Listener Feedback #169

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-407.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-407-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We'll talk a little bit about security news. There's some sci-fi news, some reviews. Steve likes to throw those in. And your questions, Steve's answers, BitTorrent Sync and other topics, coming up next on Security Now!.

Leo Laporte: It's time for Security Now! with Steve Gibson, Episode 407, recorded June 5, 2013: Your questions, Steve's answers, #169.

It's time for Security Now!, the show that protects you and your loved ones online, protects your privacy, all thanks to the fellow we call our Explainer in Chief. That's me, he says. Steve Gibson of GRC.com. How are you doing, Steve?

Steve Gibson: Hey, Leo. It's great to be with you again, as always.

Leo: Good to see you.

Steve: Shouting to each other at about a 500-mile distance.

Leo: Yeah, that's unfortunate.

Steve: Thanks to Skype, where it's just like you're in the same room with me.

Leo: Does your T-shirt say anything, or is it just blue?

Steve: It's the - I didn't realize this was the Mt. Fuji, this Atari logo. It was actually Mt. Fuji.

Leo: Which is...

Steve: Yeah, it's very cool, yeah.

Leo: Nolan Bushnell was actually a really cool guy. The word "Atari" itself is a term from the game of Go.

Steve: Atari, yes.

Leo: Yeah. So he's an interesting feller.

Steve: So we have a Q&A this week, as always, great feedback from our listeners, comments, questions, thoughts, observations, worries, concerns, all the standard things you would expect from a security-oriented audience. And some interesting news bits. I'm going to share a couple, the meat of a couple interesting articles, and we've got a really interesting video I want to put into our record from this morning's "Today" show. There is a mysterious new way that bad guys are opening cars with apparently zero effort.

Leo: Oh, great.

Steve: Yeah.

Leo: It's probably the more high-tech, fancy cars.

Steve: Oh, yeah.

Leo: Oh, yeah.

Steve: Yeah. Like I said, if it can go wrong...

Leo: It will. We've learned - if you've learned nothing from this show, you've learned that much.

Steve: It's why I love my - like I said before, I've got what I think is an '04 little 300

Series Beemer, which is coming up on 10 years old and just where I like it because I'm thinking, okay, they can't get me. My car's too stupid to open its doors.

Leo: You actually have to...

Steve: I want a dumb car.

Leo: Think about a key. I mean, that's such a primitive thing, this specially shaped piece of metal that has to...

Steve: Yeah. The little wiggles absolutely do nothing. I think they're just there to pacify us.

Leo: Turn the tumblers in just such a way that the lock goes.

Steve: I don't think it does that anymore. I think that mostly it just wiggles, and then there's a whole electronic communication going on.

Leo: It's a serving suggestion.

Steve: Even a decade ago they'd figured that much out.

Leo: Steve Gibson, let's see here. What do you want to start with? You want to start with this car thing?

Steve: I do. And the reason it works for the podcast is the audio is descriptive enough that the people who are not able to see it are able to hear it because the story explains itself. And I've also just tweeted the link [on.today.com/15ByCtB] to the story which appeared on the "Today" show this morning. And it's very apropos to this podcast.

Leo: They're stumped, police say, by the mystery car thefts. I think we're going to have an ad here, so let me just, yeah, we'll just sit and watch that for a little bit.

Steve: Do, do do, do do.

Leo: Dee, de do do do. I should have started it earlier. I should know better. I should know better.

Steve: Yeah, so we'll look at this and then talk about it. I have a theory about what's going on which appears to be more than anybody else has at this point. But just based on the evidence.

Leo: Well, that's the thing. We know the symptoms. We don't know the cause yet.

Steve: Right.

Leo: Here we go.

[Clip]

SAVANNAH GUTHRIE: We have a Rossen Reports crime alert to tell you about this morning. A new wave of auto thefts that police, frankly, can't figure out. Today national investigative correspondent Jeff Rossen's here with more. Jeff, good morning to you.

JEFF ROSSEN: Hey, Savannah, good morning. This is a real mystery. Look, when you lock your car, and you set the alarm on it, you think your car is pretty safe. But as you're about to see, criminals have designed a new high-tech gadget giving them full access to your car. Police are so baffled, they actually want you to watch this video to see if you can help...

Leo: They've got video. That's the thing.

Steve: Yes.

Leo: Because every garage everywhere has security video now, so they know it's working.

JEFF ROSSEN: Long Beach, California. Watch as this thief moves in.

Leo: So it's a late model SUV.

JEFF ROSSEN: Approaching this locked SUV in a driveway.

Leo: He walks up to it.

JEFF ROSSEN: Police say he's carrying a small device in the palm of his hand. You can barely see it. But he aims it at the car and pops the lock electronically. He's in, with access to everything.

Leo: Oh, look at that. The light comes on. The door opens. It says come on in.

JEFF ROSSEN: No commotion at all.

Steve: Probably a nice little chime.

Leo: No alarm.

JEFF ROSSEN: Then his accomplice shows up...

Leo: Wait a minute, they're doing multiple cars. Holy cow.

JEFF ROSSEN: ...and hits another car using that same handheld device.

Leo: Holy cow.

JEFF ROSSEN: Long Beach Deputy Police Chief David Hendricks is mystified.

CHIEF HENDRICKS: This is bad in the sense that we're stumped.

JEFF ROSSEN: You're stumped.

CHIEF HENDRICKS: We are stumped.

Leo: So we don't have to show the whole thing. What do you think the - what do you think's going on here?

Steve: There's another example.

JEFF ROSSEN: He says it's almost like the thieves are cloning your car remote, which is virtually impossible to do. Here's why: On most cars, when you hit the unlock button, it sends a code to the car. That code is encrypted and constantly changing and should be hackproof.

Leo: Is it a standard rolling code? Or are they doing some...

JEFF ROSSEN: ...figure out a way to crack it.

Steve: It is probably a sequential one-time.

Leo: Right.

JEFF ROSSEN: Jim Stickley is one of the country's leading security experts. He's watched the tapes, and he's stumped, too.

JIM STICKLEY: This is really frustrating because clearly they've figured out

something that looks really simple. And whatever it is they're doing, it just takes seconds to do. And you look and you go, that should not be possible.

JEFF ROSSEN: It's happening from California to Illinois.

Leo: What I want to know is what makes? What models?

Steve: I think he's - he's about to tell you.

MICHAEL SHIN: I felt pretty unsafe.

JEFF ROSSEN: That's Michael Shin. His home security camera caught this crook breaking into his Honda Accord using a similar device. But you'd never know it. He looks like the owner of the car...

Steve: Sure does.

JEFF ROSSEN: ...unlocking the doors remotely and silently. The thief stole cash and an expensive cell phone.

MICHAEL SHIN: It was shocking. It just opens magically without him having to do anything.

JEFF ROSSEN: Adding to the mystery, police say the device works on some cars, but not others. These thieves try to open a Ford SUV and a Cadillac. No luck. But this Acura SUV and sedan pop right open. And they only seem to strike on the passenger side.

Leo: Oh, that's interesting.

Steve: Yup.

JEFF ROSSEN: Investigators don't know why.

CHIEF HENDRICKS: We've reached out to the car manufacturers...

Leo: That's really interesting.

CHIEF HENDRICKS: ...the manufacturers of the vehicle alarm systems. And so far nobody seems to know what the technology is.

JEFF ROSSEN: That says a lot about how sophisticated these criminals are.

CHIEF HENDRICKS: When you look at the video, and you see how easy it is, it's pretty unnerving.

Leo: Well, the criminals probably aren't that sophisticated.

Steve: Exactly.

Leo: But they're probably buying them from somebody who is, obviously; right?

Steve: Yes. There's no chance that these random schmoes who are in stealing people's cell phones and spare change...

Leo: Yeah, they don't look that smart.

