I think they bought DoubleClick, didn't they?

Leo: Yeah, so you know that's...

Steve: We need somebody who's interested in doing this kind of really good job, that arguably PayPal and Google both do, but who also is serious about honoring our privacy. And anybody who bounces their URL through DoubleClick is just not serious.

Leo: Nevertheless, they're awful convenient.

Steve: I'm using them because they're the ones who are there. And I just - I wanted to bring to our listeners' attention that they now offer, just having a PayPal account, one-use credit card numbers.

Leo: I'm on my PayPal account. Now, you said...

Steve: It's a menu bar over on the upper left. And right under Tools should be...

Leo: I see Auction Tools.

Steve: ...PayPal Plug-in. Oh, in fact, let me see [trumpeting sound].

Leo: Products and services. Because I want to use this. This is great.

Steve: Yes.

Leo: And in fact I do have - I have a number of subscriptions. So the idea that I could have, say, you know, Amazon is a good example. And I can set up this credit card without giving it out. Because, you know, it's funny, my credit card company called me the other day because I was in Australia, and I bought some shoes. Dvorak always says if you buy running shoes, that's a red flag. In fact, he said if you want to get a credit card canceled, fill up two different cars with gasoline, right, one after the other, then buy a pair of running shoes.

Steve: I believe him on the gasoline.

Leo: It makes sense. He says apparently that's what happens is somebody will steal your credit card, they immediately not only fill up their tank but their friend's tank, and then they buy running shoes.

Steve: Okay, now, I just logged in, and I'm looking at a redesigned website. And on the left-hand side I've got a column of stuff. Oh, and I've got a nice big green bar up at the top saying "Identified by VeriSign." And I see PayPal Plug-in is the one thing...

Leo: Ah, there it is. I see it, okay. It's on the left, yeah.

Steve: Underneath Tools on the left, exactly, in the left-hand column.

Leo: Now, see, I went there, and I thought, oh, I don't have Windows. Oh, I don't want to install a plug-in.

Steve: I know. And so then you go - you click that, and then the first thing down below is Secure Card.

Leo: You don't have to have the plug-in to do it.

Steve: You do not need the plug-in.

Leo: Oh, I'm so happy about this.

Steve: Yeah. I am, I am really pleased.

Leo: That's really great. All right.

Steve: So thank you, Tim, for the Kick Ass Revelation of the Week.

Leo: And thank you, Steve Gibson, for yet another fantastic episode of Security Now!. We thank you for all your questions. If people have questions they'd like to submit, how do they go about doing that?

Steve: You go to GRC.com/feedback.

Leo: Okay.

Steve: And by all means, don't be shy. Also I have to say, if I go "doo-to-doo," then Elaine writes, "Steve makes trumpet-playing sound." It's like...

Leo: She doesn't know how to spell "doo-to-doo."

Steve: I saw that in the transcript I was looking at. And I thought, okay, I gotta go [trumpeting sound]. There she does it again.

Leo: I love Elaine. We should have some fun with Elaine. Meow. Mrow. Ruff-ruff-ruff-ruff-ruff. We'll just have some fun with her, see what she writes. That's Elaine who does the great transcriptions, which you can find online at GRC.com. I know it's sometimes hard to follow everything, but the transcripts really make it easier. If you're one of those types of people that needs to read along as you listen, or even want to distribute it to friends or classmates, we encourage you to distribute the podcast. You know, as long as you do it for noncommercial purposes, please spread the word. We really appreciate it. And there are 16KB versions on the website, too, so people who don't have a lot of bandwidth can get a copy. Not as crystal-clear sounding. But they can get a copy of Security Now! that way. It's all at GRC.com, along with all of Steve's freebies and his bread-and-butter program, SpinRite, the world's finest hard drive recovery and maintenance utility. GRC.com. Steve, have a great, safe week. And we will talk again next week on Security Now!.

Steve: Sounds great, Leo. Thanks very much.