# SECURITY NOW!

**Transcript of Episode #167**

## Listener Feedback Q&A #52

**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-167.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-167-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 167 for October 23, 2008: Listener Feedback #52. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show where we cover all the latest security news and give you some inside understanding about what it means and what it is. There he is, ladies and gentlemen, Steve Gibson in his beautiful lair. It looks like a library. For those of you who watch on video, you'll see Steve is surrounded by books. Are those all programming books, Steve?

**Steve Gibson:** I love books. Yeah, there's some software, but largely programming books. I have an unopened copy of Windows 3.1. And...

**Leo:** Why didn't you open it?

**Steve:** There's a bottle of Cabernet from Microsoft that was give to me, it's etched, a bottle that I will never open, sort of a collector's item, and other random little paraphernalia from long-gone days.

**Leo:** You know, it's funny, because if I turn the camera the other way, what I'm looking at is a very similar bookshelf filled with books. So, and many of them are programming books, as well, and computer stuff. And I even have, thanks to Paul Thurrott, who sent it to me, a copy of Lotus Symphony for the Macintosh. Yeah, look at that. There's the wine. I see it right on the top there.

**Steve:** Yeah.

**Leo:** Lotus Symphony for the Macintosh. And it's on floppies.

**Steve:** Yes, yes. Yes, yes. When you could actually fit something useful on a floppy.

**Leo:** Well, there's, like, 40 floppies. You know, and now I'm looking, it really is mind-boggling. I just got a 32GB SD card for my camera from Kingston. Thirty, you know, we're so nowadays cavalier...

**Steve:** Now, you mean CF or SD?

**Leo:** SD card.

**Steve:** Wow.

**Leo:** We're so cavalier about...

**Steve:** Gigs.

**Leo:** ...gigs. My new G1 phone has a little micro SD. I mean, that's tiny, a size smaller than my pinky fingernail. And that's 8GB. Gigs mean nothing anymore. You know? When you and I were coming up...

**Steve:** Oh, in fact, a friend of mine sent me a very cool thing he found on ThinkGeek. It's a dock cradle, but it's for docking an SATA drive. So it's got a large port. And literally you just - you plant - because SATA drives are hot-swappable, you literally just plant the drive into this thing, and it plugs it in. And it's got both a USB 2 and an eSATA interface so you can do full high-performance drive interaction. So, you know, here's hard drives have come down in price to that level where it's like, oh, just plug an eSATA drive in here and use it.

**Leo:** Steve, I have six of those. And I buy 750GB drives for under a hundred bucks by the dozen. And then I pop it in, and that's what we record all our video on. I pop it in. At the end of the week I pop it out. You know, Tony's got one on his machine.

Dane's got one on his machine. Even our office manager has one on her machine.

**Steve:** Oh, you mean the eSATA docks?

**Leo:** Yeah, and anybody can just...

**Steve:** Oh, cool.

**Leo:** Because we just - it's easy to put eSATA on these new machines because it's just putting an external port on there. And any of these drives, they're just barebones drives. I've got them on my shelf now, starting to line up. Anybody can come in, what do we need? Oh, yeah, that's on Drive 4. They'll pop it in. It's amazing. Now, I just - Dane just handed me - only people on video are going to see this. This is 16KB of memory for a Data General Nova machine. That is, it is the size - it's framed. It's the size of a, well, a framed picture, you know, like 12x12 picture. Sixteen, not megabytes, not gigabytes, kilobytes of memory for a Data General Nova. So that's 40 years ago, 30 years ago. Unbelievable. We have come so far.

**Steve:** I programmed a Data General.

**Leo:** Did you?

**Steve:** Yup, the Nova and the SuperNOVA. Those were beautiful machines.

**Leo:** This was a minicomputer; right?

**Steve:** Yeah. Minicomputer, had big 19" boards that slid out. Like it was 19" rackmount.

**Leo:** Well, that's what this must be, then. This is 19 inches.

**Steve:** Yeah. And so that was a board of core, probably, core memory.

**Leo:** It's core memory, there it is, yeah. And probably hand wire wrapped. I mean, I don't think this is stamped out. This looks like all the solders are by hand, and the wires are visible, I mean, it's just amazing what's changed. Just amazing. We live in interesting times. So what are we going to talk about today?

**Steve:** Well, today, Episode 167 is a Q&A, our 52nd Q&A, questions and answers from our listeners.

**Leo:** That's hard to believe, too.

**Steve:** Yeah.

**Leo:** Wow, all right. That'll be fun.

**Steve:** We've got some good ones. We've got a couple long ones and some short ones. And so I think it's a nice lineup of questions.

**Leo:** All right, Steve. Any updates from last week's episode, or...

**Steve:** Well, it's been quiet on the security front. There is another Mac update.

**Leo:** I did get one just last night, yeah.

**Steve:** Yup, that one. It was updating, once again, a bunch of security vulnerabilities in third-party components that are bundled in with the Mac OS, various open source UNIX gizmos. But also there were some remote code execution vulnerabilities. So I wanted to let our Mac people know. I mean, last week when we recorded this I had a major update. This one was small. This was, I think, 31MB, so not nearly as big. But you want to just check for software updates, and Mac users will find something there. Also several of our listeners commented on my mentioning about application frameworks and the CSRF topic from last week, the cross-site request forgery. And they wanted to mention that Ruby on Rails does have built-in CSRF spoof-defeating logic, and it's enabled by default, and it's been there since v2.0.

**Leo:** Very interesting. Rails is used on a lot of websites. It's a very quick prototyping system, very easy to use, and a lot of Web 2.0 sites use it. So that's good news.

**Steve:** Right, right. And so this problem was recognized, and forms automatically include a pseudorandom token that must be returned when the form is submitted. And just doing that prevents the blind request forgery that we were talking about last week.

**Leo:** Excellent.

**Steve:** So I wanted to acknowledge that anybody who is, I mean, it's even a reason to use Ruby on Rails, in fact. If you are up in the air about what framework you're choosing, all other things being considered, this is a good thing to have, just to keep anyone from messing around with your site.

**Leo:** I'd be willing to guess, before you get flooded by emails from everybody else, that other frameworks, if they don't already do that, will do that. It's an easy thing to implement.

**Steve:** Right. Right. And then I had one fun SpinRite anecdote from someone named - actually a listener of ours, Calvin. And I ran across this when I was going through the mail bag for Q&A, so I know that he's from Saint John, New Brunswick. And the subject was "Save the Last Dance for SpinRite." And he said, "Hi, Steve and Leo. I have always been the tech guy for a friend of mine living in Alberta, mainly because I lived only about four blocks away for the longest time. However, about six months ago I moved to the opposite end of the country. Well, recently I convinced my friend to buy a MacBook as her old laptop was starting to fail. She transferred her music, which she uses for youth dances at the Boys and Girls Club, onto an external hard drive to transfer over." So she apparently put it from whatever laptop she was using onto the external drive, and then she was going to plug that into her MacBook. "This is when the emails started coming. When she plugged the external drive into the MacBook, she could hear a faint clicking sound."