Steve: And also no one is actually stealing the car. At the top of the story they called it "car theft," and so it's car contents theft. So this is not dealing with the ignition system, apparently. My theory is, based on looking at the videos, that they're doing some sort of a high-energy transfer, whether it's magnetic or electromagnetic or radio. They seem to have to get very close. No bad guy would want to be in physical proximity if they could avoid it. If this thing worked 10 feet away...

Leo: They'd open the door first, right.

Steve: Exactly. And a radio would allow them to do that.

Leo: So they do have to get right up next to it, it looks like, yeah.

Steve: Yeah. And we know that cars are now covered with microprocessors. And something seems to be about the passenger side. My guess is it's simpler on that side. That is, there is nothing there, no other fancy electronics, not maybe as much as over on the driver's side. Just, I mean, there's probably a network which is connecting to the mechanical door lock there. And so they're - my guess is that this is some sort of a device which is generating a signal that is able to penetrate the relatively thin sheet metal of the car door and confuse the electronics, which is - basically it's a network controller. All of these cars now are based on - we talked about the CAN, C-A-N, network that they run on. My guess is they're just able to, like, overpower the normal signal and say, you've just been told to unlock yourself. And so the door says, oh, and unlocks.

Leo: A lot of cars' alarm will go off even if you just unlock the door.

Steve: Yes.

Leo: You know, if you don't have the right key, the alarm will go off.

Steve: Yeah.

Leo: So they must be doing more than just simply pulling, you know, if you were - let's say somebody left the window open, and you could reach in and pull up the lock on the door and get in. In most cases the alarm would still go off. So they're bypassing more than the...

Steve: Well, maybe...

Leo: They're more than just a magnetic thing.

Steve: It may be an unshielded area where they're able to gain access to the car's network and say, we've just told you to unlock.

Leo: I think it has to be that. Otherwise the alarms would go off.

Steve: And I think, though, that it is the case that our cars are using a non-repeating, sequence-based, one-time passcode. That's what this alarm technology is, which is why thieves even who copy the signal that your key emits can't use it again. It's exactly like our event-based, one-time password system. They're not doing that. This is not a crypto attack. I think it's actually attacking essentially underneath the crypto level at the car's network level. So anyway, I'm on record with my guess. I'm sure in weeks coming we will, you know, sooner or later some guy's going to get caught, and this will get out into the news. I hope that we see a news story, and it's not all hushed up. But as you said, Leo, bad guys are buying this somewhere online. This is coming from overseas, and it's like, oh, get this. And I was reminded of - you've probably seen those generic TV blasters that, like, turn off any model, make or model by sending all the off codes possible.

Leo: Right. I have one of those on the - the Galaxy S4 and the HTC One both have TV, seriously, they both have TV RF remote control devices. And you could pretty much walk into any bar and turn off anything from your phone.

Steve: Probably use IR. IR is...

Leo: That's why I said. What did I say? IR, that's what I meant.

Steve: Yeah.

Leo: Somebody in the chatroom suggested, this is an interesting thought, that it might be somehow related to the setting, and my car has this setting, that automatically locks the doors when you get to a certain speed and unlocks them when you arrive. And if you perhaps had that setting on your car, you might want to turn off that unlock setting.

Steve: Well, the advice is, and at the moment I don't think there's - I didn't have any time to do any research because I just saw - this thing came in this morning. I'm sure before long we will know what makes and models are vulnerable. And the takeaway for the time being is, even more than usual, do not leave valuable stuff in your car because, if you've got a late-model something or other, seems like SUVs and seem to be Asian makes of cars. I think they were Hondas and Acuras and so forth. It didn't like the Ford or the Cadillac for whatever reason. Maybe we just have thicker sheet metal, who knows. But anyway, it'll be fun to see what this ends up - what it ends up being. But, you know, protect yourselves.

So speaking of protecting yourselves, this isn't really news, but I thought it was just sort of an important reminder. The Zeus trojan is still out and about. I was reminded of it by Nicole Perlroth, who writes The New York Times BITS column. And we've talked about the Zeus trojan. That's the banking trojan. Essentially, it seems to be unsquashable. It is - probably because it's just so lucrative. It is backed by, we believe, Russian organized crime bad guys. And it is thriving on Facebook.

Apparently people are, like, posting fake Facebook profiles containing links that install the trojan in your machine. And unlike other trojans, this thing goes stealth until it sees you doing electronic banking to one of a growing number of banks that it, quote, "supports," unquote, in which case it's able to intercept your keyboard and do pre-encryption capture. And we've talked about this in the past. For example, it can even modify the login forms, adding fields like Social Security number, which is not on your bank's normal form for logging in. They add it in order to capture that information because that's valuable for resale for identify theft purposes.

So this is an extremely sophisticated trojan specializing in intercepting banking transactions and then sending this information off to organized crime groups in Russia. And it's on the rise. I mean, it peaked just last month, in May, largely finding, like, its sweet spot over on Facebook. So just to - I don't know how you protect yourself from this except to keep the latest antivirus and maybe just try not to click every link that is offered.

Leo: Usually these Facebooks, they either come in on your wall with a link, or they come in as a message with a link. And a lot of times, I mean, in the past what we've seen is you'll get a message - from a friend, by the way, because it has to be...

Steve: Yeah.

Leo: A friend who has been compromised. And the friend's message will say something like, "Hey, I got video from you last night; oh, man, are you in trouble," and a link. And the link, of course, is malicious in some form. Sometimes what it does is it pulls you to a page that looks like YouTube, but then it says, oh, you need to update your Flash. And then you, because we all see that all the time, go, yeah, yeah, yeah, update it, update it.

Steve: Probably true.

Leo: And of course what you're not getting is Flash. You're getting the malware in a

package that looks like a Flash installer.

Steve: Yes.

Leo: So, yeah, be careful about links. Be careful about installing software from those links, especially.

Steve: Yeah. So the EFF, our illustrious defenders of public trust focusing on the Internet...

Leo: Love them.

Steve: I know. And we got a - they actually pop in here a couple times because they're back taking bitcoin once again.

Leo: Oh, really.

Steve: Yeah, with a really cool story. But this one first really caught my eye. The story was titled, from the EFF, "Computer Scientists Urge Court to Block Copyright Claims in Oracle v. Google API Fight." The subtitle was "Dozens of Industry Leaders Argue APIs That Are Open Are Critical to Innovation, Interoperability." I'm just going to share the story:

"Dozens of computer scientists urged an appeals court today" - and this I think was May 30th, so just last week - "to block the copyright claims over application programming interfaces in the Oracle v. Google court battle," and this is over Java, "arguing that APIs that are open are critical to innovation and interoperability in computers and computer systems. The Electronic Frontier Foundation represents the 32 scientists - including leaders like MS-DOS author Tim Paterson and ARPANET developer Larry Roberts...."

Leo: Tim Paterson's still around, wow.

Steve: Yeah.

Leo: Wow. Wasn't he Seattle DOS, CDOS?

Steve: Yes. That's where Gates bought DOS...

Leo: Yeah, bought it from him, yeah, wow.

Steve: ...from Tim, yeah. Didn't pay him very much.

Leo: No.

Steve: That's another story. Anyway, "...in the amicus brief filed in the U.S. Court of Appeals for the Federal Circuit today. The group urges the court to uphold a decision from U.S. District Judge William Alsup finding that APIs are not copyrightable," which that's good news, "explaining that Oracle's attempt to over-extend copyright coverage in its case against Google was irreconcilable with the purpose of copyright law and the nature of computer science. "'The law is already clear that computer languages are mediums of communication and aren't copyrightable.'"

Leo: Yay.

Steve: Yes. "'Even though copyright might cover what was creatively written in the language, it doesn't cover functions that must all be written in the same way,'" that's exactly the right language, "said EFF Staff Attorney Julie Samuels. 'APIs are similarly functional. They are specifications that allow programs to communicate with each other. As Judge Alsup found, under the law APIs are simply not copyrightable material.'

