Listener Feedback #167

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-403.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-403-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got a lot of security news. You know, the usual warnings and so forth. Plus some great questions and answers from you, our audience. Stay tuned to Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 403, recorded May 8th, 2013: Your questions, Steve's answers, #167.

It's time for Security Now!, the show that protects you and your loved ones online, your privacy. And there he is, the man who does it all for you, Mr. GRC, Gibson Research Corporation head honcho, Steve Gibson. Hey, Steve.

Steve Gibson: Yo, Leo.

Leo: Yo, Steve. We've been having fun talking about sci-fi and Nimoy and Spock and all of that before the show. But we'll get to that in a little bit. We'll get to it in a little bit. This is a Q&A episode.

Steve: It's a Q&A episode. If we have any listeners who are, I guess, live listeners, or who will listen, well, yeah, it pretty much has to be live, KTLA is airing throughout the day the little piece, the segment I did with them about forming proper passwords.

Leo: Oh, good.

Steve: I started - Elaine, actually, I got a text from Elaine this morning. She said, "I heard your voice from the other room." And I thought, you know, she probably knows my voice better than anybody else.

Leo: She does. She listens to you more than anybody.

Steve: Exactly.

Leo: Elaine is the woman who transcribes this fine show each and every week.

Steve: Yup, and is forced to sit and listen to this, whether she wants to or not.

Leo: [Rewind sound] What did he say? [Rewind sound] What did he say?

Steve: We've actually had some great referrals to her from the show. That is, our listeners who have heard about Elaine have found her...

Leo: She's getting something from it. Good!

Steve: Yeah, yeah.

Leo: She should give you a discount.

Steve: So that's neat. And I guess everybody's happy about that. So, and she of course is.

So, yeah, we have a Q&A. We've got - I've pushed the questions that we didn't get to two weeks ago into this one because they were good and worth talking about, and then filled in with some others that were in the mailbag.

Leo: Excellent.

Steve: And of course we've got our week's news. Okay, now, the No. 1 most tweeted, like "Steve, what does this mean?" tweet that I got over the week, all was from basically an overhyped headline on a story. The headline was "Government Lab Reveals It Has Operated Quantum Internet for Over Two Years."

Leo: Is it me, or should we expect better of the MIT Technology Review?

Steve: I know. I know. Well, and frankly, the MIT Technology Review, you would think that it would be hardcore. It's really just a fluff rag.

Leo: It is.

Steve: I mean, it's not anything that...

Leo: Jason Pontin has turned it into a piece of crap, to be honest with you.

Steve: Yeah, it's really too bad because this got everybody excited [gasp], what does this mean? Well, it turns out - so it's like, okay, I'll find out. It's very disappointing. So, okay. So here's the idea. The idea with so-called "quantum communications" is that it is utterly secure. It is more secure than any cryptography because, after all, there is a key somewhere; and, if the bad guy knew the key, unlikely as that may be, then they can decrypt what you've got.

Quantum communications, the whole concept is the act of receiving the information changes it. So the idea is you cannot tap a quantum communication, which is being done by photons over a fiber optic cable. The whole deal is that any - the act of observing the information, in a quantum physics sense, makes that event detectable. I don't know if it collapses the state, or if it alters it. But there is absolutely, I mean, the physicists know it cannot be intercepted or eavesdropped on. Well...

Leo: That's the Heisenberg Uncertainty Principle. Is that?

Steve: I don't know if that's Heisenberg because that's, you know, we don't know if - wait, no, there's Heisenberg, and then there's Schrdinger.

Leo: Schrdinger's cat.

Steve: Yeah.

Leo: That's the two states.

Steve: Where you're not sure what the state is in until you observe it, and then it collapses the state.

Leo: Yeah, the idea is that any observation changes an object.

Steve: Right, right. And we do know that - we do know from current quantum physics that that is the case. So what has been done is a quantum link has been set up that allows information to flow. And the problem is an Internet requires routing. And no one has been able to figure out how to do a quantum router. And you could argue that a quantum router breaks the security because routing requires looking at the address and then sending it out in the proper direction. And the act of looking at the address means that now you have - you've penetrated the security of the link.

So the way they solve that is they use a hub instead of routing. So, like, so all of the nodes have a fiber optic connection into a hub. So, first of all, now we don't really have an Internet. Now we have a hub, which is not nearly as exciting because they don't know how to do quantum routing. And you could argue that you can't. Then the problem is, to have it be really secure, they would have to have it go in both directions. But that would require two links, and that would double the cost. And so they said, well, we don't want to do that. Well, okay.

So what they've ended up doing is they have - so what they ended up doing, I mean, this is sad, is they send a one-time pad down the quantum link to the hub, and that's what the hub uses to send data back over a conventional network. So, eh, it's like, okay. So basically what they did was they used sort of existing technology to enhance a quantum connection, and then again existing technology to, like, allow it to be actually useful for something. Basically this is like a strained way of generating some news, it seems to me. But who cares about this? Now, also - and so, now, it is true, we know about a one-time pad. We've talked about that.

Leo: And that's an effective technique.

Steve: Very effective. Now, you do need really good random numbers, or why bother, once again. So one assumes that all of the senders are using not-pseudorandom algorithmic numbers because, if they are, then that's a weakness. But they're actually generating, they're like diode noise or thermal noise or quantum noise or any of the truly chaotic processes which we now know how to harness and refine into very high quality, truly random numbers. So the idea is that it's sending those down the link and then presumably storing them locally.

Then the hub gets them and then XORs the data it wants to send back with that one-time pad. And when it arrives, then the node re-XORs it with the buffered one-time pad. And it's like, uh, okay. I mean, so you cannot intercept the optical link because it uses fancy quantumness downstream. And you can do whatever you want to with the upstream traditional link because it's truly noise, absolutely undecipherable. And you can't get the one-time pad because you can't intercept the downstream link that carries it.

However, the security of the hub must then be infinite. That is, all, I mean, if you compromise the hub, the hub has all of the one-time pad information and all of the interchange information, and it is essentially the router. So it's like, eh, okay, well, anyway, that's what it is. It's nothing.

Leo: [Laughing]

Steve: It's a science experiment in a lab, and who cares? I mean, it bears no practical application, and it doesn't mean that [gasp], you know, there's a quantum Internet operating in secret somewheres. It's like, no, because unfortunately the quantum technology is too good. It's so good you can't route it because to look at it, in order to route it, wrecks it. So, yeah, nothing.

And back to Monday news: IE8, only IE8 has a bad zero-day flaw which is being exploited in the wild, and people are being told to stop using IE8 who are concerned about this. Interestingly, it doesn't affect 6 or 7, or 9 and 10. Just 8. And people like me are stuck

on 8 because XP won't let me use 9 or 10. You don't get that until you go to Vista or Windows 7. So, but I'm not using IE for anything anyway, so it's not a problem. But there is a - this was found by seeing it in the wild in watering hole attacks where specific industries - in this case it seemed to be government, American government employees and contractors working in the nuclear research sector, and Europeans working in defense, security, and aerospace industries.

What happened is some sites that those types of people tend to frequent were infected and were bouncing them to another server to install the Poison Ivy trojan that we've talked about. It's been around for a long time. And it's very good at thwarting AV products. It's able to avoid detection of all but two major antivirus products. And this was allowing whomever it was who was wanting to gain access to this sort of demographic of target to get into their machines and siphon off presumably nuclear research sector information.

So that's been going on. And Microsoft has confirmed the problem, issued a security announcement, and told everybody, well, you shouldn't be using IE8, after all, so stop it. And they'll presumably fix it here in our next probably Patch Tuesday. I don't know that this is dire enough. However, it is in the Metasploit Framework, so commonly available now, and there is no fix. So as we know, a lot of the world is still using IE8. A lot of the world is still using XP. So there's a big chunk of target for exploitation until Microsoft does get this fixed.

And another major ISP, British Telecom, announced in this past week that they're going to be rolling out Carrier Grade NAT also. This was covered by TechWeekEurope, that covered their press release. And I thought their press release had some interesting little nuggets in it. Just the beginning of it said, "CGNAT" - that is Carrier Grade NAT - "is a response to the dwindling" - so this is their official, this is British Telecom's official statement about how they feel.

"CGNAT is a response to the dwindling number of Internet Protocol (IP) addresses available under IPv4, the version of the protocol used across the vast majority of the Internet today. While IPv6, which offers many more IP addresses, has been defined for more than 20 years, a broad implementation of it across the Internet appears to be nowhere in sight, forcing service providers to explore techniques for keeping their IPv4 customers connected.