**Leo:** Uh-oh.

**Steve:** "But the drive would never actually mount. I arranged for her to courier the drive out to me, and I set to work as I only had two weeks to get this figured out. I first tried plugging the drive into the USB port on my laptop. However, I encountered the same issue she had, just repeated clicking. That's when I took the external casing apart, that is, the case of the external hard drive. Luckily enough, it was a laptop SATA drive, so I plugged it into my laptop's drive bay and booted SpinRite. When I launched SpinRite, I was met with the ominous red warning screen saying that the drive was in danger of imminent failure." That's something that SpinRite is able to detect - I've stepped off of reading this for a minute just to tell our listeners that that's something that SpinRite is able to determine immediately by polling the S.M.A.R.T. interface on the drive and checking to see whether the drive thinks it's okay. So even the drive knew it had a problem, although unfortunately through the USB interface that information was not being communicated.

So continuing with Calvin's note, "With this in mind, I launched SpinRite at Level 2. After about 11 hours or so SpinRite finally finished its business, proudly displaying about 25 green Rs, meaning recovered data, showing all recovered sectors. I then booted to a Linux Live CD, mounted the drive, and copied the files to a USB stick to send back to my friend. Needless to say, the dance is saved, sparing my friend hours of CD ripping and recovery of songs for which she only had digital copies. Thank you so much for your amazing product and an incredibly informative netcast. Keeping my propeller beanie wound up."

**Leo:** You know, she's, or he's very - she's very lucky to have him because he's obviously a major geek, smart enough to do things like use a Linux Live CD to recover the files and things.

**Steve:** Right.

**Leo:** Obviously she has a good friend. That's a nice story. Hey, before we get to our questions, I have one story I wanted to mention. You don't - you're not a baseball fan, are you.

**Steve:** A what?

**Leo:** Baseball? You ever hear of that? It's this game, these guys, grown men, they go out with a stick, and they whack a ball around. It's really fun. The World Series is coming up in just a little bit. But the American League championship series was a very exciting playoff between the Red Sox and the Tampa Bay Rays. And Red Sox had come back in Game 4, and in Game 6 they won again. And it was very, you know, they put it all the way to Game 7, the final and deciding game to see who wins the pennant and goes on to the World Series.

I tune in TBS, and they're in reruns. They have some technical difficulty. The first two innings of the game they miss. They miss. They can't - and I go on Twitter, and people are howling. I mean, this is a big deal. But they're running some crap rerun. And I'm watching it because I figure, well, they're going to get it back pretty soon, and I want to see the game, this exciting game. And on comes - I don't remember the name of the company. And even if I did, I wouldn't give them a plug. But on comes an ad for a company, I'm sure this isn't a very good product. They claim to - you run this product on Windows, and it speeds up Windows and gets everything going faster, right, and they show - it's kind of a funny ad because it's mostly Macintoshes with Windows screens CG'd in showing Blue Screens of Death, and then they run the software, oh, it works. And so at the end of the ad they say go to our website now and download this software.

Well, I had to go; right? But I think what they weren't planning on is running in Game 7 of the American League championship series. Because I go to the website, nothing. They DDoS'd themselves with this ad. And they did not come up for another half hour. All that potential revenue gone, just shot. People who couldn't get on the website.

**Steve:** Come to think of it, that had to have been an expensive commercial to run, too.

**Leo:** Well, I think they were getting it for nothing because they thought they bought the Steve Harvey Comedy Show. But they're going crazy in Atlanta, saying quick, throw something on. I know, I've been there. Throw something on. We've got nothing from the game. What are we going to do? And so they're running whatever they got, including this ad that I'm sure these guys never expected to be on in a major ball game. Just a word of warning, you know, if you're advertising a product that speeds up your computer access on the Internet, make sure you have enough web server capacity before you get the ad on the air. Oh, sad.

All right, Mr. Steve Gibson. It is time, my friend, to delve into the questions, the myriad questions from our listeners. They're dying for your answer. Are you ready, sir?

**Steve:** I'm ready.

**Leo:** Like Carnac. Like Carnac the Magnificent. These questions have been sitting on Funk & Wagnall's porch in a mayonnaise jar for three weeks. Listeners Colin Williams - oh, everybody wanted to know this one - Dave Mackenzie, Warren Matthews, Canuck Geek, Dullin Panuru, Rene, Rick E., Igor David Schneider, Pete Lisanti, and many others ask this question. And I'm really glad they did because add Leo Laporte to this list. We've seen this from ElcomSoft, the report that WPA and WPA2 WiFi may no longer be secure. What's the story, Steve?

**Steve:** Totally bogus report.

**Leo:** Yes, that's what I said.

**Steve:** Yes.

**Leo:** I saw this news story, and I knew that we would get these questions.

[Talking simultaneously]

**Leo:** And it just, in fact, pisses me off, frankly.

**Steve:** Yeah. It was really, really, really bad. Those are just the names of the first few people, starting on October 10, when this report came out. Unfortunately, of course, it got picked up by Slashdot. And most irresponsibly, the well-known SC magazine, a good security magazine, I remember picking up a copy when I was at the RSA convention, they carried a story which really inflamed this whole issue.

Okay, so basically what ElcomSoft has come up with is not unexpected. They're using the extremely high-power integer engine inherent in state-of-the-art GPUs, the graphics processing units in NVIDIA display cards. They're using those to accelerate basically brute-force encryption attacks. And they give many examples in their flyer of different sorts of passwords that can be cracked. And what's most telling is that it's ElcomSoft themselves are only billing this, for example, as a high-powered way to maybe check for weak passwords in a corporate environment. They're only claiming that two of these cards, two NVIDIA cards and their software in a fast machine would break WiFi encryption up to a hundred times faster.

Okay, I don't doubt that at all. Except that it's already, like, 10^38 times harder to do anything with a good, random password. Now, they don't explain whether they're just brute-forcing the 128-bit encryption, or whether they're brute-forcing ASCII, which is then hashed using the WPA scheme into 128-bit key. So it's not exactly clear what it is they're doing. But the problem is that this SC magazine story which got picked up, and then which of course The Register in the U.K. picked up, and then Slashdot did, the guy who wrote the SC magazine story said, oh, this is the end of WiFi security as we know it.

**Leo:** You know, and the other thing that pissed me off is instead of saying a hundred times faster, he said 10,000 percent faster.

**Steve:** Well, yes. And the way you...

**Leo:** Moron.

**Steve:** The way you could theoretically get that, because this is also a distributed attack tool, if you had 10,000 computers, each with two of these in a huge network, each of them a hundred times faster than if they were just doing it in software alone, okay, yeah. So then you could get it up to 10,000 percent faster. But even that doesn't matter because, you know, if you have followed our advice and have a strong, really robust WPA key, which you should have in any event, then this doesn't help you at all. I mean, this...

**Leo:** In other words, if you use your special passwords program to generate a 64-character random string, you're still, you know, so what if it's a hundred times faster. It's not even two orders of magnitude compared to infinity.

**Steve:** So now you're down to several tens of billions of millennia rather than 10,000 several tens of billions of millennia.

**Leo:** I was really shocked at - I can understand the mainstream press getting sucked in by this. I was really shocked that people at Slashdot and SC mag, they should know better.

**Steve:** Yeah. Well, especially when even the original report from ElcomSoft makes no claims about its ability to crack WiFi. I mean, I read the whole press release. They're saying a hundred times faster. It's like, okay, I believe that. But that doesn't help you. It doesn't in any way weaken WPA because it was already strong enough to withstand a factor of a hundred gain in cracking. I mean, and besides, a hundred is not that much. If WPA weren't strong enough to withstand a hundredfold increase, it wouldn't be strong enough to withstand a onefold increase. Because, again, a hundred isn't a huge number.