"Furthermore, as the scientists explain in today's brief, the real-world ramifications of copyrighting APIs would be severe. All software developers use APIs to make their software work with other software. For example, your web browser uses APIs to work with various computer operating systems so it can open files and display windows on the screen. If APIs are copyrightable, then developers can control who can make interoperable software..."

Leo: Oh, I love that.

Steve: "...blocking competitors and creative new products."

Leo: Yeah, yeah, thank you.

Steve: And then again, "'Without the compatibility enabled by APIs that are open, we would not have the vibrant computer and Internet environment we experience today, with new products and services routinely changing the way we see and interact with the world,' said EFF Fellow Michael Barclay." Continuing, "'APIs that are open spur the development of software, creating programs that the interface's original creator might never have envisioned. We hope the appeals court rejects Oracle's appeal in this case to protect technological innovation.'"

And, you know, hear, hear. So what's happening really does upset me because Oracle is trying to close the Java API against Google. Yet the entire value of the Java API has been its openness. The only reason that Java even matters today, that it's on those three billion devices that we keep being reminded of painfully, is because it was an open interface, and anyone could write to Java who wanted to. Now Oracle is trying to say to Google, oh, no. People can write to the API, but we're not going to let you implement the API. They're trying to maintain control of it. And so that's just - that's really bad news.

There, for example, there are - it's like FreeDOS that is a DOS clone. It's completely written from scratch, no Microsoft copyrighted code in there. Yet it implements the DOS API, allowing DOS-generation applications to run just as if they were on MS-DOS. And there's something that's called ReactOS, which is a written-from-scratch Windows API clone that I've been watching for a few years, and it's coming along. And then we have POSIX and the UNIX API. I mean, these interfaces have to be kept available and open. And really it's the creator of it trying to have it both ways. They're trying to create the benefit of the initial openness and then come along later and say, oh, nobody else can use it.

So this is important, and I'm really glad that the EFF is there to establish some precedent. And, I mean, I'm almost glad that Oracle and Google are having this battle now because we do need some legal precedent established, hopefully in the correct direction, going forward. Because what we're seeing is we're seeing that innovation is slowing down. Major organizations like Microsoft and Google, I mean, they've been on the other side of these things, too. And Oracle, they're now trying to use the copyright system and the patent system to obtain material wealth in absence of ongoing innovation. And we need to keep this in perspective.

So we talked last week, one of our top of the podcast stories, I went into detail into the announcement that Google had made about the way they were going to be changing their certificates. And what has popped up on the news, actually Sophos is the one story that I saw, but it looks - I think a number of people carried it, was that my version of IE, IE8, which is the last one I am able to run on XP - now, this is not a big problem for me because I don't use IE. I use my Firefox, or I use now Opera I've really kind of fallen back in love with because it's so lean and mean, or Chrome. I mean, IE is the last browser that I will use. It does not have Server Name Identification, SNI.

And that's that feature - someone tweeted since last week, and I didn't confirm this, but the tweet was that SNI was actually relatively recent. It was added to the SSL/TLS spec in '06, says the tweet. I'm not stating that myself, but that's what the tweet says. If so, it's like well, okay. I guess recent is variable. That's seven years, which ought to be enough. It's not enough for IE, but it is enough for everybody else.

So any state-of-the-art browser will already support this SNI. That's the thing that allows multi-hosting on a single - multi secure hosting on a single IP, server name identification, SNI, where that, as I mentioned it last week, that first packet that the browser sends identifies the site that is the domain name of the server it wants to connect to at that IP. It has to be in the first packet because the second packet, which is the first packet being returned by the server, has to be the certificate for that site. So the browser has to identify the site it wants immediately so that the certificate can be chosen from an array of them that are available to a multi domain hosting server, all at that one IP.

Normally, it's okay to wait until the protocol-level transaction underneath, that is, in the secure tunnel after the SSL/TLS transaction has been set up. Not, however, if you've got multiple domains all sharing a single IP because the server doesn't know which one of the many the client wants. Well, so it turns out XP has no IE available to it which has SNI enabled. But if you're running Firefox on XP or Chrome or Opera, that is to say, anything but, you're fine. And this would only be a problem with this one particular domain on Google. Notice that there's a lot of XP still around. Nobody's running IE later than 8 because you can't. And this doesn't seem to be a big problem already.

So it will start to be a problem for this particular set of people and multi domain hosting, and it just sort of came up because of Google's mention of it. So I'm staying on XP. Actually, when I rebuild my system, I'll rebuild my system, and I will absolutely be

switching to 7. I'm completely comfortable now with Windows 7. So I'll be...

Leo: Oh, aren't you a daredevil.

Steve: I'll be catching up.

Leo: Have you ever used Windows 8 at all?

Steve: Actually, no. I have never touched it. I just know it's bad. Actually I've listened - I've watched you trying to use it. There was that one show with Paul...

Leo: Yeah, Mary Jo, yeah...

Steve: And Mary Jo where you were, you had it, and half of the show was, okay, now, wait a minute.

Leo: Yeah. What, uh, I do what? I did this? Huh?

Steve: I go on the right, and I slide over to the left? What?

Leo: Oh, dear.

Steve: And then I did love - I did love that great - Chris.

Leo: Chris Pirillo showing his dad, yeah.

Steve: Yes. And the dad, very unscripted, finally saying, are they trying to sell Apple Macs?

Leo: [Laughing] I should ask Chris if his dad - what his dad ended up using. That's a good question.

Steve: Never, never had...

Leo: Never, never, never.

Steve: Hopefully I won't have to. I'll just...

Leo: Skip ahead.

Steve: It's the every other OS phenomenon. I mean, they ought to just stop, Leo. Aren't they done? I mean, what more do we need?

Leo: I do wonder, sometimes, if there is - at this point you're changing for change's sake. Now, Office, that happened with Office, like, eight generations ago.

Steve: Oh, yes. When they dropped the menu and went to that whole...

Leo: It's change for change's sake because we have to give you a new version or you won't buy it. Well, there's a fairly significant revision coming in the fall that might make Windows 8 more tolerable. We'll see.

Steve: Is that the 8.1 or Windows Blue or something?

Leo: Yeah, yeah, Windows Blue, 8.1.

Steve: I only know about it because I keep listening to you and Paul talking.

Leo: Thank you.

Steve: And Mary Jo.

Leo: We're glad you do.

Steve: So I just wanted to mention that LinkedIn has finally joined Twitter and Evernote offering second-factor authentication. LinkedIn has had big problems in the past with people hacking accounts. So they've added second-factor authentication. The bad news is, I don't know what it is with Twitter and LinkedIn, that aren't going the right way. Oh, by the way, I've also been loving listening to you loving the whole Google Authenticator style...

Leo: Oh, that's so great, yeah.

Steve: I mean, you know, we talked about it on this podcast, what, six or seven years ago. We were ahead of the game, of course. That's our job. And now here it is in the real world. And, I mean, it is really cool, to be able to bring that up and have these ever-changing numbers.

Leo: Fabulous.

Steve: I just - and so the problem is people are reporting that they're now getting SMS spam after using LinkedIn's second-factor authentication.

Leo: Oh, tell me it isn't so.

Steve: Hey, I know, I know. And weren't you also complaining that there was - I think after you used - you set up Twitter's, and you started getting, like, unwanted stuff.

Leo: Yeah, that's not - and I wonder, it may be the same thing with LinkedIn. What it was is, in order to use Twitter's authentication, you had to register a cell phone number with Twitter. And by default...

Steve: Of course, to get SMS.

Leo: Yeah. And by default, Twitter then starts sending stuff to your cell phone, like messages. And you could turn that off. I just hadn't had a cell phone registered with it yet.

Steve: Okay. Okay.

Leo: And maybe that's what happened with LinkedIn. But that, again, argues for using Google - or not, it's not Google, but using an authenticator, because then you don't have to set it up for a cell phone. You don't have that whole issue. And I'm not giving you anything.