"IPv6 landscape" - oh, I'm sorry, that's an insert. It says, "The technique has been criticized because it imposes certain limits on users by virtue of the fact that their broadband connection no longer has the use of a fixed unique IP address, but is rather sharing an address with other users - in BT's trial, up to nine other users. This means, for instance, that users cannot serve content to the wider Internet from servers on their home network; and BT admits that it can also affect activities such as online gaming and dynamic DNS services.

"Defending its trial, PlusNet" - the subset of BT that's doing this - "pointed out that NAT is commonly used on LANs within homes and businesses, which mostly present one IP address to the wider Internet. Home routers use NAT, and BT has pointed out that NAT is also 'standard practice' for mobile broadband providers, who have had to accommodate large numbers of new connected devices. Critics, however, responded that mobile Internet services lack the flexibility that, until now, has been standard with ordinary broadband services."

So anyway, we see another major organization saying, okay, we're running out of IP space, and our subscribers are on IPv4, and they're not ready to move, so we can't

move. So...

Leo: Wasn't it, like, the British government that had all those - that big Class A or whatever it was?

Steve: Yes, it was a 16 million, it was a Class A network that they were just using internally. Just, oh, doot doot doot.

Leo: Come on, BT, talk to them.

Steve: Yeah.

Leo: It's your own people.

Steve: And it was like the people in charge of paint or something. I mean, it was not...

Leo: They weren't using this.

Steve: It was like, come on, what?

Leo: Oh, boy.

Steve: Yeah. Okay. So Syria is back on the Internet.

Leo: Oh, boy. They were off?

Steve: Yesterday, 19.5 hours yesterday, starting 18:45 UTC on Tuesday. They just - I've seen the chart. And it just went - it's like someone pulled the plug somewhere. What they say is that someone pulled an optic cable.

Leo: Oh, please.

Steve: I know. I know. This is not the first time Syria has had problems. In fact, it was a 19.5-hour, or it was a several hour, rather, outage - several times in the last year there have, you know, they've sort of just dropped off the 'Net and then come back. So we don't know why. The state-run Syrian Arab News Agency (SANA) posted on sort of a banner at the top of their site, they said: "Internet services back to normal across Syria after repairing optic cable malfunction." And "malfunction" was not spelled correctly in their banner, but we knew what they meant. So it's like, okay. Who knows? Maybe, I mean, we don't know. But anyway, they're back.

Leo: Yeah. Remember Egypt did that during the upset.

Steve: Yeah.

Leo: And it's not unusual for governments to say, gee, if we only didn't have an Internet, everything would be so much better.

Steve: So, yeah, people couldn't be tweeting and...

Leo: Couldn't be talking to each other and that sort of thing, yeah.

Steve: ...making all this mess. Okay, so I wanted to let everybody know that HoneyWords is on my radar, and I've got it set to discuss in a couple weeks, once you're back, Leo, because...

Leo: Where am I going?

Steve: Aren't you leaving next week? You're not here next week. I thought you were going somewhere.

Leo: News to me.

Steve: No?

Leo: I won't say I'm not. I don't think so.

Steve: I thought we had Iyaz set up to do the podcast.

Leo: Oh, because of Google I/O. Yeah, yeah, you're right.

Steve: That would be it.

Leo: Somebody, John came running in, said you're not here next week because of Google I/O. Yes. That's right. Okay.

Steve: Anyway, so we were familiar with honeypots, and I think might have been our first podcast was the classic "HoneyMonkeys" [SN-002]...

Leo: Yeah, "HoneyMonkeys," yeah.

Steve: ...that we had a lot of fun with. Well, now we're going to do HoneyWords. But it's an interesting concept that Ron Rivest, the "R" of RSA, has assembled. It's a 19-page research report, so it won't fit in a little "top of the show" piece. So we'll do a podcast on it because there are many really interesting ideas. The short, very, very, very short version is that online services would plant, not only fake accounts, but fake passwords, thus HoneyWords, mirroring real ones in people's accounts, so that if their database ever got loose, and people went to cracking it, if the cracked HoneyWords were ever used, it would be like a canary in the coal mine. It would be an immediate alert that somebody, that somehow their encrypted password database had gotten loose, and somebody was encrypting it - or was trying to decrypt it.

So anyway, but there's many subtleties and interesting parts to this. So, and a bunch of people have been tweeting me, saying, hey, is this good? So we're going to - it is really interesting, so we'll give it a podcast in a few weeks. I just wanted to let everybody know.

GRC has some news. We passed the 5,000 mark in finding exposed Universal Plug & Play ports for people. So I'm really happy we've got that service. GRC is now also - I've joined the ranks of sites which are 100% HTTPS.

Leo: Yay.

Steve: You can no long - yes. You can no longer get a page that is not secured at GRC. I did that over the weekend. Then I added the HSTS facility. That's the HTTPS STS is - I'm blanking on it now. Secure transport? Wait. STS. I've said it so many times, and the headers are...

Leo: Supersonic transport? Oh, no, that's something else. That's another STS.

Steve: No, STS, transport security something. [Laughter] Come on. Somebody...

Leo: The chatroom will know. Socket.

Steve: No. STS. It's source code or...

Leo: Hyper Secure Transport Stuff.

Steve: No.

Leo: Strict Transport Security.

Steve: There it is, Strict Transport Security. Thank you, whoever that was.

Leo: That was Encoded Reality.

Steve: So here's the deal.

Leo: And JBR. And Strength.

Steve: And this is very cool. So if someone makes a connection, for example, to a site that really wants to be secure, like mine, over non-SSL, then what my server will do is immediately send back a 301 redirect saying, no, please make this connection over a secure connection. The problem is that they're initially able to make a connection that is not secure, and a man in the middle could, and we've talked about this before, could arrange to strip off the HTTPS outbound query, changing it to HTTP in order to still try to make the service usable. I am blocking that. I refuse to offer any content over HTTP.

But the cooler thing to do is to declare to the browser that it has the permission to upgrade all HTTP links to HTTPS. And the way you do that is everything that GRC now sends back has a header added, Strict-Transport-Security, with a lifetime of one year, in seconds. You can specify the max age. And so what that does is that informs all the browsers that support it - and I know that Firefox, Opera, and Chrome do. I haven't seen whether IE does.

But so what happens is the browsers, anyone who visits GRC, for example, with Firefox, Chrome, or Opera, those browsers see that header and essentially cache that information, that is, semi-statically permanently remember that GRC has said that for the next year we're not changing our policy. Any connection that you start to make that is not secure, you have our permission to upgrade to secure.

So what's cool is that no user is going to put in https://www.grc.com. They're just going to put GRC.com. If they've ever been to GRC in the last year, then the browser will remember that, hey, this is - well, and every time they go another year gets added, essentially. That expiration gets updated. So they're just instantly moved to a secure connection.

And then we went one step further. I also shot the guys at Google a note asking them to put GRC.com and www.grc.com into Google's base code so that, even absent that first contact with GRC, Google knows, that is, Chrome knows that we want security. And the Mozilla people pull from the same configuration file that Chrome does. And although it's not yet out in the normal release channel, the file's already been updated. GRC is there. So that, even on a new machine, the very first time you use Chrome, it'll just know GRC is HTTPS all the time.

So this is what a growing number of security-aware sites are doing. For example, I saw LastPass.com and www.lastpass.com are already in the list, as are a number of other sites. So this is something where the browsers over time are learning that there are sites that are all about security, and they're never to establish a connection that's not. So that was neat.

Oh, and there's a new page on GRC that will be of interest to existing SpinRite owners. Two Sundays ago a SpinRite user tweeted me a photo, just a screenshot, of his SMART

page, the S.M.A.R.T., Self-Monitoring Analysis Reporting Technology page, and was concerned by what it showed. And it was such a perfect example of sort of everything going on at once on that page, that I thought, okay. This is a great - this is a teachable moment.

So I created a new page at GRC.com which is just /sr for SpinRite, /smart - and it's also in the main menu under the SpinRite category - which is a complete explanation and tutorial about everything going on on that S.M.A.R.T. system monitor page that SpinRite has. So I know that some people have wondered, you know, what does all that mean? And so now it's - because that's completely new in SpinRite 6, and there's a lot of information there [/sr/smart.htm] that I think people will find interesting.

Leo: Some people in the chatroom are saying, well, when's TWiT going to the HTTPS? Is there a compelling reason for us to do so?

Steve: No. There really isn't. I've got so many pages that have to be delivered securely, you know, the Perfect Passwords page, the Password Haystacks page, now the Fingerprints page. Oh, and I forgot to mention, what's really cool is it used to be that my technology that I had deliberately switched people back, sort of in old-school fashion, back to non-HTTPS when it wasn't needed. Well, Google quickly saw that I was sending out the Strict-Transport-Security header. And if you just put GRC into Google, I'm of course the first thing that comes up.