**Leo:** No. You know, that's I think why they couched it in percent, which makes it sound like it's so much more. But even then it's not a significant - I'm really - I guess I've been doing this show long enough, I've learned a thing or two. And I debunked - I had the same debunking reaction on the radio show. It's just - but of course it scares the heck out of people.

**Steve:** Yeah. Well, because we have seen situations. There was a report recently where the encryption scheme used for the remote car keys had been cracked. And in fact it has been. And it was kept secret for two decades. And it leaked out, and some cryptographers got a hold of it, and it turns out that under certain circumstances it's possible, if you receive several successive outputs, to determine the master key in the keys we use for unlocking our cars and garage door openers and things. But even then, the only good attack is a so-called "side channel attack" that we've talked about before where you measure the power being consumed by the transmitter. Well, okay, how do you measure the power being consumed by the transmitter someone's holding in their hand, you know, across the street? So just receiving the radio, it turns out, is still very secure. And so people get these stories mixed up because they're technical, and we end up upsetting people needlessly.

**Leo:** Right, right. You know, one thing that it does raise, though, is this issue of you could sit out on the curb with a wireless connection and collect a lot of data and then go home and analyze it. You're not doing this on the curb. And I guess - is that right?

**Steve:** Well, yes. The ElcomSoft or any - and we've talked about...

**Leo:** Any brute force.

**Steve:** We've talked about the only, as far as we know, the only vulnerability in WPA which has now been, I mean, seriously reviewed by the world's top cryptographers, the only weakness we know of is a brute-force attack where - and you only need a few packets. You don't need much. Although if you were going to - if you wanted to crack the security, you would be wanting to suck in a bunch. But then you would only analyze a few.

**Leo:** So you'd say maybe take 10 minutes worth of data? Would that be enough?

**Steve:** Half a second worth of data.

**Leo:** Okay.

**Steve:** Would be enough. Because the goal is to find a key by trying them at random that happens to decrypt a couple packets.

**Leo:** But it does - it is a form of vulnerability because unlike, you know, if you want to brute force, for instance, SSH to break into my server, you can't really automate that. It slows you down. You can only do one try every few seconds. But this does at least mean you can get a batch of data, take it home, and you can throw a lot of hardware at it and hammer it.

**Steve:** And when you're not playing whatever your videogame of choice is...

**Leo:** World of Warcraft, yeah.

**Steve:** World of Warcraft. You can idle your computer trying to crack some WiFi.

**Leo:** So you can do it at your leisure, which is a little different than a lot of brute force cracking.

**Steve:** Well, for example, the WEP crack, because of the vulnerabilities in WEP, the prior generation encryption, WEP, anyone can crack that in a minute.

**Leo:** Sitting on the curb, yeah, yeah.

**Steve:** So, you know, that's just broken now. But WPA is still safe as long as you're immune to brute force attacks. As long as you use a really good key. So again, GRC.com/passwords.

**Leo:** Breathe safe.

**Steve:** And we will give you a good, strong key.

**Leo:** Nothing to fear. Mike in Toronto, Canada needs a public VPN service. We get this question fairly frequently, as well: I hope you're reading this, Steve. I'm looking for - yes, he is. I'm looking for a VPN service for surfing the web. The problem is I tried Strong VPN, but the service is very poor. Could you tell me or ask your readers if there's any good VPN service in the USA? I'm scared to get another one, fearing getting ripped off again.

**Steve:** And this was an easy one. I know of, and you and I both used, and while I was using it, you know, I had a trial subscription that the owner of the service gave both of us, Leo, and that was HotSpotVPN.

**Leo:** Yup. And it's 10 bucks a month, 8.88. It's very affordable.

**Steve:** Yup. And it works. I mean, their servers are strong. It's a standard. They just use OpenVPN. So when you download the client from them, this installs OpenVPN into, for example, your laptop, with it all preconfigured and ready to go. And so it's simple to use. And while I was using it I was very impressed with it. I had no trouble with it.

**Leo:** And there are others. But, yeah, I think it's a very good one that I would highly recommend. You do get some slowdown by using a VPN service. I mean, it's not, you know, you have to go through their server; right?

**Steve:** Right, yes. And you also need to trust them because, remember, just like TOR, where you're using essentially other servers out of which your traffic is being emitted, there's inherently a traffic concentrating aspect to that. So, you know, somebody could be looking at all of the traffic coming in and out of the HotSpotVPN network figuring that maybe it's higher value because somebody wants to encrypt what they're doing in their local connection. So there is some traffic concentration consequence of that. But, you know, for email and web surfing and so forth, it's certainly safe.

**Leo:** And I wouldn't dream of doing anything that you needed to be safe in a hotel, especially a hotel.

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

**Leo:** In a hotspot, I mean, these things are risky. So you do need something like this. Bruce Kincheloe in Denver, Colorado, USA, says he just wants to plug in and turn on and tune in and drop out. No, no, just plug in. Hi, Steve. Thanks to you and Leo for the great work you do with Security Now!. I love the show. My question is about power line networking. These devices are newly available. From a security point of view, is the encryption used sufficient to prevent eavesdropping by others? You know, I haven't tried this. They kept foisting it on us years ago. And I think now the new power line networking actually is pretty reliable, pretty fast.

**Steve:** And the good news is, it is very secure.

**Leo:** Oh, that's neat. So they encrypt the data.

**Steve:** And they do a - well, yes. And we've seen keyboards that said they encrypt the data, and it turns out they're XORing an eight-bit byte with it.

**Leo:** I just saw a hack of a wired keyboard from 20 feet away.

**Steve:** The good news is I did a check. All of these come from the same company. And this company understands security. They understand that, if they're sticking your network on your wires, and for example you're in an apartment building, so that your wires are the same as your neighbors' wires, they'd better get the encryption right. And they look like they did a, I mean, I haven't done an absolute full security analysis. But in order to find an answer to the question, I did look around. I took a look at the security and the technology, and they were using all the right words. And it really looked like they understood they had to get this right, and they did.

**Leo:** Good. That's excellent news.

**Steve:** So I would tell Bruce, yes, it's safe to use power line networking.

**Leo:** Very good. Lance Reichert in Greene, New York wonders what his corporate security people are meaning when they say, well, let me read it to you: A quiz circulated by my company's security department says filling out online forms like web questionnaires or registrations to receive work-related magazines, for instance, when you're doing it from work, is a serious risk. Quote, "Every time you log onto a web page you create a scenario hackers could potentially use to crack your employer's network." Huh? Every time? If this is so, how is anyone going to safely conduct any business at all on the web? Are they talking about avoiding shady offers, or are they talking about exploits through well-known, well-managed sites such as EE Times Online?

**Steve:** I thought that was a neat question because you can sort of see a little bit of FUD spreading. I would say that his particular corporate security people are a little over-concerned, though it's probably a good thing from a standpoint of educating the employees of the company to sort of give them a sense of things you do on the 'Net are not completely without risk. And I think he summed it up nicely. It is, you know, these are what we've talked about. We've talked about how the number one attack mode now is going to bad websites with browsers containing vulnerabilities. And I guess that's being redundant to say "browsers containing vulnerabilities." They all do, apparently, from everything we've seen.