Steve: TOTP, Time-based One-Time Password, TOTP.

Leo: Yeah. And then I could have one app that had it all.

Steve: Right.

Leo: You know, Facebook uses their own authentication built into the Facebook app. That's their way of making you have it. Twitter you have, you know, it sends you a text. It's the only way to do it. I'm not sure what else LinkedIn does.

Steve: Yeah. So I'm hoping that Twitter and LinkedIn will get with the plan. Maybe they just feel that requiring people to have an app is too high a bar, and they just want to ease them into it, figuring that, well, everybody has a cell phone, we'll just send them an SMS message. Isn't that just as good? And it's like, well, okay. The good news is were

moving towards a standard. We're really seeing everyone rallying around.

Oh, and by the way, I had my first experience using Pay With Amazon, worked frictionlessly, a couple days ago. I was very pleased. I went somewhere, it was JR.com, the big electronics retailer. And there it was under their button, was Pay With Amazon. It's like, ooh, cool, let me see how this works. And it was fantastic. It was as good as using the Google Pay service. So I was very pleased with it.

Leo: Makes sense.

Steve: Now, EFF.

Leo: Yes.

Steve: We'll remember with a little sadness back in 2011 they stopped accepting bitcoin donations. And it was - I was only sad because it was them pulling back from - okay. Their feeling at the time as they expressed it was, and we covered this on the podcast, they worried it was being seen as an endorsement of bitcoin. And they felt uncomfortable then making that endorsement.

However, that Treasury Department financial document a few months ago that we also talked about, that we were overjoyed about, that solved their problem. That said to them, okay, users of bitcoins, which is different than people who are exchanges, we know that that can be apparently problematic if you're not official with the U.S. Treasury, that apparently users are okay. So they have resumed accepting bitcoin donations through a service called BitPay, which is one that they have chosen.

Now, the headline was interesting because they said, "This week, the Electronic Frontier Foundation received a generous donation of 726 bitcoins," worth currently $95,000 and some change in U.S. dollars. And then they said, "See the blockchain transaction here." And they gave a link with the whole bitcoin crypto deal at Blockchain.info for the transaction. And they said, "This is in addition to over $7,000 USD we've received through bitcoin donations in the last couple of weeks."

So what's interesting about this is it's their own bitcoins coming back. What happened was, back in 2011, when they decided to suspend accepting bitcoin donations, they had a repository of bitcoins. And I think I remember the number at, like, 37 or 35,000 back then, BTC, which they donated to the Bitcoin Faucet. Just figuring, hey, you know, we're not - we don't feel comfortable exchanging this for dollars. So, but we want to support the community, so we're going to dump this on the Bitcoin Faucet. And we talked about the Faucet back in our original Bitcoin podcast.

Leo: I interviewed the guy who did it. We had a Triangulation episode with him.

Steve: Cool.

Leo: Yeah.

Steve: Yeah. And that was just...

Leo: It was just to prime the pump.

Steve: It was, yes, it was a site you could go to, and it just gave you a piece of a bitcoin. Just like, here, here's a bitcoin, just to kind of get you started so you could kind of see. It was cool. So what happened was there had begun to be a problem with the Faucet and fraud. People were attacking it and trying to pursue and trying to perpetuate fraudulent transactions. So the guy closed down the Faucet. And he said, okay, sorry, but we can't do it anymore. Apparently there's a Minecraft Faucet somewhere. And he gave a bunch of bitcoinage to - he donated...

Leo: Interesting. We're talking about Gavin Andresen, by the way...

Steve: Yes, yes.

Leo: Who's now chief scientist at the Bitcoin Foundation. That's why...

Steve: Oh, good.

Leo: Yeah. He's like the frontman. He's one of the few people who's ever emailed with Satoshi Nakamoto. I think he might be Satoshi Nakamoto in a Keyser Sze kind of way. But I don't know.

Steve: So anyway, so in his distributing funds, the Minecraft Faucet got some. He also kindly paid off some of the major mining groups that took a financial hit during that recent fork in the bit chain where there was that chain fork that we covered on the podcast. He helped to give them some relief. And he gave 700 of the bitcoins essentially that the EFF originally donated back.

Leo: Wow. Gavin. Good man.

Steve: So it's now worth $95,000.

Leo: That's putting your bitcoins where your mouth is.

Steve: Very cool, yeah.

Leo: For him.

Steve: And this is totally random, but I thought it was fun. There is an iPad app, and it's

apropos to the podcast, an iPad app called the iHeart Locket Diary, which the picture is adorable. It shows, I don't know, maybe a six or seven or eight year old youngster, female, a girl, wearing her locket around her neck. This thing produces a coded audio sequence which the iPad can hear and unlock her secret personal diary.

Leo: What? Ohhhhhh.

Steve: And I just think that's really neat.

Leo: [Vocalizing coded audio sequence a la R2-D2]

Steve: Yup. And so it's her little techno secret that she wears around her neck, so very much like an old-style diary key.

Leo: That is so cool. I'm getting one of those.

Steve: There's another button that allows you to hide or reveal your secret writing. So you can press the other button, and then again [vocalizing], and then your writing mysteriously - your secret writing appears, allowing you to hide your annotations from Mom and Dad. So I just thought that was way cool. Just a neat...

Leo: I want.

Steve: A neat, neat application of technology.

Leo: I love it. That's great. That is so cool. I love it.

Steve: I thought you would like that one. And now we have the dumb security story of the week. Arguably, unlocking passenger doors without needing a key or needing some sort of a weird thing might be dumb. This is arguably dumber. This is courtesy of our frequent contributor Simon Zerafa.

This was a posting on a web app security group: "Our state's Governor's Office recently started a health clinic for state employees. This clinic, run by a third party, set up a website to allow users to set up appointments at the clinic and to provide private health information. When setting myself and my family members up, I was startled to receive a warning saying that the password I wanted to use was not available."

Leo: [Laughing] You mean somebody else used it?

Steve: "And I needed to choose another one."

Leo: What?

Steve: "Understand that this wasn't because I failed to meet the password criteria, but because that particular password was already in use." And then he explains: "In fact, I wanted to use the same password for my children's accounts, since they are under age, and I will be setting up their appointments anyway." And it sounds like he chose a very secure password, very random, lots of random gibberish. And so he says, "I entered the same password as for my account," so it accepted it the first time for him. Then he received, he says, "and received this error message, 'That password,' and then it put it up on the screen...

Leo: No. It showed it to him?

Steve: Yes. So they had stored it. They had not hashed it. There it was, "'...is already in use. Please choose another.'" He says, "I raised my concerns about this to the third-party provider, and was told they are requiring 'unique usernames and passwords for enhanced security.'"

Leo: Oh, yeah, that makes it more secure, sure. Especially when you show it to them.

Steve: "I replied that, since the web application is helpfully telling me that a password is already in use, and would also tell me that a username is already in use, I could develop a dictionary attack to build a list of known passwords and known usernames, put the two together..."

Leo: Unbelievable.

Steve: "...and be able to access accounts. This would provide me with Social Security numbers and health-related private information about other users. I raised this issue with our state security officer, who told me that they were told not to comment. Am I out of line here?"

Leo: Oh, wow.

Steve: "I'm a UNIX server admin, not a security pro, so I am certainly not up to date on best practices for web apps. But this 'unique password' idea strikes me as a severe problem."

Leo: It bothers me. What do you think it means? So I don't - what would they be using as a password technology if they couldn't have duplicates?

Steve: Well, okay. They could be using - they're not. They're not doing any of this. But,

like, trying to give them, like, the benefit of the doubt, they could be using a salt and a hash and see a collision of the hashes and then say this password is in use. But again, who cares? They shouldn't care is the point. But we know they're not doing that. Nor are they using a unique salt because then even the same password with unique salt would give them - would not give them the same hash, in which case they could not detect a duplicate password, and passwords would automatically be allowed.