And there were four links there. Only two of them used to be HTTPS, and that was the Perfect Passwords and the Password Haystacks. The other one was DNS Benchmark, and another one I can't remember. Now Google has already seen what's going on and updated all of its links for the pages. It still has nonsecure for the default root page, but I imagine it's just a matter of the index getting updated. So Google is quickly seeing, oh, look, let's just change GRC over to HTTPS. But so it's really - it's a site like LastPass or a site like mine. I would argue that banking sites ought to just broadcast their security all the time.

Leo: Oh, yeah. For sure, yeah.

Steve: So sites that are about it being very important that transactions never be eavesdropped on, essentially doing what I've done really narrows the attack surface. I don't know, it's hard to imagine now how somebody could wedge themselves in, especially that we're an EV site. And we now know that the EV display for Firefox and Chrome will not come up if there's a man in the middle because the certificate is being checked also internally by the browser, not through the regular public key infrastructure. Thus you can't spoof it with a fake CA certificate in the machine.

But to answer the question, really, sites that are not about security, really, there's really no benefit. And it is administrative overhead. And notice now that I'm committed. I cannot now not ever have security at GRC because I've declared to the world that we will always have HTTPS. So I'm never going to let my certificates expire, that's for sure.

Leo: Also we'd have issues with, as somebody pointed out in the chatroom, mixed content, those mixed content warnings because we pull content from insecure sites.

So if we were secure, that would confuse the hell out of people.

Steve: Yes, and, for example, on the Security Now! page, we bounce all of the links through Podtrac for Podtrac tracking. And so I don't, for example, I have a media server, media.grc.com, and that's why I did not do - you have, with Strict Transport Security, you can say GRC.com and all subdomains. But I explicitly did not do that because I need media.grc.com to be able to be accessible over a nonsecure channel because Podtrac doesn't support HTTPS redirection, only HTTP redirection. So there are some places; but, you know, for MPEG-3 files and so forth, that's fine.

Leo: Any advantage, our chatroom's asking, to protecting from DDoS? Does it kind of slow down attacks? I don't think it would.

Steve: No. And the arguments against SSL, as we've talked about, from a computational burden standpoint, have really been diminished by state caching. It's only when you initially negotiate your very first connection with a site that there is the asymmetric, the public key expensive processing moment, essentially. And then, from then on, all subsequent SSL connections are able to use the cached credentials that each end has. So the client says, hey, I've been speaking to you recently, server. Here's a token that represents the conversations we've been having. The server checks to see if it has it; and, if so, it's a super fast connection. So it's really even not a slow thing to do anymore.

Leo: All right. So I'm not going to do it.

Steve: No.

Leo: But you should.

Steve: Yeah. Oh, I'm really - I just feel good. It's just it was a, like, "what am I going to break" sort of concern that I had because, I mean, I had - I was explicitly moving things back and forth between secure and not secure. So it was - I was holding my breath this weekend. But it went very smoothly, and now all of our pages are secure.

Leo: Yeah. I got it. Right out of the bat. Now, the other question is, we get a lot of bots registering accounts on our wiki. This is always a problem when you have a wiki is that people try to spam it. It wouldn't make any difference there. Do bots not want...

Steve: I would imagine bots are probably secure-aware. That was one of my concerns in the old days was that search engines were not all able to spider into secure pages. And then another problem was that some sites have a lot of scripting. So essentially, in the same way that, like, news sites have had paywalls, sites have inadvertent scripting walls because you can only get to their content if you run JavaScript. And so search engines were, like, hitting that and going, whoa, we're not going to run JavaScript in order to spider this. Good luck. And so that problem has been solved over time. So, yeah, I don't

think you'll see any real advantage.

Leo: Yeah. Good to know.

Steve: So in Totally Random section, I got a tweet from Donald Holben, who said that he wanted to decommission some drives, and he scratched the surfaces like crazy in order to do so. And he tweeted me a picture of a drive, the surface was just - you could hardly even see it, it was so scratched up. But one thing I noticed was that he did not pull the magnets. And so in Totally Random section I wanted to say to our listeners, hard drive magnets are the coolest things you will ever play with.

Leo: Always pull the magnet. What kind of magnet is it? What's so special about it?

Steve: What's so special is they are the most bizarrely strong magnets ever made.

Leo: Are they rare earth, or what else...

Steve: Yes. They are...

Leo: Neodymium?

Steve: They are hyper rare earth. So the idea is that you've got - you have two magnets that are being held apart. And what moves inside them is the coil that runs the head positioner. So this is the head-positioning servo coil. And so what happens is the electronics puts current through the coil to generate a magnetic field which needs something to act against. What it acts against is the magnetic field created by these permanent magnets in the hard drive. And so there's been a huge need to create the strongest magnets possible to generate the highest gauss field in order to generate the greatest acceleration and thus the lowest seek times with the lowest input power.

So the point is you could always get this thing to generate a higher acceleration by putting more power in, but that's one of the most expensive things that a drive does is seek the heads. So if you have a stronger magnetic field, then less input power will generate more physical torque in order to create acceleration. The point is huge economic need for creating strong magnets. And, oh, baby, these things, they are just bizarre, they are so strong. So they're in every hard drive. If you are ever decommissioning a hard drive, don't forget to get the magnets out because...

Leo: Is it dangerous? Is there anything I should...

Steve: Oh, they are. They're...

Leo: Don't swallow them.

Steve: Don't get them, you know, don't swallow them. Take off, if you have a mechanical wristwatch, put that in the other room. But, I mean, and when I said "yes" to your "are they dangerous," it's that you can pinch yourself.

Leo: Right.

Steve: I mean, if you got them, and they pinched some skin, they would just - they are so determined to get themselves together that - or if you reverse them, they generate such repulsive force, it's freaky how strong they are. I mean, you can spin one a foot away from the other, and it's like they're linked. They're really cool.

Leo: Well, that's the danger, I know, of these rare earth magnets and these, neo, what is it, neodymium, is that, if you swallow - kids might swallow them. And it can pinch your intestine and cause a blockage and things like that.

Steve: Yeah. There was a problem, there were - ThinkGeek was selling Buckyballs, which are...

Leo: Yeah, they put - turned them off. I have them. I love them.

Steve: Yeah, they're very fun. But again, they are swallowable. And these really aren't. They're sort of kidney shaped and maybe about an inch or an inch and a half long, depending. So they're, you know, you wouldn't think, oh, I'm going to swallow this. But still, they're very cool. And maybe you've got old drives around that are dead. And so...

Leo: It put Buckyballs out of business, by the way. They had to - they went belly up.

Steve: Wow.

Leo: Yeah, isn't that sad?

Steve: It is sad.

Leo: Yeah, they were basically forced out of business by...

Steve: Wow. Okay. So I tweeted yesterday probably the best ad that, I mean, the responses to the tweet were "Best ad ever." And for those who do not follow me on Twitter, I created a shortcut, as I do, bit.ly/snnimoy. So that's Security Now! Nimoy, N-I-M-O-Y, as in Leonard Nimoy, of course, snnimoy. This is the new Spock, Zachary Quinto, and Leonard Nimoy in an incredibly wonderful Audi commercial.

Leo: Shall we play the ad? I mean, it's two minutes long. Three minutes long, at least.

Steve: Yeah.

Leo: You want to play it. All right.

Steve: Yeah.

Leo: Here you go, ladies and gentlemen. Spock and Quinto. And this is an unpaid, unsolicited ad.

NIMOY: Hello.

QUINTO: Check.

NIMOY: Check and mate, my young friend.

Leo: So Quinto and Spock, actually Quinto and Nimoy, are playing chess.

QUINTO: How about another challenge? Want to play a round of golf at the club and get some lunch? Whoever gets to the club last buys lunch.

NIMOY: Stand by to have your wallet emptied by a tractor beam.

QUINTO: Anything's possible, but probably not that.

Leo: So Quinto goes to his Audi S7.

Steve: We should mention that our commentary doesn't do it justice. Everybody has to go...

Leo: No, you have to watch it. But there's no many audio listeners and transcription readers that we'd better explain it. So he pops his clubs into the S7, no problem. Nimoy's got a Mercedes, and profanity ensues when his clubs don't fit in the trunk. Quinto turns on his GPS, which pops out of the dash. Leonard, meanwhile, is buckling his clubs into the passenger seat of his Mercedes. I'm sorry to have to do this. It just - but we have, I have to comment. Otherwise the audio listeners just will hear music.