**Leo:** Some more than others, but yeah.

**Steve:** Well, and vulnerabilities known or not yet known...

**Leo:** Right, that's the problem, you can't guarantee that...

**Steve:** ...discovered or not yet discovered.

**Leo:** Yeah, right.

**Steve:** And so the problem is that some bad websites can do this. Now, we've also seen situations - and he refers to EE Times Online. It might very well be that the EE Times Online webmaster and company are above reproach, their integrity, and would never deliberately hurt anybody. But their server could have a vulnerability that allows people to change their web pages and put malicious code on them. And we also see that happening all the time. So you can't just trust a highly credible site not to do something bad to you because highly credible sites are being infected because, while they may be credible, they're not keeping their own security up as much as they should. You know, they might have a framework which is using SQL database on the back end in order to generate their web pages and have an exposed SQL port with a vulnerability that allows somebody to get in and take them over. So, and there are - we've talked about various types of exploits of this nature. So it's true that the web is not completely safe. I sort of think that the corporate IT people are maybe making a little more of this than they should. But it's certainly something to keep in mind.

**Leo:** Yeah, I mean, yeah, I guess it is a good thing to say, you know, be careful out there.

**Steve:** Yes.

**Leo:** Don't order EE Times - well, you're right, you can't assume even EE Times would be safe. I mean, so what do you do? Because he has the point that it kind of makes the web kind of useless if you can't fill out forms.

**Steve:** Well, you turn off scripting, Leo.

**Leo:** Ah, yes.

**Steve:** Sorry about that.

**Leo:** Well, you know what, I'm coming more and more on your side on this one because it really - it seems to be the only thing to do that secures you against most of these exploits. And something like NoScript for Firefox makes it very easy. I mean, you just, you know, when you get to a site you want to - the problem is, okay, now you go to the EE Times site. And I guarantee you they use JavaScript in some context. And you want to use the site. You're going to turn it on. But now you're vulnerable to an exploit they may not have known about in the form.

**Steve:** Right.

**Leo:** So you're still kind of stuck.

**Steve:** We will be talking soon, in fact we're going to have the author soon of Sandboxie because...

**Leo:** Which is a great program.

**Steve:** Yes, a large number of the people who hang out in GRC's newsgroups are, I mean, they're using Sandboxie. They love it because it sort of is a lightweight sandbox. And I've had some dialogue with the author, and I've just been waiting for a window of opportunity to get him on and talk about it because it is a great program, and it does have the advantage of putting some protection around your browser to keep your browser from being able to do anything to your system that you don't want it to. And so the heavyweight approach is to use a full VM, a full Virtual Machine system like Parallels or VMware or...

**Leo:** But they raise this interesting point. You're on the corporate network now. Even if you're using a virtual machine, can't something bad spread through the network?

**Steve:** Yeah, um...

**Leo:** You really want to isolate it from the network, too.

**Steve:** And of course you can't isolate a browser from the network because...

**Leo:** You can't.

**Steve:** ...it's got to be on the network to browse.

**Leo:** We're screwed, basically.

**Steve:** Yeah. It's not good.

**Leo:** It's not good. You just, what, do you pray? You just hope. You say okay and just...

**Steve:** I think all you can do is be as aware as you can. You know, as I'm reading email from our listeners, the overriding sort of background theme is, you know, listening to this podcast has raised their level of awareness. They're more aware of these things. And it's changed their habits. You know, we don't want people to just disconnect from the 'Net and go sit under a tree. We don't want to keep them from doing the work they have to do. But there are things you can do like considering trying Firefox and NoScript and seeing how that works for you, and knowing that you really do have more protection than if you're just using IE with scripting turned on.

**Leo:** And it's important, even though there is no perfect protection, it is important to remember that some protection is better than no protection at all. You shouldn't just throw up your hands and say, ah we're screwed, and give it up.

**Steve:** I so often think, as I'm using my key in my front door, what a ridiculously poor security a lock and key are. But it's better than leaving your door unlocked. It certainly won't keep anyone from getting in if they want to. But again, some is better than none.

**Leo:** Lance - oh, no, that was Lance. Matt Ludlam in Weybridge, London has a few questions about stressing his socks. Got Sockstress? Steve, love the show, the only one I listen to and learn from every week. Okay. One thought on the most recent Q&A, you mentioned that the latest versions of Microsoft's web server IIS have been hardened against some forms of TCP attack. My understanding is an application like IIS would pass information to the TCP stack, and the TCP stack would then manage the lower level communication. Following on from there, if Microsoft hardened IIS, in effect they'd be hardening the entire TCP stack. Ergo, we are all safe. Are we? Obviously my above conjecture must be wrong, but where? Does IIS have its own TCP stack in users mode? Does Sockstress pick up on areas that Microsoft has not hardened? Your thoughts, as always, eagerly anticipated. So he's saying basically

Microsoft says we've fixed IIS, we've hardened. And he's saying, but wait a minute, isn't the problem at TCP?

**Steve:** Yeah. I liked the question because I didn't really explain that very well when I talked about it before, and a number of our listeners had written with similar questions. The relationship between the TCP stack and the applications that use it is such that the stack is sort of a service that the application uses. So a web server like IIS says I want to accept connections coming in on port 80. But I'm not wanting to reinvent the wheel. TCP is a complicated protocol. So I want the operating system that I, IIS, am running on, to deal with all the messy details. I want to accept connections on port 80. I want to be notified when someone connects. I want to receive their data. I want to send them data. But I don't want to have to worry about the bandwidth delay product. I don't want to worry about packet loss in the connection. I don't want to be - I just don't want to deal with any of those details. I want to be told when they connect, told when they disconnect, get their data, send them data.

And so the so-called "socks" interface, the socket interface that the operating system creates is an abstraction of all of that, everything else that the TCP protocol deals with. So one problem, for example, that I discussed when we were initially talking about sock stress would be the idea of a client creating a connection and then stalling the connection by saying that it had no available buffer space at its end to receive any data. So the server would sit there and patiently wait for some buffer space to become available. Meanwhile, that client could be creating connection after connection after connection doing the same thing, building up this large number of stalled connections.

So an application like IIS, but one that wasn't aware that this could be considered abusive, would sit there and go, oh, look at all the people that want to connect to me, isn't that nice. I wonder - I wish I could send them something, but none of them are willing to receive any data. Doot do doot do doot do doo. And it would sort of sit there waiting until somebody received data. And before that happened, something would collapse. The OS would run out of space. The stack would collapse. The application wouldn't be able to hold any more connections. Something would just, you know, go wonky. So a smarter application, a hardened application, not necessarily the stack itself, but the application, could be told, okay, look. We're not going to put up with this. If lots of people are connecting, but no one is willing to have us send them any data, we decide that's not okay. And so after 15 seconds of this, which is really - it should never happen for that length of time. Then we just say, okay, sorry, you had your chance, and we hang up. Because the application can disconnect in the same way that the client can disconnect.

So the idea is that the service using the stack, which inherently kind of creates the vulnerability by telling the stack to open the port and please accept connections, the service could be hardened against these kinds of abuses, where it inspects the - like it inspects what's going on on those connections and becomes intolerant of behavior that technically is okay, but unfortunately in the 21st century of the Internet can more often than not be indicative of abuse. And so it says, eh, you've had 15 seconds, you're still not getting any buffer space. Look, so don't call back because, if I can't send you anything, what's the point of hooking up to me anyway? And so just hang up.