But they're not doing that. And the fact that they are, later, when a separate account is being set up, later - oh, and obviously with a different username, because otherwise you'd be - you would have a username collision. So they are clearly storing the passwords in the clear because that's the only way they could be returning it - well, okay, wait a minute. That's not true. They could be holding it...

Leo: Yeah. They could have run the hash on it, saw the hash collision, and then have just been storing that password because you just entered it.

Steve: Yes.

Leo: And said, hey, you know, this thing, we already have that one.

Steve: So as a user convenience they might have been sending back to you the password you just gave them because there was a hash collision. And so they're saying it's in use. So maybe...

Leo: But what would the harm be in a hash collision?

Steve: None. Zero. Leo, no. I mean, it's, you know, you want, I mean, we know how many people use...

Leo: First of all, they're highly unlikely; right? How likely is a hash collision?

Steve: Well, presum- well...

Leo: I guess for monkey123 it's going to happen.

Steve: Exactly, yes. So the hash collision is as likely as the password being hashed, assuming that they're either unsalted or a static salt and not a dynamic salt per account. It'd be nice, what you'd like to use is like a hash based on the account name, which then hashes the password, and then they're going to all be different. So then you would not detect a collision. And there's no - no one has ever - no one before has ever seen a requirement that your password be unique. Which tells you this not a good idea.

So, yeah, if anyone is listening who happened to have implemented that system or is at the state where this person was, change this. This is bad. And we do know that word of these bad things gets out. I've been very impressed by the response of banks, most

banks, in the wake of the SSL Labs revelation that their SSL security rated an F. Many of them have immediately fixed their servers because it's not hard to do. It's a few minutes of some admin just removing SSL 2 support, which is typically a config file, and moving one cipher up to the top in order to prevent you from having the BEAST attack. No biggie. Just have it done.

Leo: Here's an interesting thought. Somebody in the chatroom said, you know what they're doing? They're using your password as the database key, and they can't have duplicate database keys, so they want each password to be unique.

Steve: Could be. That's, actually, that's not a bad thought. The actual collision creates a technological problem.

Leo: A technical difficulty, yeah.

Steve: Yes.

Leo: Like that. Whatever it is would be bad.

Steve: Wow.

Leo: Unbelievable. Unbelievable.

Steve: So a little sci-fi movie and TV news update. Jenny and I saw "After Earth."

Leo: Oh, boy, are the reviews bad. 12% on Rotten Tomatoes.

Steve: I know. 12%. I think it's a five dot something on IMDB. We didn't hate it.

Leo: Because you missed it. What, did you go? You really went?

Steve: Oh, no, we saw it, we saw it.

Leo: And you didn't walk out on it.

Steve: Knowing how bad it was. The problem it had, I mean, it wasn't wonderful. It wasn't a state-of-the-art killer amazing sci-fi movie.

Leo: This is the Will Smith/Jaden Smith adventure.

Steve: Yes, yeah. And afterwards Jenny was puzzled as to why it had been so roundly hated. And I said, well, what I read, because I read all the hateful reviews first, and the people who most disliked it were upset that there was no surprises. That is, you did know, and this is not a spoiler because, I mean, it spoils itself. You know right off the bat what the movie is about, and so what the kid's mission is, because Dad's legs are broken, and the kid's got to go on a long trek. And so that's the movie. But it was, you know, it wasn't horrible. So for what it's worth, I don't if it's worth what movies cost these days because they're getting pretty expensive. So I'm still liking "Oblivion" as my really, really, really enjoyed it movie of the summer. And I can't wait for "Man of Steel." That's my...

Leo: Yeah, I'm excited about that one.

Steve: Breathless for that one. We also saw "Now You See Me," which was with the magic act with Jesse Eisenberg.

Leo: Yeah, I want to see that. Was that good?

Steve: Something felt missing. I think it's one of those where the movie was too long, and the editors really had to cut out for length. As it was, it was over two hours long. I think it was like two hours and 12 minutes or something. But it was just - it felt kind of uneven. It's like, wait a minute, how did we get here? We just sort of seemed to miss a big chunk. And it was like, yeah, it was okay. Seemed to be heavy on sort of fancy special effects, but light - and, like, just sort of drama and music. I don't know, I was less impressed by it than I was hoping to be.

Leo: Too bad. That sounds like one that I'll wait for DVD.

Steve: I think you can. And I wanted to tell people who have been following this series, "Falling Skies" restarts this weekend, for its third season. And it's one that has held me where both "Revolution" and "Defiance" have lost me. What we're sort of seeing are these attempts at sci-fi where they're desperately trying not to spend any money, and unfortunately they're succeeding, generally. So they're just sort of cheesy. They've got some special effects, but they're not very good. And they're trying to use people who are not - can't act, really, and trying to create drama from the setup.

And, eh, I just - but I'm now watching the end of the second season of "Falling Skies" - it came out on DVD, naturally, just before the third season starts - because I had stopped watching it. But then a review that I read said that, you know, the second season really did pick up and got really good. And I have to say I'm having a hard time not watching it. I mean, I'm really enjoying Season No. 2. So for anyone who may have given up on it, or if you've been waiting for Season 3, I wanted to let people know it is starting. And you can find it at the torrent closest to you, whatever that may be. It's on TNT.

Leo: Or TNT, which is a - isn't that a free channel?

Steve: Yeah. Yeah, it's available anyway.

Leo: Maybe it's a paid cable, I don't know.

Steve: And so rather than talking about SpinRite this week, because everyone knows about SpinRite...

Leo: They'd better.

Steve: It recovers disks and kicks butt and so forth. I just - this sort of just - I was tickled by this because as I was going through the mailbag yesterday, I saw, "Curse you, Steve Gibson." And I thought, well, okay, that'll get my attention.

Leo: Yeah, that works.

Steve: It's like, what? And so he says, "Steve, I'm a constant listener to Security Now!, and I have a bone to pick with you. Back in March you recommended a book called 'The Second Ship.'" And it's like, yes, that's the - I did, I recommended the Rho Agenda, R-h-o. The Rho Agenda is the trilogy. "The Second Ship" is the first of those. I think "Immune" is the second one. Anyway, so continuing, he says, "I had a few extra credits sitting in my Audible account, so I tried it. It was so good, I ended up listening to all three books in a row" - in this case it's r-o-w - "over three weeks of driving back and forth to work. That put me behind in my Security Now! and Windows Weekly podcasts, but it was worth it.

After finishing the third book, I started listening to Security Now! again, and in the next episode you recommended the 'Gibraltar Earth' series of books. I hesitated to try it out of fear of getting further behind in the other webcasts, but figured what the heck. After starting 'Gibraltar Earth' I quickly realized I was going to get further behind in Security Now! and Windows Weekly. The 'Gibraltar Earth' series was great, and three weeks later I finished those three books."

Leo: Wow. This guy listens a lot.

Steve: "I have started back up with Security Now! and, curse you, heard you recommend the Antares Trilogy."

Leo: Oh, no. Antares, yeah, yeah.

Steve: The Antares Trilogy, which, oh, my goodness, that's the next thing I'm going to read. And in my case it's in print. I really miss that trilogy. In fact, I'm going to start soon, I think. He says, "You are killing me. I'm going to resist temptation for now and get caught up on Security Now! and Windows Weekly. Thanks for the recommendations and for making me fall way behind in listening to your podcasts. If you do mention this on the webcast, I am sure I will not hear it for a month or so as I am way far behind and need to get caught up." So Scott Maser is in Colorado Springs, driving to work, listening to the sound of our voices, Leo, and you and Paul and Mary Jo. So once he gets caught up, I do,

Scott, I do recommend, I will say it again, the Antares Trilogy may be better than all those other...

Leo: Really.