NIMOY: [Singing a hobbit song]

Steve: Yeah, I think maybe they just have to get online, though.

Leo: Well, we have to acknowledge that 90% of our audience is not seeing this. Apparently this is a song that Leonard Nimoy actually recorded some years ago.

NIMOY: ...Bilbo Baggins, the greatest little hobbit of all. Yeah.

Leo: Like the lens flare. Very J.J. Abrams.

NIMOY: Go, Bilbo.

QUINTO: Call Leonard.

NIMOY: Hello?

QUINTO: Hey, where are you?

NIMOY: Use your sensors.

QUINTO: No need. I'm already here.

NIMOY: You're there already? I feel like I'm stuck in a black hole.

QUINTO: No worries. I can practice my swing if you need to pull over and take a nap.

NIMOY: Smartass.

Leo: Leonard pulls up at the club, trapped in his car.

NIMOY: [Coughing, choking] I have been, and always shall be, your friend.

QUINTO: Really?

NIMOY: I had you.

QUINTO: Nice try. You lose.

NIMOY: No, no, no, I definitely had you.

QUINTO: Not for a second. Obviously, you're buying lunch.

NIMOY: Technically we're not inside yet.

Leo: And he gives him the Vulcan pinch and knocks him out.

NIMOY: I'll see you inside.

Leo: And Quinto's left lying on the ground. That is an awesome ad.

Steve: So, huge number of Star Trek references throughout.

Leo: So which - that was the movie, right, where Nimoy dies...

Steve: That was the one that predated "The Search for Spock." Oh, wait, I guess it was "The Wrath of Khan" that was...

Leo: It was "The Wrath of Khan." So that was...

Steve: At the very end where Spock sacrifices himself: "The needs of the many outweigh the needs of the one."

Leo: Right, the terraforming has gone terribly wrong or something.

Steve: Well, the probe is going to explode and kill everybody who's within its range. So, yeah.

Leo: Of course he comes back because you can't really have Star Trek.

Steve: No.

Leo: I wonder if he thought he would...

Steve: And he's still having so much - he's still having so much fun.

Leo: Yeah, yeah. What a great ad. Many agree. Perhaps the best ad ever.

Steve: Bit.ly/snnimoy, Security Now! Nimoy, and everybody can see it for themselves. It was great. Now, The Onion, of course, is well known for having a lot of fun spoofing things. There was a note that appeared in The Onion from Karen Seubert, who's the privacy and security expert for Chase Bank. And she says, "At Chase Bank, we recognize the value of online banking. It's quick, convenient, and available any time you need it. Unfortunately, though, the threats posed by malware and identity theft are very real, and all too common nowadays.

"That's why, when you're finished with your online banking session, we recommend three simple steps to protect your personal information: Number one, log out of your account. Second, close your browser. And then, three, charter a seafaring vessel to take you 30 miles out into the ocean, and throw your computer overboard. Yes, online banking security is as easy as one-two-three. Chase is committed to making your banking experience enjoyable, trouble-free, and, above all, safe."

Leo: Love it.

Steve: "Which is why you should strike your computer with 20 to 25 forceful blows from a pipe wrench as soon as you reach international waters, toss the plastic and metal shards into the sea, and then immediately sink the ship you're on. And then, once you dive to the sea floor, grab the scattered computer pieces, and shove them all inside living clams, you'll be able to rest easy knowing you're banking smarter and safer with Chase." So thanks to The Onion for that.

And lastly, the first season of a show on FX that I very much enjoyed is over, and I can recommend it without hesitation. It's called "The Americans."

Leo: Oh, yeah. I was wondering what you thought of that.

Steve: Extremely good. IMDB gives it an 8 out of 10. It has been renewed, and I imagine they're going to keep it going for a while. It stars Keri Russell, who we know. J.J. Abrams likes her a lot. So, for example, he was the creator of "Felicity," and so she was the Felicity character for four years on that show. And of course J.J. used her briefly at the beginning of "Mission Impossible 3." She was the agent who ran around a lot and died after the first 10 minutes of the show. So she didn't last very long on that.

Leo: He liked her, but not a super lot.

Steve: She was an original Mickey Mouse Club person and has a very long filmography. She plays with Matthew Rhys, who we've only really seen him briefly. He was best known playing Kevin Walker on the "Brothers & Sisters" Sunday night soap that was on for a number of years. Anyway, season one is finished. Number two is coming. And I'll give just a sense for it.

The description that they have for the show was "The Americans is FX's period drama about the complex and complicated marriage of two KGB spies posing as Americans in suburban Washington, D.C., shortly after Ronald Reagan was elected President. Philip and Elizabeth" - played by those actors - "have a network of spies and informants under their control, while their two children, 13-year-old Paige and 10-year-old Henry, know nothing about their parents' true identity. Even though Philip's growing affinity for America's values and way of life leads to tension with Elizabeth, who is quite gung-ho Mother Russia, the two must work together to keep the FBI from discovering who they really are."

And I have to say I love the show. It was really compelling because it was very well written. It was not in a hurry. It wasn't - I saw a criticism that it wasn't enough James Bond. But the fact is, there was plenty of stuff going on. I mean, it was exciting. But it

mostly is a study of, I mean, really written as if it were true, of this is what, if you assume the setup, this is what these people would really be going through. And I really liked it. So it gets a Steve Gibson 100% recommendation as something that people may want to take a look at when it's on Netflix or at your favorite media outlet, whatever that is.

Leo: BitTorrent.

Steve: Yeah. I hesitated to say...

Leo: I know what you were thinking. Your favorite pirate media outlet.

Steve: And I did have a nice note from a John Cole. And I think I pronounce this Gifu City, Japan. He said, "Dear Mr. Gibson, I just had to tell you what happened because I'm so amazed again." He said, "On another desktop computer I ran two other registry cleaners and then noticed in the ReadMe file of one that definitely does not clean out Windows registry entries to any degree, and recommended Microsoft's RegClean for that. I ran it and found some registry problems left by the two other reg cleaners and backed them up with no problem.

"So I decided to run Microsoft's reg cleaner on another older desktop, and somewhere along the way it seemed to have frozen up. I read the ReadMe file there, which says that sometimes RegClean may appear to have stopped, but is actually working. Hmm. So I waited and waited. I finally ran another instance of RegClean to check out if it would stop at the same point, and it did. So I rebooted, thinking that would clean up the ongoing confusion, but...." And we know where this is headed.

"Upon reboot, after entering the BIOS password, Windows started coming up normally, but the red LED indicating reading to the hard drive stayed lit for more than three minutes, while normally it takes only 20 seconds or so. I waited longer, telling myself this must be a fluke, and it'll be okay. Well, I got tired of waiting and finally realized something was wrong. So I ran SpinRite at Level 2, my first time to do this. I've always run Level 4 in the past.

"In the initial window that comes up, each sector was processed, but no sector came up recovered or bad or unrecoverable on that window. After the operation finished, on another window I saw many ECC corrections and other things, but I don't know exactly what those mean." Of course we've taken care of that now with the new screen that I just mentioned earlier. Anyway, "After SpinRite scan I rebooted. And just like magic, everything is back to normal, a good boot and Windows XP running perfectly again. I don't know exactly what it is that SpinRite does, but I know it does it extremely well. I can't thank you enough."

Leo: It's magic.

Steve: "When I purchased SpinRite, I thought it was a bit expensive. But it's paid for itself many times over. P.S.: I listen to you and Leo every week, and I love the show." So, John, thanks for sharing your story.

Leo: Gifu Prefecture. Prefecture.

Steve: Ah.

Leo: Yeah.

Steve: Okay. Now...

Leo: We got - go ahead.

Steve: Lastly, lastly...

Leo: Yes.

Steve: This also generated a huge feedback, mostly from people saying, what, Steve? You're saying SpinRite can't fix that one? This is the "I really want my data destroyed" photo of the week. And there's the link, Leo. You can click on that.

Leo: Let me go pull that up.

Steve: This was somebody who was determined not to have his hard drive data read.

Leo: Did he take it on a boat, bang it 45 times, and then...

Steve: I think he almost followed the Chase security...

Leo: That platter is pretty - it looks like he could - he's made an ashtray out of the platter, actually.

Steve: Someone said, "Steve, you could just steamroll it and then SpinRite would probably be able to run over it and fix it."

Leo: Actually, yeah, I mean, I think you really still need to do something to make that unreadable. I don't know.

Steve: Anyone? Anyone? Actually, you can see that he forgot the magnet. The magnet is sitting there on top.

Leo: Which one is the magnet?

Steve: That's that kind of curved-looking thing held between four dots in order to hold it in place.

Leo: Yeah, this thing here. Huh. All right.