**Leo:** I don't trust you. I don't like you anymore.

**Steve:** And so that's a much better thorough description than I gave last time. But it does also tell you that, while you might have IIS running on a server that is protecting itself, you might also have an SMTP, an email server running there, not protecting itself. So while port 80 might, on a given IP address, on a given server, might be invulnerable to a Sockstress attack, the attack could simply switch over to port 25, where SMTP is running, and you might have a non-stress proof email server which you could do the same thing to and bring things down. So it is a per-application solution unless the stack itself were hardened. So either the stack could be hardened, TCP stack - and doing that would protect all the applications on the system.

But it might be that there are some applications that would want to tolerate that kind of behavior. For example, you know, one of the things that IIS does, as I mentioned, is if it sees a connection that's been held open for a long time and nothing going on, it'll close it. But TCP the protocol deliberately allows that kind of connection. That is, TCP, you don't have to have any packets go by for weeks. And then you can send something. And as long as both ends still agree that there's a connection, that packet, that data will go across the 'Net and be received. So TCP the protocol allows for infinitely long connections with no data transit. By definition, some things want that. IIS can decide, or whatever hardened web server, I'm not an application where that makes any sense. We're going to shut those connections down. So you have to be careful if you harden the stack in a way that would break things that are making assumptions about TCP, and you're changing those assumptions.

**Leo:** All right. Makes perfect sense when you explain it that way.

**Steve:** There's a complete answer.

**Leo:** Yes, as usual. Sheldon Smith in Apple Valley, Minnesota wonders why Visa is not enough: Hi, Steve and Leo. Let's talk about Internet security and online shopping. The two of you frequently mention PayPal, but PayPal is tight with DoubleClick. And recently you mentioned Amazon is coming out with a competing online payment service. Google has one, too, as a matter of fact. My question to all this is, but why do I need something else? Visa already provides online security and, as you know, watches out for fraud so I don't have to. I already have a Visa card. In fact, both my credit and checking account and debit cards are associated with Visa. So why do I need anything but Visa? Why are Amazon, PayPal, and Google doing their own payment service? Even Amazon offers a Visa card.

By the way, I started back around Episode 7. I've listened to every episode so far. Steve, back when Leo first came up with the idea, who woulda thunk this funny little podcast would still be going strong after four years? Great job, guys. Well, thank you. That's very nice, Sheldon. I guess it's true. Why do we need other payment services?

**Steve:** Well, there are a number of reasons. First, I like the idea of insulating myself and my financial...

[Talking simultaneously]

**Leo:** ...credit card to a vendor.

**Steve:** Yes. Yes. But one thing that Sheldon doesn't mention is, it is a hassle losing your credit card. And when I say "losing," I mean losing it onto the 'Net. It's happened to me now three times, even though, you know, I'm Mr. Security Now!. I'm not giving my card out to random people that I don't have to. I will say, however, I'm giving it out much less often now that PayPal allows me to generate cards on the fly. I'm liking that and using that a lot more because it'll allow me to create a temporary card that is just there for one use, and then I shut it down. So in my experience what has always happened - and it happens that I'm a Visa card user. I don't know why I got onto Visa, but that's what I use. As I mentioned once on the show a few months ago, I got a call from them saying, hey, somebody's using your card in France. Is that anything that's authorized? And I said, eh, no. And so they said, okay, we didn't think so. Someone made a test purchase, which they denied, and then a big purchase. And that was the trip that tripped them up. And so I was protected. So that was really nice.

**Leo:** And I have to point out that's something that I don't think you get - the credit card companies do it by law because they're required to by law.

**Steve:** Yes.

**Leo:** I don't think PayPal, Google payment or Amazon payment has that same requirement. I know, in fact I know PayPal doesn't because I got defrauded. And unlike with a credit card, where you just - by law they have to stand behind you, PayPal I had to go through many hoops. And frankly, I think if I hadn't escalated it to the office of the president, I wouldn't have gotten my money back.

**Steve:** And for what it's worth I have heard that American Express is even more pro-consumer. American Express...

**Leo:** Yeah. Well, you pay for that, believe me.

**Steve:** Yeah, they don't even ask a question. They just give, you know, put the money back on your card.

**Leo:** So credit cards by law are, you know, the banking laws in this country require them to do that. And some do better than others. But I don't know, and maybe this is just a gap, and maybe the law will fix it at some point. But I don't think they have the same - you have the same kind of protection with these payment services. So that might be a reason not to use one.

**Steve:** Well, in my experience, I guess the point I wanted to make was that while, yes, you are protected from the financial consequence of losing your card, having it get loose on the 'Net, you are not protected from the hassle of changing the number. I've got a bunch of things, you know, Amazon knows my card number. I subscribe to the little toll road pod that deducts automatically from my card whenever the account runs low and a number of things that, last time I lost my card, had to have the number changed, it was like, oh, god, okay, now, what are all - and my cell phone billing goes to my card and all that kind of thing. So it really is annoying to have to change your credit card number. And going through an intermediary that either doesn't use, doesn't expose your card to the 'Net, or someone like PayPal that allows you to generate a pseudocard for the purpose of doing a single transaction, it prevents you from having that exposure.

**Leo:** I guess what I'd like to see is the same requirements put on these payment services. Now, here's a question. If I use that one-time-only Visa number that PayPal gives you, I presume now I'm using a Visa card that I'm protected. Right?

**Steve:** Actually it's MasterCard in the case of PayPal.

**Leo:** I would assume that that gives me now those protections because I'm using a PayPal credit card.

**Steve:** So let's see. So somebody else uses it again, it's not going to work.

**Leo:** Yeah, but I'm just saying the fraud protection. Here's the deal. When you buy something with PayPal, if you get defrauded, it's up to PayPal what they want to do about it. Not so with a credit card. If I use a PayPal credit card, I would presume, because now we're using MasterCard, that we are protected.

**Steve:** Yeah, I don't know.

**Leo:** That's a good question. Like to find that out. See, it's a tradeoff. And what I'd really like to see is the banking laws say, you payment services, you have the same requirements as a credit card has.

**Steve:** Yeah.

**Leo:** Let's see. Let's go to New Jersey. Paul Corr in Trenton, New Jersey was concerned and a bit confused about Skype quality and the need for port forwarding, which is something we do. We'll talk about it. I have a colleague in the U.K. We use Skype to talk to each other. I decided to research best practices. Skype has a security page. I see connections point-to-point are encrypted to guard against man-in-the-middle attacks - unless the man in the middle is Skype, but we'll talk about that some other time. I see connections - right. Important because it is a peer-to-peer network. I found a page on improving performance by using port forwarding, and I found my router setup details on PortForward.com. After reconfiguring my router I visited ShieldsUP! to test vulnerability and found it failed due to ping exposure. I reenabled "block anonymous requests" in the router admin screens, tested again. Now it passed. I will return to Skype's preference for using dynamic port assignment rather than the explicit high port I set following the article on performance.

So now I'm wondering what is a best-practice approach for Skype security? I did find the GRC page on NAT and saw that if one port forwards, it should be on an isolated machine. Any light you and Leo can shed would be appreciated. I found Security Now! a while ago and returned to the archive of earlier podcasts until I caught up. Thanks again. Well, thank you, Paul. I'll tell you what I do, and you tell me if it's safe, Steve. I have a dedicated port for Skype, 22222, something like that. And I port forward from my router to that particular machine, 22222. So that is the only machine that incoming connections on that port can be accepted. And that gives us, I think, better Skype results.