Steve: Oh, I - yes. If I were to say, if I were to recommend one book for people to start on, this is Michael McCollum at SciFi-AZ.com. He's there. You can get them in eBook and print, and they're non-DRM'd, which I really appreciate. It's like that's the way he wants to do it. He wants to trust people. They're all now on Amazon, in Kindle format also. And they are all on Audible. When they first began to appear in Audible, someone sent me a note saying, hey, Steve, Michael McCollum's books are appearing on Audible. And I shot a note to him because I edited for him. I was the first person to see his latest book and edited that, and it was actually extremely clean, edit-wise. And so we had a conversation. And he said, yes, they're all, you know, all of my books have been picked up and are going to be converted to Audible. So...

Leo: You know what, they have, because they've got "Gibraltar Earth." They've got the Antares series. Now they also have "Life Probe" (Makers Book 1), "The Sails of Tau Ceti," "The Clouds of Saturn," "Procyon's Promise," "Thunderstrike!."

Steve: So good.

Leo: Eleven books. They've been recording like little demons. Wow.

Steve: If you have time, and it won't upset your podcasting experience, the Antares Trilogy. Is it "Antares Dawn," I think?

Leo: That's Book 1, yeah. It's in my library. You know, I was trying to figure out why the Rho Agenda was in my library, "The Second Ship." And now I realize it's because you recommended it. See, I'll listen to you, Steve. I haven't gotten around to listening to those. Are you ready for some questions?

Steve: Let's do it.

Leo: Let's do it. Starting with Richard Eaton, who says GRC.com is being blocked: Steve, I tried and rejected another VPN solution called Astrill, A-s-t-r-i-l-l. After numerous support emails, finally a level four support rep told me that GRC.com is blocked by Astrill. Thus, if you want to use it with that website, you're going to have to exclude it using Site Filter. Well, hey, at least they give you a way to do that. You can say, okay, I want to see GRC.com. So I had to "de-tunnel" GRC.com. What they are hiding? Actually, the question is, does this have to do with you?

Steve: Okay. So this is relevant not only for Richard but for all VPN users. And I've seen some questions raised about proXPN that is one of the sponsors of this podcast, as we were talking about at the top of the show. What happens when - and this is something

many people, security-aware people do when they're using a VPN. They bring up the VPN, and then they go to check shields. They go to ShieldsUP!.

Leo: Oh.

Steve: At GRC.com.

Leo: Okay.

Steve: Now, when you do that, the IP address that GRC and ShieldsUP! sees is the VPN server.

Leo: It's not seeing you, right.

Steve: Exactly, where your traffic is emerging. Now, what that often means is that there are ports open on that server on purpose. For example, it may also be their web server, so they're using, like, proXPN.com, that may be a server which was also the VPN server and the web server. So, yeah, it's going to have port 443 and 80 and maybe other ports open. Or if it's not a web server, they could deliberately have their VPN client configured to accept incoming traffic on port 80. For example, I'm using that port on some of my IPs where I've got an OpenVPN server present because it is - it's very easy to get out of other networks where port 80 is your destination port. So they could be accepting incoming VPN client connections on that port. Thus it's not a web server. It's the web server port, but behind that is their OpenVPN service.

So everybody who has wondered really need not worry. You'll see that the IP that we're showing is not your ISP's, probably, what is it, 24 dot something or whatever IP that you see if you go to GRC when you're not through your VPN tunnel. The IP that GRC's ShieldsUP! service shows will be the IP of them. And that's what anyone outside on the Internet will see as you because your traffic is being tunneled from that IP. Then it's encrypted and tunneled to your actual IP.

Now, as to why these guys are blocking us, it can only be for this reason, and that is, just tech support. Too many people were asking, hey, why are there ports open when I'm using the Astrill VPN, and I'm going to GRC? Unfortunately, Astrill, instead of, like, I don't know, giving them a notice or something - I guess you really couldn't give anyone a notice, you just have to block them - they've just blocked GRC. So you cannot test your shields. And they figure, well, that's better than having - than worrying people or having the tech support burden. So apparently it's possible to, with that VPN client, say do not tunnel the following URLs or IPs or something. And so that traffic won't go through the tunnel, it'll go direct. And then you're not going through the VPN, and then GRC sees you, not the VPN IP.

But anyway, that's what's happening. It's understandable. It's nothing to worry about because, again, it's not you, your ports being shown. It's the VPN server's ports. And I can see where it could cause a tech support problem. I know, I mean, I've witnessed it confusing people in my Twitter feed who are asking proXPN support people, why are ports open when I'm using your VPN?

Leo: Why, why? Yeah, that make sense. Some other VPNs may do - does proXPN do it?

Steve: Yeah.

Leo: They do, oh. Trevor Green in London, U.K. wonders about SSL Everywhere - or Mostwhere. Steve, I was listening to Security Now! in the archives when you talked about Firesheep - remember that? Those were the good old days - and how it makes session hijacking easy.

Steve: Life was so simple.

Leo: Ha ha ha, those days. We take credit card payments on our website, so our team has implemented SSL encryption everywhere. Enter the SEO guy. Our SEO guy insists we can use HTTP until the user needs authentication, then switch to HTTPS with HSTS for the remainder of the session. Steve, his idea sounds plausible. Authentication cookies are still only transmitted over SSL. But I'm sure I'm missing something. Will his idea work? Why are people recommending SSL everywhere? Is it because it's necessary or because it's simple? And I'm going to add the question, why does the SEO guy care?

Steve: Correct. First, that's one thing that hit me was he said that the Search Engine Optimization person cared whether they were secure or not. Well, maybe 15 years ago. But all search engines can crawl secure pages just as easily as non-secured pages.

Leo: It's not a message to a search engine anymore, oh, don't crawl me.

Steve: Correct.

Leo: Put that in the robots.txt, if you want that. But they're going to crawl into the SSL.

Steve: So, Trevor, here's the reason, and this is important. It is in the transition from nonsecure to secure that games can get played. So if you have a man in the middle, which is entirely possible with HTTP, I mean, the ways to do that are legion. It can be ARP spoofing. It can be somebody with a simple utility in an open WiFi coffee shop network, for example, who's able to intercept all the traffic.

So they're intercepting the traffic in the clear, and they see the page coming where the user wants to log on securely. And since it's over an insecure connection, they simply strip out the S's. They remove the - and the man in the middle removes the "S" from the end of HTTP on all the URLs and even the form submission URL. So the user, who just assumes that they're being provided security, has your site security stripped from it before - and never able to come up. So they get a form, not over SSL, and they fill it out, and they submit it, and all their login information is captured by the guy in the middle.

You have to have security up from the beginning or verifiably before you - with transport, with HSTS style so it can't be removed, well before you start the login process. So it's just better always to have it.

And the problem is, if you ever don't have it, you can never be - you can never get it. So if you ever allow it not be secure, then from that point on, if every interaction is filtered, then normally when you're at a site, like the first person, the first thing someone's going to do is to log in. They're going to log into Facebook. They're going to log into eBay. They're going to present their credentials. Now, maybe here, in this model, it says you take credit card payments. So there's a lot you can do on the site before you switch into that. But it's just safer if you're always HTTPS so that there's no way somebody can wedge themselves in and then strip out the attempted conversion to HTTPS connections.

Leo: Good stuff.

Steve: And what you really want, you want to use that HSTS header and tell the browser we're always HTTPS for the next year. Or whatever. It's like, for a long time. The browser will remember that, and then it helps the user to stay HTTPS. This behavior is quickly becoming the standard. It's going to take a while. It's going to become the standard. You might as well be a leader in that.

Leo: Somebody said maybe because it slows down page loads. That doesn't slow it down appreciably on modern servers.

Steve: No. Again, that's 15 years ago that was a problem. Now it's only the first connection where there is a public key negotiation. All current clients and servers cache the credentials that are established securely so that all subsequent connections come up just as fast under HTTPS as under non-HTTPS.