Steve: Yeah, it's very cool.

Leo: That's that magnet. Get the magnet while you can.

Steve: Get the magnet out.

Leo: I'm going to go take apart some - we got any extra hard drives lying around, John? Let's just pry them open and take the magnet.

Steve: They're fun.

Leo: Leave the gun, take the magnet, as they said in "The Godfather." All right, Steve. Questions and answers. Are you ready, sir?

Steve: You betcha.

Leo: All right. "The Wrath of Khan." It was the, what was it, the Genesis device?

Steve: Yes, the Genesis probe...

Leo: The Genesis probe.

Steve: ...was the thing that was - or I think they also called it the Genesis device. That was what, when it went off, it was going to reconfigure all the matter within its range, and so you had to be out of that nebula where they were setting it off, or you'd be toast. And so Spock had to get the engines back online, he had to stick his arm down some horrible...

Leo: Sacrifice himself.

Steve: ...radiation thing. Yeah.

Leo: But then came back, and so everything is fine. That's why the reboot is so great.

Steve: He just - he looked great in that ad, Leo. He was, you know, I think, well, we've got plenty of more Nimoy here in the future.

Leo: Plenty more Nimoy.

Steve: And then speaking of which, Kirk looks fantastic, too.

Leo: And Shatner, too, yeah.

Steve: Shatner's in great shape.

Leo: That shows you, when you do what you love, you stay young.

Steve: Well, it's the time travel. That's...

Leo: That'll do it, yeah.

Steve: If you have time travel, you can do all - you can play all kinds of games like that.

Leo: Question #1 from Joe Roderick, Massachusetts. He wonders about the value of stealthing IPv4 ports: I love the show, thank you, et cetera. I'm wondering what the virtue is in having stealth ports these days. My understanding is, when you're stealth and somebody pings the port, no response. Nothing to attack here. Move along. However, with IPv4 nearly full, are there really any attackable IP addresses that have no device behind them? In other words, hackers might just assume, hey, it's an IP address, there's going to be a computer there. With IPv6, of course, so many ports, many of them, most of them, a vast majority of them will be unoccupied. What do you think?

Steve: Well, that was an interesting idea, I mean, the idea being that, okay, if IPv4 is all allocated, then you pretty much know there's something there. Okay. But then I love the idea that, well, wait a minute, what about with IPv6? Well, yes. When you have a 128-bit address, which is what IPv6 gives us, then it is no longer feasible to scan the address space. HD Moore scanned - recently he's been scanning a lot, the Internet often, finding all kinds of things. But that's exactly the point. The fact that there are all these devices available, visible on IPv4 says - and they're being discovered by spiders and by scanners - says you really don't want ports open. You want to be stealth. So then the question is, is it worth saying I'm here, but my port is closed, or I'm just not here at all?

Stealth doesn't cost anything. It's not like you have to pay annually to be stealth. It's

just a matter of not sending anything back when someone sends you a probe saying, can I connect to this port? You can say no, or you can just ignore them. And so all stealth is is just ignoring them. So why wouldn't you? So it's like...

Leo: As we know from this British, whatever, post office, there are plenty of places that aren't using all their IP addresses.

Steve: Yes. Exactly. And in fact, the blocks that are still unknown are known. I mean, sorry, the blocks that are still unused, unallocated, nonpublic, are known. For example, nobody is going to scan the 10-dot chunk of 16 million addresses because there's nobody there. That's been reserved. And the fact is, as IPv6 begins to roll out, the people who care about such things will know which blocks of IPv6 have been allocated to whom. So there will be allocation maps available, saying, if you want to scan, these are the blocks you would scan. And there'll be all kind of leakage of which IPv6 addresses are in use.

For example, right now every server gets all the IP addresses of everybody who contacts it. So if, in some future world, maybe not this one, IPv6 ever does exist, it'll be easy to start building logs of what IPv6 blocks are apparently allocated based on traffic coming into servers. So it's really never going to be a mystery. Even vast as the IPv6 space is, we'll be pretty much - there'll be lists and well-known, these are the ranges that are alive, and the vast majority of the space will always be empty. And again, stealthing is free. Just don't say anything.

Leo: Right.

Steve: Yeah. Just ignore the nonsense that's coming in.

Leo: Why respond?

Steve: Right.

Leo: David Riggleman in Indianapolis suggests that the SSL Labs report doesn't tell the whole story: Thanks to your recommendation of SSL Labs, I ran a report on one of the banks I use, Huntington National Bank. They are a larger bank in the Midwest, and I was shocked when they had a grade of F because they supported SSL v2. I immediately contacted customer service and eventually reached the IT department. After some investigation, it turned out that the bank's main page did support SSL v2, although they did plan, there was a plan in the works to drop it, but it hadn't yet been carried out. However, and this is important, that's different from the server being used for online banking. I reran the SSL Labs test, and this time the grade returned was a C. I presume he put the banking URL in instead of the front page address, which is of course what you should do. Anyhow, I wanted to make you and possibly others aware the grade they see from SSL Labs when first visiting a site might not tell the entire picture. Thanks for the great show.

Steve: Yeah, that was a great note. Many people - first of all, the SSL Labs referral has been really useful. I've had a lot of feedback from people who, frankly, stunned me with

how quickly their banks did reply, credit unions and banks and so forth. I think it's just, it's so easy to be concerned by a grade of an F, and SSL Labs will give anybody who has SSL v2, because there are so many exploits possible against v2 of SSL, an immediate flunking, failing grade. So many people said, my credit union had an F. I told them. The next day it was a B. And it's like, wow. Okay. I mean, but not just once. Over and over and over and over.

So I've really been impressed with the power of the visibility. And of course banks are going to be more concerned about their reputation. So the idea that someone is rating their security an F is going to get the attention, you know, is going to shoot through at lightspeed to the IT department.

But the point that David makes is a good one, and that is, you absolutely - and many people have been confused in the same way - absolutely have to make sure that you are testing the proper domain because you might have BofA, for example, dotcom, and but when you actually do online banking, it's onlinebanking.bofa.com, which is an entirely different network or server or whatever. That's the security that you want to test, not just BofA.com. So definitely important to make sure, as you also amplified, Leo, that they're checking the right domain.

Leo: Yeah, that makes sense. Lance "The Paranoid Cheapskate" Reichert, who is enjoying the muddy season of upstate New York, wonders about the security of new era common interfaces. He says, I'm looking for a Drobo to use with one dedicated computer which will remain turned on, attached to the Drobo all the time. This would be the server. And one or more computers will share the Drobo through that server over a network. There seem to be three interfaces for the Drobo family: Thunderbolt, USB 3.0, and Ethernet. Ethernet is definitely not what I want, since I want a single machine to own the device array, but I'm unsure of the security aspects of the Thunderbolt and USB 3.0 ports.

In the past you have mentioned that DMA ports like Firewire make it theoretically possible for a physically present intruder to peek into a running system and retrieve keys to encrypted drives. Do either Thunderbolt or USB 3.0 leak that kind of access? If the server PC lacks an integral USB 3.0 port, would adding a USB 3.0 interface card give that Firewire-like access to internal memory? Same question for Thunderbolt adapters. Thanks.

Steve: Great question.

Leo: Do you have to freeze the memory in order to read it? I mean, isn't it, like, complicated?

Steve: Actually, not for Firewire. He's remembering correctly that Firewire, unlike USB, any version of USB, Firewire is a DMA interface. And here's the key: So is Thunderbolt. So...

Leo: That's for maximum speed, I would guess.

Steve: Well, what it is, is instead of it being a...

Leo: Oh, it's peer to peer as opposed to master/slave.

Steve: Yes, exactly.

Leo: Yeah, yeah, client-server, yeah, yeah.

Steve: Exactly. So the Thunderbolt device, just like a Firewire device, has access to all of your system's memory. And it does that in order to be a so-called master on the bus and essentially be able to transfer its data into the system memory without any intervention, like without having to be continually polled by the processor running in the device. So it's able to get much - that's the way it's able to get much higher throughputs is you're able to tell the device, send your stuff to this block of memory, and it does it autonomously. In order to do that, it's providing both the address and the data through the interface which gives it access to everything. Now the specification for Thunderbolt gives it unfettered access.

But we have seen that in Firewire, and I'm sure in Thunderbolt, the implementation may put boundaries on the region of memory that it's able to access for the sake of security. So if Lance is concerned, I would choose USB 3.0 over Thunderbolt from a security standpoint because Thunderbolt does have some potential concerns. And especially if it's running on Windows. I don't know if this is - if he assumes it's a Mac. Maybe it's on a Linux box. But you'd want to make sure that it was bolted down from a security standpoint because the Thunderbolt can potentially access all of your memory, just like Firewire.