**Steve:** Yeah, there are a number of things going on here that are interesting and non-obvious that Paul's question brings up. First of all, I'm not sure what he did on port forward. But he says that by reenabling "block anonymous requests" he was then able to get a true stealth pass on ShieldsUP!. Port forwarding itself should not cause a ShieldsUP! failure, especially on a high-numbered port. So what he may have done - there are two ways to enable unsolicited incoming traffic through a router. There is port forwarding, which you mentioned, Leo, where you specify by - explicitly say I want this port number whatever it is to be forwarded to a specific IP behind the router, to a machine on an IP behind the router. And then only traffic bound for that port will go to that machine.

The alternative means is something called a DMZ, the so-called demilitarized zone, which is what DMZ stands for. And that's an entirely different approach. That says allow anything unsolicited to be sent to a specific machine. Now, if you do that, ShieldsUP! will go nuts. I mean, it'll be lighting up in red because...

**Leo:** Yeah, DMZ is a pretty big cannon to use against a little gnat of a problem.

**Steve:** Yes, if you'll pardon the pun.

**Leo:** You're opening everything.

**Steve:** Yes. Now, I should also mention, though, stepping back from both of these, that the only time that this is necessary, that any DMZ or port forwarding is necessary to improve performance or call quality, is in the event that both of the endpoints are behind NAT-hostile routers. That is, it's more the case these days that port forwarding won't buy you anything. You and I do it, Leo, because we absolutely positively insist on having a really good connection between us. It happens that my NAT box is NAT hostile. It is not something that Skype is able to penetrate.

Remember that Skype came from the - Skype was developed by the guys who did Gnutella. And one of the Gnutella technologies was very good NAT traversal where they came up with the idea of how Skype Central could talk to both endpoints and arrange a direct connection between them. Well, that requires that one or the other of the NAT routers be NAT traversal friendly, which means it'd be predictable in the way it works. Mine isn't, so I had no choice but to statically map a port through my router. So what I would tell Paul is that one thing you can do, with no port forwarding established, is to use a program like Wireshark, a packet-capturing program, which is actually pretty easy to use. It's a nice program. It installs cleanly. And while you're talking to your friend in the U.K., take a look at the packet flow and see whether the UDP packets, which will be streaming out of your system, are going to his IP, that is, the IP that he currently has for his router or his Internet connection. So that's a robust way of determining whether there's any relaying going on.

The reason performance and call quality drops in some cases is that if Skype is unable to establish a direct point-to-point connection, it will use somebody else's machine, who knows who, somebody who is out on the 'Net, who is not behind a firewall. It will actually relay traffic through a so-called Skype supernode in order to still allow that connection to be connected. One of the ways that Google Talk differs is that it doesn't use its customers' machines as supernodes if it can't establish a NAT traversal, a direct link between the two endpoints. It will do the traffic forwarding on behalf of that connection.

So it's not the case that you ever gain - that you necessarily gain anything from doing port forwarding. But oftentimes you can. And if you care about higher quality, it does make sense to do that. You do not need to use this DMZ mode, which as you said, Leo, is really - it's easy to turn it on, but you're opening yourself up to lots of security problems because essentially it's like putting that machine right out on the Internet. Unsolicited traffic can all get to it. So that's the case where you really want to make sure that machine is isolated. But again, you don't need to do it. All you need to do is route a single port through to Skype. And then you tell Skype in the UI which port you have sent to it. And that will cause it to then route the traffic in to you. And, also, only one of you really needs to do that. Because, if one does it, then the other person is always able to initiate a connection out through their NAT, no matter how hostile their NAT may be, in through your forwarded port to your machine.

**Leo:** I find it really - maybe it's voodoo. But it seems to make a difference.

**Steve:** Oh, it's a good thing. It's better.

**Leo:** I mean, we probably, because we have routers, we're never going to be a supernode or use supernodes; right?

**Steve:** No, that's the other nice thing is, if you were to DMZ your machine, you would be exposing it to carrying Skype traffic from other customers. But if you use port forwarding, then you're not able to accept supernode traffic.

**Leo:** That's very interesting. On we go. More questions for you, sir. Hi, Steve, says David Greenland in Perth, Western Australia. I have just found out that my ISP, Telstra, is blocking port 25. They claim this will help eliminate spam through the port. I need to know how me using port 25 on my mail server affects Telstra. They claim that to overcome this issue I need to register and pay $10 a month for a static IP address. Well, $10 a month may not seem like much to U.S. Internet users with their 25GB limits - ha ha. It's actually 250GB. It is an exorbitant amount since I already pay $99 a month for a mere 25GB which by the way is upload and download combined.

Is there any way I could change my SMTP port to still send mail from my mail server whilst using my dynamic IP address? I have this through dnsExit, which periodically an application on my server checks my ADSL IP address and updates my DNS records to suit. This works great and is absolutely free. Thanks for any help you may be able to offer. I enjoy the netcast, though much of it is beyond me. Keep up the good work. It won't be beyond you for long if you keep listening, I promise.

**Steve:** Okay, well, there are a couple of things going on here. So one of the things I've been expecting sort of for a long time, and I'm still expecting it, I can foresee the day where ISPs will simply drop incoming SYN packets, incoming TCP SYN packets at their border. It is so trivial to do. And what that immediately does is it prevents any of their customers from being a service, from serving over TCP, like the SMTP protocol, the Simple Mail Transfer Protocol on port 25 that David's talking about.

**Leo:** So I just want to make this clear. They're not talking about blocking port 25 to protect you from spam. They're talking about blocking port 25 so that you can't send spam, or some demon on your machine without your knowledge can't send spam. This is a big problem; right?

**Steve:** Well, now, that's the other question, is that there's - when he says they're blocking port 25, it's not clear whether they're blocking traffic inbound to port 25 or outbound to port 25. And both can be done. For example, many ISPs, in fact I think Cox does it, for example, there's a big cable modem company here in Southern California, many ISPs will block outgoing traffic to port 25 because what that prevents - because that prevents a client, their customers, from sending traffic to other people's SMTP servers. They allow you to only connect to their own ISP-provided SMTP server. For example, in the case of Cox I think it's west.smtp.cox.net. So you have to configure your email client to send your outgoing email there, and then they will forward it on. So that's blocking outbound traffic with a destination of port 25, which is for sending email to somebody else's - sending email out to the Internet.

Now, what David is describing is different, though. And it's further assured because they talk about registering and paying $10 a month to receive a static IP. What that's implying is that he would be - he'd have a fixed IP. And they would then allow incoming traffic to his port 25 for his email server. And he talks about running his own email server. So there normally what you do is of course you use your ISP's email server. So, you know, yourusername[@]yourISP.com. And so email traffic coming in to you goes to port 25 on your ISP's email server. And then your email client picks it up using POP protocol or IMAP protocol in order to obtain the email which is sitting on your ISP's email server.

What David is saying he wants to do, and he's using a dynamic DNS service in order to keep his own domain pointing at his own machine, even though its IP may move around, he wants to run his own email server for whatever reason. So, well, and for example, that way it could be david[@]davidgreenland.com, for example. He'd have his own domain that he's come up with. And so it's just sort of nice. He can, you know, he's got his own domain for his email. There might be, you know, family or special interest or who knows what it is. So in this case his ISP is saying, ah, we're blocking incoming email on port 25 unless you pay us money. We'll give you a static IP, and then you can run an email server. So, again, I'm - at this point that's a less common thing to do.