Leo: And it's not going to add more than a second; right?

Steve: Not even a second. It's not going to add 100 milliseconds.

Leo: Unless you have some crappy server that's way overloaded or something. UWACES - I don't know what that means - in Shanghai, China asks: Are my ShieldsUP!? Hi, all. Long-time listener and, idiotically, a first-time user of ShieldsUP!, your wonderful service. I live in a house with three people and seem to be the only one concerned about security, privacy, and redundancy in our home. In an attempt to help with our technical problems, I started to look into our Internet and realized the tangle of wires kicked under the desk in my dad's office was not the same as the theory I had spent so many hours learning. But I didn't fret. I went to look at your site, and I used the relatively simple, as compared to the jumble of wires anyway, ShieldsUP! service. The result concerned me. The results, your text summary below, showed most ports being closed.

Now, back to the jumble of wires. Here's what we have: a residential gateway for the DSL line, which is connected to a switch, which is hooked to a router for each floor of

the house. Wow, this is elaborate. This is the reason for my confusion: Every router has its own settings for the way that it looks at the WAN. So how do I know which router is the correct one to stealth the ports on, or is it in fact the dinky residential gateway which, by the way, I can't change out? Now, remember, he's in China.

Steve: I know.

Leo: Two ports open, 1,045 ports closed, nine ports stealthed. The ports that were open are 23, which is...

Steve: Telnet.

Leo: ...telnet. Ooh, that's not a good one to have open.

Steve: Not good.

Leo: And 80, which is web surfing. And then a bunch of stealth ports including the SSL ports. Which probably shouldn't be - well, I don't know.

Steve: That's probably ISP is blocking them.

Leo: Oh, that's China.

Steve: Yeah.

Leo: That's China. And of course the NetBIOS, which should be stealthed. What do you think? What's your diagnosis?

Steve: And 21 is FTP.

Leo: FTP, okay.

Steve: Yup, and then he's got the standard Microsoft ports - 135, which is NetBIOS, 137, 138, 139, 445. So, okay. So here's what - I thought this was sort of an interesting configuration.

Leo: Yeah, yeah.

Steve: First of all, so it sounds like there's a gateway, a DSL gateway going to a switch.

And then he didn't say how many floors. But let's say three floors. So, and each floor has its own router.

Leo: Wow.

Steve: And because - and I think that's the configuration because it says each has its own settings for the way it looks at the WAN, which probably means that there are three public IPs, one for each router, rather than, for example, a single public IP on the DSL router. I don't think it's a DSL router. I think it's a true DSL gateway, which is probably just bridging the DSL over to Internet. Then it's switched so it goes to individual routers.

So, UWACES, what you need to do is try ShieldsUP! from each floor. You tried it from apparently one router, and you got a particular set of results which were some concern, and I think should be. You really don't want, if this is in fact your IP and not an ISP that is doing NAT for you, that is, you ought to look to see whether the WAN IPs are public IPs, or are they, for example, 10-dot, or 17, or, I'm sorry, 10-dot, or was it 172 through 17 something, you know, the various private ranges.

Leo: 192.168, you mean?

Steve: There is that also. But there's also a middle-size one that's like one - I can't, it's been so long since I've looked at that.

Leo: Oh, yes, if you get - if you can't - yeah, yeah, yeah, yeah. Unroutable. Oh, I can't remember it, either. But I know what you mean.

Steve: It's like - yeah.

Leo: 172.16 through 30, according to...

Steve: Yeah, there you go, exactly, thank you.

Leo: That sounds reasonable, yeah.

Steve: So if those are the WAN IPs, then your provider is doing NAT, in which case the port 23 and 80 are its ports that are open. But if your WAN IPs are public IPs, routable IPs, then you need to go to each router in turn, run ShieldsUP!, and see what the results look like because then ShieldsUP! will be actually showing you these ports which are open and closed are your router itself. So then you want to go, you want to reconfigure each router, turn off the web server if there is one, turn off the telnet port, basically secure the WAN side on each one. But you will need to do it on all three of your floors since apparently each floor has its own router. And the results you get from ShieldsUP! will probably differ depending upon the router configuration per floor.

Leo: That makes sense. It's the router that you're connecting with at any given time.

Steve: Yes, yes. And apparently his household has more than one.

Leo: It's complicated, of course, because we don't know what's going on in China as far as the Internet access.

Steve: Right, right.

Leo: Sam in Dallas commented about blocking third-party cookies: I'd love to be able to block all third-party cookies (I use Chrome), but it does break some sites. I'm job hunting, for instance, right now, and most companies bounce you over to an external job listing service. Blocking third-party cookies tends to break those. I've tried whitelisting the sites, but there are so many, it's just - it's too much of a pain. Plus, I tend to forget about it and then wonder, why is this site not working? So he's just turning them on.

Steve: Well, this is interesting. I mean, it's unfortunate because we are beginning to see, as we've discussed on this podcast, and I'm promoting it, this default blocking of third-party cookies. Safari comes that way from Apple and always has. And I've always loved it for that reason. And Firefox is struggling with the politics of making that same decision. But it was interesting, from Sam, to hear that he's had experience with some sites that break when he's got third-party cookies disabled.

My take is third-party cookies should have never been. This is an abuse of cookies. This is not the way they were meant to work. They were meant to be a stateful relationship with the site you're visiting. It's a side effect, a side effect consequence of ads that they're able to also use cookies. This was not what cookies were meant for. So unfortunately, because this notion of third-party cookies didn't exist initially, some sites have assumed that they will be enabled, in the same way that some sites are now assuming JavaScript is enabled. And I'm seeing many signs, because of course I run with JavaScript by default disabled, thanks to NoScript on Firefox, I'm seeing notices saying this site only works with JavaScript. Turn it on. And then, if it's worth it to me, I do. It may very well be that we get to the same point where sites begin to say, this site requires that you accept third-party cookies. Please turn them on. And then I imagine at that point browsers will give us a way to do so. So it's really a function of the fact that they've always been on.

And so it doesn't sound like there's a commercial incentive in this instance. If it's some sites bouncing him over to job listing engines, it sounds like it's just they've assumed the presence of third-party cookies, and they're relying on that as some glue between sites, and turning them off is breaking that glue, which they've relied on. And this, you know, it may be the reason that we don't see everybody running with them disabled under Safari. There is a percentage of people using Safari who have turned third-party cookies on, presumably because they found out that they did need them. But still about 80 percent run with them off.

Leo: So I'm thinking about what the scenarios could be that a site could legitimately want third-party cookies. And this would be a very - this one's a good example because you're referred to a job listing site from a - you go to visit a site. You're referred to a job listing site. The job listing site might do something, maybe collect information, and then send you back to the originating site. Is it not conceivable that there would be some third-party cookie exchange here? Maybe the job listing is embedded in the first-party site, that kind of thing?

Steve: Well, the problem is that you don't, you definitely don't need third-party cookies. It was probably just a convenience.

Leo: Okay.

Steve: For example, when you go to the third-party site, the HTTP header, the referrer header, provides any information that the site wants about where you came from, for, like, linking you together. So it's easy for the site that referred you to the third-party site to send you back there afterwards. But they may have chosen to use cookies instead.

Leo: Right. Not necessary.

Steve: So without really digging into the technology, it would be hard to dissect what the problem is. It certainly isn't necessary. It's just the way they chose to do it. And turning it off was, I mean, the good news is, if third-party cookies start being off more and more, the people who implemented the site technology could say, oh, this is generally no longer reliable. Let's do this without third-party cookies. And they certainly can.

Leo: So there's no technical, you can't think of a technical scenario where you'd need third-party cookies for a legitimate reason.

Steve: No.

Leo: Because that's not how cookies were designed.

Steve: Right.

Leo: They were designed to be first-party.