Leo: I'm not sure I'd do what he's saying to do. I'd just get a NAS.

Steve: Yeah.

Leo: Okay. But anyway...

Steve: But for whatever reason, that wasn't what he wanted to do.

Leo: That's what he wanted to do. Maybe he has a Drobo lying around. Gianpaolo Racca in Italia wonders: OpenVPN build or buy? Hey, Steve, thank you for your show. I heard the last - I can't. I won't do that. I heard the last, 400th, episode, and it made me think. It's been a while since I started considering a VPN service. I own a home router flashed with Tomato. So my question is, my only concern is privacy of mobile data. And since I saw there's an official OpenVPN client for iPhone, can I set up my own VPN network, then route my mobile traffic through that, through my system, to the public Internet? Not just to save money, but also to learn something and not have to switch VPN if I have to access my home network. What do you think about that? Thanks, and keep on rocking.

Steve: Answer is one word: Yes.

Leo: Yeah. Good idea?

Steve: That's a perfect solution. Use Tomato. Tomato supports the OpenVPN server.

Leo: Is it pretty easy to use?

Steve: Yes. Yes. It is very simple to use. And you can - if you also use ipchains, I believe that's what it is, you're able to have multiple ports that all feed into the port that serves OpenVPN. The advantage of that is that you have a much better time getting out of whatever network you're in, onto the Internet, and over to your home. For example, you might use port 80 because OpenVPN is an SSL VPN.

So I think OpenVPN, it's been a while, it's like 11 something is the default port, 1191, or I don't remember now. But I would say also use, like, port 80, maybe 443. Use some common ports that are typical web ports. Those are probably not going to be blocked outgoing, like from Starbucks, for example. So then you'd be able to use your iPhone to connect to your own router at home.

When you do that, you'll get a 192.168 IP address, literally an IP address on your home network. And then it will route your - then you'll be able to talk to your home devices. You'll see them just like you're on your home network. But any external traffic will go right back out to the public Internet. So that's a terrific solution. So that's many more than one word; but, in one word, yes.

Leo: Yes, plus annotations. Joseph in Los Angeles wonders whether Carrier Grade NAT, or CGN, is more anonymous: Is Carrier Grade NAT more private? Is there a way for the ISP to uniquely ID a user except by modifying the HTTP_USER_AGENT on a non-SSL session? How would an ISP respond to a warrant in that case? Could they? The RIAA must hate this idea.

I don't want to sit behind a 10.x.x.x IP. But I think for my wife, kids, and friends, it's a great idea - except when they have a problem and call me for help. I hope the CGN only blocks inbound ports and not outbound ports. You'd better explain. I don't understand what he's talking about at all, Steve.

Steve: I could hardly even hear you, Leo. Is my audio coming through to you okay?

Leo: Yeah. Sorry. Maybe I should talk louder.

Steve: No, it was Skype. It was bad, bad, bad.

Leo: So what is he - can you just explain what it is? What is CGN, anyway?

Steve: So this is what we were talking about that BT telecom and Verizon also announced that they were going to be doing soon, and that is Carrier Grade NAT. So the

idea is that they're a NAT router. Your ISP is a NAT router. And so what he's wondering is, is there a way for the ISP to uniquely identify their user in traffic that they can see? So that's why he says "non-SSL sessions" because the ISP is unable to see into that traffic. And so what he's wondering is, is once CGNAT, Carrier Grade NAT, comes into use, organizations like the RIAA will no longer see per-customer IPs that they then ask the ISP who was your customer with this IP at that time?

So the problem is the ISPs are keeping records. And so they will know what non-routable IP and routable IP was in use. So my guess is we don't - we probably don't get, like, an increase in privacy as a consequence of our ISPs using NAT for us. It's probably still possible for an external organization that wants to track down people who they presume or believe are acting illegally. I'm sure there'll be a way for ISPs to say, oh, yeah, that was this customer of ours.

Leo: Of course. All the RIAA does anyway is contact the ISP and say this is what we know. Tell me who it is.

Steve: Right. But, I mean, his...

Leo: So presumably the ISP knows exactly who it is. That's the only question. If the ISP didn't know, then they couldn't say anything. But they know.

Steve: Well, it does require additional recordkeeping on the ISP's part because now the ISP has to know, not only which private IP they assigned, but which public IP that was mapped to, because somebody on the outside sees the public IP, not the private IP. So, I mean, it will definitely require the ISP to, like, to maintain that mapping, which right now they don't have to maintain.

Leo: So a privacy-inclined ISP could say, hey, we're not going to log this information, so when we get a subpoena we won't be able to do anything.

Steve: Yeah. I mean, think of it exactly this way. It's like, imagine you have, like right now, you've got your normal NAT router in your household, and somebody on the outside says, hey, your IP was doing such and such. Well, and if you had a household of six people, there's no way of knowing which one of those people was the one. Except, if you used things like time of day and...

Leo: Say, hey, who was using the computer at 4:00 o'clock yesterday? You're in trouble.

Steve: So you see what I mean. Then that router obscures the identity behind it.

Leo: Sure, that makes sense.

Steve: And so the identity stops at the NAT router. So what CGN, Carrier Grade NAT,

does is it pushes that NAT router boundary out to the ISP. So now everyone behind that is obscured. So it does increase the level of obscuration.

Leo: Obfuscation.

Steve: Obfuscation.

Leo: Obfuscation. So Greg - in Montvile, Montville, must be Montville - Ohio wonders about proXPN servers. I assume you'll be answering a lot of questions about proXPN on Security Now! next week. We should say, if you're tuning in, that is the sponsor for the show. Here's mine: While software such as this provides a secure connection between me and one of their servers, the endpoints, what about the connection between proXPN and the site I'm trying to access? My Internet traffic has to exit that VPN tunnel before it goes to its final destination. Won't it once again be vulnerable at that point? And won't proXPN know everything I'm doing on the Internet because they're acting as an intermediary? Why should I trust them any more than I trust my ISP? Or is my understand of how this works incorrect?

Steve: Well, okay. So we're back to the same problem we've talked about often relative to, for example, the Tor network, the so-called Tor exit nodes, where because everyone who's using Tor has their traffic essentially concentrated from all over the Internet down to just squirting out of a few exit nodes, you would think, logically, that those would be prime targets for monitoring. So in theory Greg is right, that traffic is being routed in full crypto tunnels to the proXPN servers, and then at that point decrypted and released onto the Internet. So those servers represent all of the traffic concentration points of all of proXPN's users.

Leo: It has to exit somewhere, otherwise you wouldn't be able to - unless you had VPN directly to the website. But as far as I know, nobody does that.

Steve: Well, that's the advantage to having it at home is that then your traffic goes to your house and then is emitted from your house, rather than being aggregated by a big server in the cloud where it's all coming in and out with everybody else's. On the other hand, there's a ton of traffic coming in and out of those servers in the cloud, so that's - so your traffic is mixed in with those. But I guess my point is that the use model is a little different. Greg sort of is thinking, well, wait a minute, why would I use this at home? Well, I don't think you probably would unless you wanted to obscure your traffic from your ISP, as you were saying, actually, as one of your use cases during the - when you were explaining about proXPN earlier, Leo, that would be something you could do is use proXPN to keep your ISP from snooping on you.

Leo: For the six strikes law, for instance, yes.

Steve: Yes, yes. But the real advantage, I think, is for a road warrior who's out in hotels, who's traveling, who wants to encrypt their traffic. So if you were saying that, you know, you lived in California, and you were in New York, well, you could set up a tunnel all the way back to your home in California. But if proXPN has a server in New York, you're

going to get much better performance using a VPN server close to you. So again, it's a set of tradeoffs. It's an option that you would have. But there are many use cases and many different ways you could connect a cryptographic tunnel, either to home or to a central point. But it's absolutely true that there is some inherent concentration of data in any of these cloud-based servers.

Leo: Yeah, and presumably the RIAA would, instead of sending a note to your ISP, would send it to proXPN. But I don't know whether proXPN would be able to tell who was using what when, or, I mean...

Steve: Well, and what logging they do. I know that a lot of our very savvy users were asking proXPN, because I saw this Twitter traffic going back and forth, which country's laws do you follow? And the answer was we follow the laws of the country in whose - where the servers are located. So for U.S. servers, they follow U.S. laws; and for foreign European servers, they follow the laws of the country where the servers is.

Leo: They're a Dutch company. Am I right? I can't remember.

Steve: Yes, or The Netherlands, yeah.