Now, we are seeing other ports blocked. We're typically now seeing, for example, as a consequence of the history of Windows vulnerabilities, we're seeing ports 135, 136, 137, 138, and 139 are blocked, and often 445, which are all the Windows filesharing ports. Those are often blocked coming into an ISP, which protects all their customers from the traditional bad Windows filesharing attacks. So again, I wouldn't be surprised if, in the fullness of time, we see ISPs just saying, eh, we're not going to let customers be services at all. You can be clients of the Internet. You cannot be services of the Internet. Unless you make special arrangements, like at this point Telstra is doing with port 25 for somebody who wants to run their own email server.

**Leo:** Right. All right. No, that makes sense. I think this isn't just Telstra. You're seeing this, as you said, most cable companies are now doing it. Comcast resisted this for a long time. And people said, look, if you just block port 25, you're going to eliminate a lot of the zombie spam that's coming out of your network. And they said, but if we do that we're going to get millions of dollars in tech support calls from people who suddenly whatever was set up isn't working. So they resisted it for a long time. They finally did it. And I think it probably does make a big difference in the amount of spam that's being sent by, not intentionally, but being sent by these zombies.

**Steve:** Well, that, again, that's outbound port 25.

**Leo:** That's outbound. Right.

**Steve:** Right. Because in order for people to send spam they need to send it to somebody's remote server. Now, you can certainly send spam to your own ISP. They'd get unhappy very quickly.

**Leo:** They'd know. They'd know. Exactly. What a lot of these zombie programs do is they actually put an outbound mail server on the PC, an SMTP server on the PC. And for it to work, it uses port 25. You could use any port; right?

**Steve:** Again, it uses outbound - it's sending...

**Leo:** Outbound port 25, yes.

**Steve:** Yeah, it's sending packets to somebody else's SMTP server which is available and open on the 'Net. And there are so-called "open relays" which are SMTP servers that will accept email from anyone to anyone.

**Leo:** Well, couldn't it just - what if I'm running an SMTP server on my machine, whether with my knowledge or not? Why would I need to go to another SMTP server? Wouldn't it just become an origination point for spam?

**Steve:** No. Well, if you were running an SMTP server on your machine, you would put your spam on your SMTP server. Then it would need to forward it to somebody else's

SMTP server in order to deliver that spam.

**Leo:** Oh, I see, as part of the process.

**Steve:** Right.

**Leo:** Right, yeah, I get it.

**Steve:** So in that case it would not be using probably an open relay. It would literally, for example, if you had spam bound for AOL...

**Leo:** It would just go right to AOL, and AOL's going to accept it and say it's...

**Steve:** It would look up, yes, it would look up the so-called "MX records," the mail exchange records, for the AOL domain. It would give it a whole list of IPs of AOL's SMTP servers. It would then - those would be listening on port 25. It would then connect to one of them on port 25 and start sending garbage to it. But in every case that would mean that traffic would be egressing from the ISP bound for port 25, which the ISP - and that's what ISPs have blocked.

**Leo:** That's what they don't want, yeah.

**Steve:** Right, yes, exactly. There is no reason that their customers should need to be directly connecting to foreign SMTP servers. Their customers should connect to their SMTP server, and then their server will forward it out to AOL, for example, in the...

**Leo:** But that's what David's doing, he's running his own SMTP server.

**Steve:** Well, no. He's receiving on port 25, which is different than sending to port 25. So he's running his own SMTP server because he wants to support his own email domain, and so allow people to send email to davidgreenway.com.

**Leo:** Oh, okay. Well, because there are people who run SMTP servers for outbound mail purposes. You're...

**Steve:** Yes.

**Leo:** I just thought that that may be what he was doing.

**Steve:** Ah, okay. But if he were, then he wouldn't need - he wouldn't go through the dynamic DNS and all that.

**Leo:** Ah, you're right, that whole point of that is so that you can get inbound stuff. You're absolutely right. Yeah, I get it. Yeah, I get it. I love this idea of blocking SYN packets.

**Steve:** Well, it's simple. It is so trivial. It's one command given to a router, essentially. And...

**Leo:** It would eliminate all of this stuff.

**Steve:** Yes. It ends all incoming connections.

**Leo:** What would be the negative?

**Steve:** All kinds of things would break.

**Leo:** Things like remote access, things like that.

**Steve:** Well, and for example, I believe that Skype uses TCP connections for its persistent connections. I know that Hamachi does. And so Skype uses UDP, as does Hamachi, for its bulk data transit. But TCP is still often used. On the other hand, those are not incoming connections. Those are outgoing connections. Those are clients connecting to the Hamachi server or clients connecting to Skype. So it's not the case that most things that people are doing would be broken by simply disallowing incoming TCP connections. And I expect it in the future.

**Leo:** But it is exactly that issue that I talked about, with Comcast saying, yeah, we'd like to do it, but it's going to cost us millions in people going, you broke XYZ. It was working.

**Steve:** Well, and remember, too, Leo, we have seen instances, we know there are ISPs that are NATing all their customers.

**Leo:** Right.

**Steve:** ISPs are running big NAT boxes, and all of their customers are receiving private IPs, not public IPs. Well, the fact that that's happening means none of those customers are able to receive incoming TCP connections, or UDP for that matter, neither protocol, because it's just like they're behind their own NAT router. And their computers are being protected from incoming unsolicited connections. So it's certainly the case that ISPs are already not providing those services to their customers. And apparently it's working.

**Leo:** Ian Clark in Sydney - we have a lot of Australian listeners. You ever notice that?

**Steve:** Yeah.

**Leo:** Ian Clark in Sydney, Australia wonders whether all solid-state drives are created equal: Hi, Steve. Is a thumb drive and the new, no-moving-parts, solid-state hard drive, are those the same? Can they both read and write the same as a normal hard drive? What's their lifespan? Thank you. Oh, this is a good subject.

**Steve:** It is. And I did a little - I updated myself on the state of the art a month ago because I decided I was going to splurge when I did my little OQO machine and have it configured with the 64GB solid-state drive.

**Leo:** Quite a splurge, if you get a good one.

**Steve:** Yeah. And I did. And so I wanted to find out exactly what was the technology going on, what was I paying so much money for. Because here you've got a 32GB SD card. Why aren't two of those the same as one 64GB solid-state drive, you know, a full-on SSD? There are a couple things going on. Not all - first of all, the answer, are they all created the same, the answer is no. There is cheap technology. And in fact I don't remember now what show it was of yours I was listening to, but I had your TWiT Live channel on in the background, Leo, and there was some discussion of multilevel storage versus single-level storage.

**Leo:** Yes, SLC versus MLC.

**Steve:** Yes. Yes. SLC is much more robust and much more reliable and more expensive because it is less dense. It only stores one bit in a single cell, rather than multiple bits. The way the MLS, the multilevel storage functions, is it's literally they're not bits, where "bit" means binary digit. You know, that's what "bit" is a contraction of. They're mvts or mivits or something. They're multilevel digits where an analog value stored in the single cell is used to store several digits or several bits' worth of data rather than just one. So the cell isn't storing a 0 or a 1. And you might think of that as like a voltage of 0 or 10, for example. It might be storing 0, 1, 2, 3, 4, 5, 6, 7, 8. So it might store eight different levels of voltage in a single cell that allows that cell to represent three bits of data.