Leo: The Netherlands, yeah. Well, I'll have to look at the site, and we'll ask them. But meanwhile, Kent is next on the docket here. He says he's located somewhere on that third rock from the sun and wonders, when is a router too old? Hi, guys. Insert nice gratuitous comments here. I'm wondering, how old is too old for a router to still be safe? I've been running a old D-Link DI-604 with its final firmware. It hasn't been updated for several years. So I'm wondering, is it still safe to use such old hardware to protect my LAN? Or should I start shopping for some shiny new one? And, if so, what would you recommend? I don't use WiFi as I don't ever see it as being totally secure. What do you think about firewalls that use old PCs, like pfSense? Signed, Kent.

Steve: Okay. Well, we're asking the wrong person whether you should upgrade something that's working just perfectly for you.

Leo: [Laughing] Yeah. Steve is the guy who uses old technology.

Steve: Yeah. I've still got cranks on the sides of my machines, and they just run. As long as the watch springs don't break, we're all fine. I think there is no reason. If the router does what you want; if you don't, for example, want to switch to Gig Ethernet, which is probably not supported, well, I'm sure it's not supported by the DI-604; if you're happy with the Ethernet, if you're happy with the speed, if you're happy with the features, if you don't want WiFi, I mean, we see instances where the new stuff is where the problems are.

Leo: Right.

Steve: I mean, it probably doesn't have Universal Plug & Plug. Yay.

Leo: Yay.

Steve: So, yes, stick with it. I see, you know, again, I'm probably the wrong person to ask. But I see no reason to change it until you need some features that it doesn't offer. And old PCs make really great routers, although they're just much less of a sort of a tiny, turnkey, low power consumption box. They've got fans and power supplies and so forth. So, I mean, I think running a PC makes sense, if you've got one, and you like the flexibility of having more of a Linux-based, bigger iron solution. But it's definitely - there's just more to it than a cute little router running in the corner.

Leo: Mark Prescott, Calgary, Alberta, Canada, has some terrific input about Butterfly Labs and bitcoinage: Steve, I just finished Episode 401 of Security Now!. I thought I'd send you two thoughts on the Butterfly Labs question. Butterfly Labs has produced and shipped some Jalapeno units. My impression is the majority of these units went to bitcoin review sites, but some likely have gone to paying customers. To my knowledge, no other units have been finalized.

According to their statements, BFL has run into problems developing the ASIC units, as you suspected, in a few areas, namely power consumption, heat generation, and the amount of processing power they can get onto a single chip. This has resulted in price changes, expected output for the units, and changes in the casing and fan assembly. Quite frankly, I believe them, but that doesn't change the fact that they're facing an uphill challenge which could result in orders not being fulfilled. That's his speculation, by the way, not something coming from Butterfly Labs.

Steve: Right.

Leo: Second, your final question on Episode 401 referred to the ability of a 5GHz per second - I'm sorry, giga what? "GH."

Steve: Hash. Gigahash. Gigahashes.

Leo: Gigahash per second Jalapeno unit being able to create $900 of bitcoin in a month at the present time. I just wanted to clarify that, while this is true, it doesn't really have any basis in what will happen when the units are officially released and widely available.

Steve: Right.

Leo: The reason is difficulty. The difficulty of mining bitcoins adjusts every 2016 blocks, roughly every two weeks, to keep the rate of bitcoin generation consistent. That means the total network hash rate, currently about 80,000 gigahashes per second, is used to determine that difficulty. So as these units start being spread out

on a widespread basis, the difficulty is going to rise proportionately and ensure that the bitcoin production of these 5 gigahash units will not result in $900 a month worth of bitcoins being produced unless the value of bitcoin rises dramatically. Which of course it might. Or if you're like, it's like a pyramid scheme. If you're the first one to get it, you're going to make more money than the later people.

Steve: Exactly. Exactly.

Leo: Keep in mind a large portion of the current network hash rate is derived from GPU-based bitcoin miners, which have much worse megahash per second per dollars and megahash per second per - what's "J"? Jalapeno rates? What is this? You're starting to lose me. What? Joule. Oh, because we're talking about heat use.

Steve: Oh, energy, yes, energy usage, yes.

Leo: Megahash per second per joule rates. Obviously we've got a bitcoin miner in the audience here - than even the Jalapeno unit. This means that as the cheaper units become available, it will become economically nonviable to mine with GPU miners, and everyone will be using the Butterfly Labs or similar ASIC units.

Steve: Yup.

Leo: Yeah, because that will be the standard.

Steve: It's just going to push everybody in that direction, and a lot of people will no longer be able to play.

Leo: The end result: The entire network hash rate will likely depend almost entirely on the cost, initial hardware and cost of running, of whatever the most widely available mining hardware is. That is, $500 worth of hardware/power will now likely produce the same amount of bitcoins as $500 worth of hardware/power in a year or two. That's good logic. Its just the nature of bitcoins. That make sense?

Steve: Very nice piece of work.

Leo: Yeah, yeah.

Steve: So thank you, listener.

Leo: That's how it's designed.

Steve: Yup.

Leo: Hi, Steve, says Volker Nebelung in Bonn, Germany. Nebelung, isn't that a - I think that's from Wagner ["Der Ring des Nibelungen"]. He reports weird ShieldsUP! results: Steve, I used your port scanner tool today in my new router FRITZ!Box 7360 SL - der FRITZ!Box - and I'm getting very weird results. Both links show images of two scans of my IP address. I'll show those in a second after I finish reading this.

Every time I scan, ShieldsUP! shows different ports - oh, weird - as closed or stealth. Additionally, the closed ports are always appearing in a certain pattern with a diagonal line of closed ports shown in the screenshots. Is this a bug in the port scan, or is my router actually responding with weird port information? Thanks for answering, Volker. What?

Steve: This is a wonderful and very interesting question. We encountered this immediately after I added that new feature to ShieldsUP! where it was being smarter about not detecting stealth when things were not stealth. Remember that I added its ability to understand ICMP echoes coming back from closed ports. Originally ShieldsUP! would send out a TCP SYN, and it was only looking for a SYN/ACK or a TCP reset, the reset saying go away, we're closed here. But the other thing that a TCP port can send back is an ICMP packet saying port not available.

Now, here's the gotcha. The rate at which ICMP packets will be sent is limited. The Internet specifically rate-limits ICMP traffic. So you can't have, like, ping floods and other sort of bad situations where ICMPs would start flying around the Internet and, like, never go away. So what's happening is the reason Volker is seeing this strange pattern is ShieldsUP! is sending out probes at a certain rate. And his new FRITZ!Box is not stealth. The way it's currently configured, and he can probably change the configuration, it is responding with ICMP packets.

But either it or a router along the way is saying, wait a minute, you're trying to send back too many ICMPs. We're going to drop some of these. So that's why ShieldsUP! is not receiving all of the echoes back. It's not seeing all of the ICMP packets. So sometimes it'll see closed, and sometimes it'll see stealth. The ports are really closed, but we just can't get all that information back.

[http://imageshack.us/photo/my-images/832/ohnetitelf.png/]

[http://imageshack.us/photo/my-images/407/ohnetitelt.png/]

Leo: Wow.

Steve: So what you end up with is this weird pattern.

Leo: That's cool.

Steve: Yeah, it really is cool.

Leo: That is really cool.

Steve: Yeah.

Leo: Amazing. Couple of tweets for you. Dale in Fresno, wondering about re-using the Blizzard Authenticator dongle. Re-using it. Is the authenticator dongle which Blizzard's selling at their website usable for more than one site? They are selling them for $6.50 each, which seems to me a great price [bit.ly/10RQX89]. We were talking about how authenticators, it's kind of a standard now. Is it using the standard? Do we know?

Steve: Yeah. Okay. So I feel like maybe I - because I saw a lot of questions like this, and I feel like maybe I rushed through explaining that. The problem is that, if you were to - behind every authenticator like the Blizzard Authenticator is a symmetric key. That is, there is a key that goes along with it. Users who set up software authenticators, like with Google and Amazon and Microsoft and Twitter and so forth, users who set those up see those keys.

But in the case of Blizzard, for example, what you have printed on the back is just a serial number, and the key is secret. You never know what that key is. And that's what the authenticating organization, maybe it's Blizzard is authenticating themselves, or maybe it's VeriSign, as is the case, for example, with the original PayPal and eBay footballs. So a third-party knows what that key is, and they will not tell you. They won't give you that key.

So the model for the authentication that Blizzard offers is of an authentication service where you ask the third party what code the authenticator should be showing. And you're never able to, like, give that to someone else. You'll never know what the code is. And so you can't provide it to someone else. But more importantly, in this model, you really don't want to because, if you provide it to multiple people, and any of them gets their database hacked, and of course databases are being hacked all the time, unfortunately, then your secret code for your one authenticator gets loose.

And it's very much like using the same password on every site. We know you don't want to use the same password on every site because, if it gets loose, then you can be logged in, people are then able to use that same password to impersonate you elsewhere. Similarly, you do not want to reuse, ever, the same authenticator code on multiple sites. So you really have to think of the Blizzard dongle as first-generation technology. It's cool, but it's hardware. And, frankly, we've already moved past that. We've moved past hardware dongles. We're now into software dongles, essentially virtual.

Leo: I love the Google Authenticator.

Steve: Yes.

Leo: It's just fabulous. And so help me understand, then, what's happening. Because with the Google Authenticator, it's software running on my phone, Android

or iPhone. And when I want to add...

Steve: It knows what time of day it is.

Leo: It knows what time of day it is, okay. So when I want to add an account, I can enter in some numbers or scan a barcode, which is what I always do. Currently mine has three. It has Google, LastPass, and Outlook.com. All three of them are using second-factor authentication. I've turned that on. And by the way, I saved those bar codes, you're probably not supposed to, but I saved them in LastPass. So if I want to add a new phone, because I'm always using new phones, I have the barcode. I just take a picture of it.

Steve: Nice.

Leo: And so that's great. So what is in that barcode? Is that a serial number?

Steve: Yeah, well, that is the private...

Leo: That's the key.

Steve: That's the private key that the agency authenticating has given to you in the form of a 2D barcode. And then...

Leo: So that's what you want. That's the problem with the Blizzard Authenticator. It's the same key all the time.

Steve: Exactly.

Leo: In software, my Google Authenticator can have as many keys as I add.

Steve: Yes.

Leo: And so I look, and I get three different codes, depending, and I just pick the one that I need.

Steve: So this solves the problem of the so-called key ring. We talked about we'd like - oh, we hope, years ago, when this was just emerging, we were hoping that we weren't going to have a big key ring full of individual dongles, each with their own code. And this has been solved, thanks to the proliferation of smartphones.

Leo: And everybody should be using this because this is now a standard. It's not a Google standard. Others could make an authenticator that would work exactly the same.

Steve: Yes. The one thing I think we're going to see, and this is premature, but I think there's a way to leverage public key crypto, and we're not doing that yet. This is all symmetric, private key crypto. That is, that key is secret, and you need to keep it secret. But I think there's a way, when we take this one level up in complexity, and I kind of think that's where Google is headed. We'll have to see how this evolves.

Leo: And that's why I'm proper to keep my QR codes locked up in LastPass because that's the key to the kingdom. Anybody could then...

Steve: Yes.

Leo: ...add that to their authenticator.

Steve: And you're exactly right about wanting to keep those because that allows you to clone those. It's funny, someone sent me a picture of three different phones, side by side, all showing the same code. And that person said, well, so much for authentication. It's like, no.

Leo: That's the point.

Steve: That's what you want. All three have the same code. They all think it's the same time of day. So they're all going to show you the same result.

Leo: They're behaving properly.

Steve: Yup, exactly.

Leo: Otherwise it wouldn't work, if it wasn't always - yeah. No, I do, because I've always got a new phone; right? So I just install Authenticator. I scan in those codes. It couldn't be easier.

Steve: Flash the barcode, yeah.

Leo: I just think everybody should do this. It's just...

Steve: It's a win. It is the right way for now.

Leo: It's awesome.

Steve: I think it won't last. It's going to - we're going to already obsolete that soon.

Leo: Really.

Steve: But for now it's absolutely the right way.

Leo: With some sort of identity feature where I'll have - because I'll have my private key, and I'll give out my public key.

Steve: Exactly that. Exactly that.

Leo: Okay.

Steve: Exactly that. Right now we don't have the horsepower. But we will shortly.

Leo: This is great. I love it. I have to say. I feel so much more secure. And I wish everybody would. I turn on second-factor now anytime I can.

Steve: It's the right way.

Leo: Oh, yeah. That's great. It just gives you peace of mind. Anne Stellingwerf, @AnneSt on the Twitter in Apeldoom, tweets - and I'm surprised we didn't get any questions, this is the first question about BitTorrent Sync, which we covered last week, the one and only question: If there's no authentication on BitTorrent Sync, isn't it insecure? Because I can try keys and download people's files anonymously, in other words, brute-force the key. How is uniqueness of the generated key guaranteed? Generating a duplicate key would lead to downloading someone else's files. She's got a good point.

Steve: Yes. Absolutely does. And it's funny because I went back and forth in Twitter trying to explain that, if the key was four characters, then we would have a problem because that's just not - that's not enough bits. But we believe, and we don't have the full technical readout from them yet, but I'm sure we're going to get it, it's too - we believe that it is a root key of 168 bits. Now, we're just - people are bad at understanding probabilities. But that means there are 2^168 possible keys.

Now, that happens to be, I'm not doing this in my head, I did this ahead of time because I knew you were going to ask me this question, Leo, 3.74 x 10^50. Okay. That's three, and 50 zeroes, 3.74 and 50 zeroes. I mean, so yes. We definitely need good pseudorandom generation. I mean, for example, if you wanted to use your own key, you could use the Perfect Passwords page at GRC, which generates incredibly, very high-

quality, pseudorandom keys. But the beauty is we are hiding in this vast key space. 2^168, that is a huge key space. And it is true...

Leo: Somebody in the chatroom said 300 trillion trillion trillion trillion.

Steve: Yeah.

Leo: I don't know if that's right, but it sounds like it to me.

Steve: It sounds right.

Leo: It's the right order of magnitude.

Steve: And so, but, I mean, yes. If you, I mean, imagine, think of it as 168 random bits, like pennies, heads or tails, 168 of them. And you have to have every single one exactly right. Well, the fact is that is an incredibly vast key space. So, I mean, for example, it is much more secure than a username and password.

Leo: What? Oh, that's interesting.

Steve: A username and password, think of the total number of characters.

Leo: There's potential collisions there, too, aren't there, after all.

Steve: Yes. There are many fewer characters in a username and password. And the beauty of this is there is no central repository. If you had accounts, you'd have to have an account center somewhere. This is just saying that we're going to have so many bits that you can just pick one at random out of the air, and it is vanishingly small chance of ever colliding with someone else. Of course, if you did, you'd know instantly. But it's just not going to happen. It's just not going to happen.

Leo: Wow, that's really - so collisions are possible, but highly unlikely.

Steve: Ridiculously unlikely.

Leo: Like the universe is going to end unlikely.

Steve: I mean, just like, yeah. It won't even get started, Leo. And we forgot to mention the "Ender's Game" trailer while we were recording. So I just wanted to let our listeners know, "Ender's Game" is a fabulous sci-fi by Orson Scott Card. It's a classic sci-fi concept and story. There is now a trailer. I'm sure people can Google it and find it.

Leo: Oh, it's easy to find. That's how I found it. It's on YouTube.

Steve: Harrison Ford stars. It's coming out, I believe it's November 1st of this year, so the beginning of November of 2013. Go find the "Ender's Game" trailer. Oh, goodness, it looks wonderful.

Leo: And we have verified it is spoiler free.

Steve: Yes.

Leo: And we do recommend, though, at least I do, read the book. You have till November to read the book. Because...

Steve: The book will be better.

Leo: ...one or the other's going to spoil it for you. So be spoiled by the book, the original. Although some people prefer the spoilers to be delivered in visual form on a screen. And if that's the case, then don't read the book. But one or the other is going to spoil it for you. Really, really good. I can't wait. Looks awesome.

Steve Gibson is the man at GRC.com, the Gibson Research Corporation. That's where you'll find SpinRite, his bread and butter, the world's finest hard drive maintenance and recovery utility. If you have a hard drive, you must have SpinRite. But you'll also find lots of freebies there as Perfect Paper Passwords; Password Padding, which has really changed my life. All my passwords are super long, thanks to Steve. Lots of information there, including ShieldsUP!, the absolutely must-use Plug & Play detector, the probe to make sure your router is safe. GRC.com. 16Kb versions of the show are also lurking there somewhere, as are text transcriptions by Elaine Farris.

And I should point out that, if you have a question for Steve, we'll do another Q&A episode in a couple of episodes. GRC.com/feedback is the place to leave those. Don't email him. It's not allowed. We keep bigger quality, higher quality versions, larger files, on our site, TWiT.tv/sn, both audio and video. Or subscribe, and you'll get it every single week. You could pick the form you prefer. Steve, I thank you.

Steve: Thanks, Leo.

Leo: See you next time on Security Now!.