Well, while the advantage of that is that you get three times the density, the problem is now you've got to be much more careful in distinguishing the voltage level. It's not just either 0 or 10 volts where you set a threshold, for example, at - well, actually you set a threshold generally low because, if the cell discharges over time, you want to make sure you know that it was once 10. But if it's 0, it's going to stay at 0. So, for example, you would set a threshold of maybe 2. And if it's anything greater than 2, you call it a 1. And if it's anything less than 2 volts, you call it a 0.

The problem with multilevel storage is you still have that uncertainty, but that means that you could have more problems because there is a cost in reliability of storing more bits in a single cell. The advantage, of course, is you get higher density and lower cost. So solid state drives that need to be high-performance and highly reliable, they're not only universally single-level storage, so they're much - they're the most you can get in reliability. They also go to great lengths to do so-called "wear leveling." That's the other thing that you need in a high-quality thumb drive that will be missing from the cheapo thumb drives they give away now free at the cash register at Micro Center and Fry's and things. Those things, I mean, again, you get what you pay for. What it means is that it's much easier to burn out spots in a highly used thumb drive that is not doing good wear leveling than is possible in a thumb drive that has high-quality wear leveling. You pay more for it because there's more logic involved, and it's just a higher cost solution. But in this case you get what you pay for.

**Leo:** Right. Yeah, it was with Ryan Shrout of PC Perspective - in fact we're going to start doing a little hardware show with him, he's great, on Thursdays on TWiT Live. And so we were talking about - I was talking about the Mac, the new Mac laptops. And it's very easy to remove the drive and put in a new solid-state drive. They only charge a few hundred bucks for - I think 400 bucks for a 128GB drive. And that's...

**Steve:** Whoa, whoa, whoa, whoa.

**Leo:** That's cheap.

**Steve:** What?

**Leo:** Yeah. Well, and that's probably because it's SL - MLC; right? That's the cheap memory.

**Steve:** Wait. Mac? Apple?

**Leo:** Apple, for a premium of I think it was $400 you could get the 128GB solid-state drive in there.

**Steve:** Wow.

**Leo:** But it's not a good - so Ryan was saying the Intel is the best drive, and it's twice as much for that storage.

**Steve:** Yes. And again, you're getting something for what you pay.

**Leo:** Yeah. So, yeah, I'm wondering what they're using in there. Obviously they want to promote SSD drives. And I was very intrigued. But what I decided was I'm going to buy the solid - the regular hard drive. And when solid-state drives come down in price - will they come down in price? I think they will in a year or two.

**Steve:** Yes. And I heard you say that, Leo, and I thought that was very smart. So, you know...

**Leo:** Simple thing to pop it in.

**Steve:** Yup.

**Leo:** And then you get a big upgrade in value for - you kind of get another year out of the thing.

**Steve:** Yup, I think that's very smart.

**Leo:** Steve, are you ready for one more Wells Fargo? It's just - it's so funny. Should we give people the background? If you haven't been listening, this all started with one email from a guy who's a Wells Fargo online customer, who said, hey, it's ignoring, it's chopping off the extra five characters or whatever in my password. It seems to be case insensitive. Is this secure? And then we've been going back and forth ever since.

Here's the latest from Gary Warner. He's the director of research for the University of Alabama Computer Forensics - this guy ought to know - in Birmingham, Alabama. Man, we've got smart listeners. He says: Steve, sorry, I'm far behind on my listening so only now getting to the September 11 broadcast. That's the one we talked about Wells Fargo. But I wanted to comment that banks still run on mainframes. Mainframes have been accepting userIDs and passwords since the '60s. Many web apps in banks are just front-ending mainframe applications. And it is the problem that may mainframe systems can't have userIDs or passwords longer than eight characters, in some cases seven characters.

It's also not possible on these same systems to have a case-sensitive userID. Everything's uppercase. Recall again that some of these systems were implemented before we even had shift keys on computers. I just thought you'd get a kick out of that. What you describe is actually quite common for front-ended mainframe applications. I'm listening to Security Now! tonight on my iPod while my Computer Forensics students at UAB take their mid-term exam. I bet he's a great teacher. Gary Warner, director of research, University of Alabama Computer Forensics in Birmingham. Thank you, Gary.

**Steve:** And it's certainly the case that...

**Leo:** It's true.

**Steve:** ...the way a lot of these systems have been moved onto the web is that a front-end GUI-like application is still talking to really old, traditional technology on the back end. And basically somebody was given the job of, we've got to get online, darn it, get us online immediately. And so someone glued together a web surface. But it's still talking to the same database technology on the back end.

**Leo:** Yeah. I know that because when I first started using my Bank of America online banking, I think I might have mentioned this. It was white text, black screen, all uppercase. You enter a menu item, 1, 2, 3, or 4. Now, this was in the '80s. But I bet you, I wouldn't be surprised if it's still the same mainframe behind the scenes, doing all the same things. You know, I mean, it works. Why mess with it?

Brian Voeller in Ashland, Oregon brings us the Fun Observation of the Week: Happy DVD Day. Greetings, Steve and Leo. I just wanted to drop you a line of congratulations acknowledging the passing of a significant milestone in your program. All of your episodes will now no longer fit on a single DVD. As I type this, I am able to archive Episodes 1 through 164 for mandatory distribution to security-deficient family and friends. Oh, my goodness. I hope they're geeks.

**Steve:** Boy.

**Leo:** Note that while I've been saving the high-quality version, a bit of math reveals that the lower quality versions should fill a DVD just after January 2019, with Episode 692, assuming you keep to your current schedule. And if I know Steve, we will. That's cool. So we've passed, I guess, 4.7GB worth of Security Now! episodes at 64kbps.

**Steve:** Yup. And in fact we're not even filling up your hard drive shelf very quickly at that pace, Leo.

**Leo:** No. Look, I've got, you know, we'd better hurry up. I've got three 750GB drives so far. We get about two weeks. And this is video. The video that I'm saving is 10GB an hour. And still just three drives for the three months we've been running. It's pretty amazing. Pretty amazing.

And finally, Matt Bender, Madison, Wisconsin with the Big Topic for Next Week: Hi, Steve and Leo. I'm relatively new to the Security Now! - ahem - "netcast" and find it very informative and entertaining. As an IT professional the topics you cover are very relevant to my daily activities. The show on Sockstress was extremely interesting and, well, scary, to say the least. I feel the same way. I've been following another, possibly even more scary exploit called click-jacking. I'm sure you must know about this, so I'd love to hear your views about it. Keep up the great show. Matt. Thank you, Matt. We talked about click-jacking, didn't we.

**Steve:** You and I never have.

**Leo:** No?

**Steve:** No, we've not talked about it here. It's been on my radar for some time. And it is, as Matt suggests, important and potentially even more scary, many people feel it is more scary than many of the other things we've been talking about. It's been in the news, the security news a lot lately. And we will cover it in detail and in depth next week.

**Leo:** Oh, good. This is one, yeah, I've been reading a lot about it. I've been testing stuff and seeing how it works. I'd be very interested to know how it works and what we can do about it. Besides running NoScript.

**Steve:** I was just going to say.

**Leo:** It all comes down to running NoScript. Hey, Steve, always great to talk to you. Thank you so much for joining us, and we'll see you next time on Security Now!.

**Steve:** Talk to you then, Leo. Bye.