Steve: Yes, they were designed to allow you to maintain a stateful relationship with a site you were visiting. So you could log on and stay logged on, query to query, as you moved through those pages. It was the whole concept of third-party advertisements which were being hosted by the first-party site. Suddenly it's like, oh, wow, those ads are putting cookies on my computer. That wasn't what the guys who did cookies ever intended.

Leo: No, in fact they were very explicit that no third-party could read your first-party cookies.

Steve: Exactly.

Leo: Which I think tells us that the intent was very clear that this kind of thing not happen. Question 4, I'm sorry, 5, Andrew Hallmark in Cambridge, United Kingdom wonders about the Quantum Internet: Steve, I'm a computer science student. When I heard you talking about the problems implementing quantum internet, that's when it hit me: Why can't we use some kind of envelope system that will contain the quantum data, and the only thing the routers will see will be the address on the envelope, thus maintaining the quantum state but still sending it to the right place.

I've no detailed knowledge on physics in general, but I'd like to hear your opinion on this idea since I am currently thinking about starting physics in September.

Steve: Well, first of all, Andrew, go to physics.

Leo: Really.

Steve: Oh, my goodness. I just think physics is so great.

Leo: Me, too.

Steve: I loved it in high school, and at Berkeley I was in engineering physics, which was like the tough one, the Physics 5. And, oh, goodness, it was just a joy. And it's so applicable to everything that we run into later in life. I've really found my interest and love of physics to be worthwhile.

In this instance, what we're dealing with is bizarro physics. I mean, you know, classic mechanical physics is almost intuitive. There is nothing intuitive about physics at the quantum level. It is just insane. And I don't see how it would be possible to create an envelope because we're actually taking advantage of, like, the simplest aspect of the nature of quantum communication, which is the act of observing the quantum data changes it. And that change can be detected.

And so I just don't, I mean, it's an interesting concept, but I think you've formed some semantics that just don't make sense in the actual physical world. This notion of putting an envelope around the quantum data, I don't know what that means. The quantum data is the data that you're transferring, and the whole - the beauty of the elegance is that it cannot be eavesdropped upon. There's no way to - and this was when we were talking about an Internet, it's inherently not Internetable because the Internet is about routing. And the moment you intercept the quantum data, this optical connection, with a router, it is the terminating endpoint. And then you've broken, essentially, your envelope at that point. And you could put it in - you could re-envelope it and send it back out. But then the point is that that router represents a point of vulnerability.

So by all means, I couldn't recommend physics more highly. I think it's, I mean, it sounds like you're a computer science and physics interest, which would be a great combination.

Leo: Long as you got the math.

Steve: Yup.

Leo: Got to have a lot of math for that. Brian Tanner in Southwest Wyoming notes you could store energy by pumping water uphill, too. And I think I was referring to that when I was talking about the old school methods. This isn't the one I've seen, but it's the same idea, and he points us to a website, ConsumersEnergy.com.

Steve: I tweeted the link to this earlier [bit.ly/1b4psXV]. So if anyone's curious, you can look at my Twitter feed, Twitter.com/SGgrc. I really like this, Leo. It's just it's a large reservoir deliberately elevated above Lake Michigan.

Leo: You pump it up, the water up into there.

Steve: Yeah.

Leo: Using energy. And that's - the energy's reclaimable when you let the water flow back through.

Steve: And did you see the diagram down below, where...

Leo: Oh, yeah, there you go.

Steve: Yeah, it's just beautiful. But, I mean, it's able to supply energy for 1.4 million people, generates some huge amount of gigawatts of power. I was just stunned. There's, like, eight pipes that come down from above, from the elevated reservoir, that are 24 feet in diameter. You could drive a semi through any of these eight pipes. So massive water flow to spin turbines, which run generators, which then double as motors. And so during the night, or at off-peak times, they use power which is less expensive to pump, basically to pull water out of Lake Michigan and pump it uphill into this huge ecologically friendly reserve, essentially. And then, during the summer months, during peak energy use, when energy is more expensive, they minimize their external energy consumption by allowing the water to run back downhill.

Anyway, I thought it was obvious. But this is just really, really elegant. I was, as I looked at the page and read more about it, it's just like, well, this is just beautiful. Sadly, it was done back in 1969 to '73, this whole thing was constructed. And you just don't see us doing things like that these days because they're expensive. And this is just - it's beautiful and elegant and, you know, bravo. And I did get some other tweets from people who saw this tweet and said, oh, yeah, we've got one around the corner from us. So they

do exist in various places.

Leo: Sure they do, yeah.

Steve: But I just wanted to sort of point it out. I thought it was very nice.

Leo: Neat idea. Andrew McGlashan in Melbourne, Australia wants to talk about - and worry about - BitTorrent Sync some more. He says: Here's my problem. Any newly created generation of a standard user-generated secret may collide with any other existing secret and, depending on how well they are generated, may collide more frequently then would be predicted assuming 100% entropy. And for a breach of privacy you don't need to find any one specific collision, you just need any collision.

If someone else recreates the identical secret, they will see the collision and be able to see your files immediately. You'll get no notice. You have to watch all connections to your machine constantly to see the new connection - too late, your files are owned. Sure, finding someone specific's target secret is virtually impossible. That depends on good secret creation, of course.

Now, just because it's likely to take a zillion years to guess your target secret, it can occur on the first try. At least for additional security you can use 40+ Base64 characters if you choose. So I'm advocating for an option to unlock to allow new connections. You monitor for the new connection - that's a good idea, actually - and accept it by arrangement. The other end gives you another secret, and you store that to allow both the original secret and the special access allowed secret to connect to your sync. Then you relock the system to only allow those that have already been granted access.

This actually is a clever addition, if you're worried about this. This way, you can vet every new possible connection, one at a time, in a very secure fashion. No one can gain access to your shared sync without you accepting them deliberately, and your own secret becomes very, very private indeed. No one seems to get this. It would make the whole sync situation secure. Without the lock/unlock option, you have no real choice other than to make sure that you encrypt everything yourself before you place it in your sync folder. A TrueCrypt volume will suffice, if well secured.

I fully understand that, if you find a physical house key at a major train station, it would be futile to try that key in every house lock until you found one that opened. But that's a different problem, and house keys only have so many tumbler combinations. In the house key scenario - we don't have to go on and on about the house key.

Steve: Yeah.

Leo: Because it's completely not analogous.

Steve: Okay. So...

Leo: What's your answer?

Steve: So Andrew is among the people who are unnerved by the idea that nothing protects them other than that no one has guessed, they hope, their BitTorrent Sync secret. And the fact that there are three times 10^50 possible secrets doesn't put them off any. They say, well, but what if someone did guess it? And it's like, okay, I mean, there's no arguing that. And first of all, we're still waiting for the protocol disclosure. There does seem to be additional bits. Somewhere they're using 256. It seems that 168, I think that was the number, come from the user-provided key, but the balance of those making up 256 come from somewhere else. We don't know where else.

So I'm still feeling it's a little premature to, I mean, we really can't audit the security of BitTorrent Sync until we have the protocol. And we do not have that yet. All we have is them saying, this is in beta. Here it is. Have fun. And I think it is, given that you've got good entropy, and he says, yeah, but what if you don't, it's like, well, yes. If everyone uses the same key, then that's a problem. But we're not arguing that.

And notice that, if you - the problem with the lock scenario is that somebody would try to use a key, and they wouldn't be able to because they would be told that, well, sorry, that network is locked. Well, now they know that there is a network at that key. And then they have to just keep trying it until they find it unlocked. And then you're back in the same situation. So, I mean, the truth is it's larger than three. I think it's 3.1 or something times 10^50. And remember that was - you only needed, well, anyway, we talked about the number of molecules in the universe.

Leo: It's hard to figure out, yeah, yeah.

Steve: All that. It's just it's a ridiculously large number. It is never going to happen. Never, never, never. But people just cannot be comfortable with that. It's what I'm seeing. And so I almost agree that - and even as you were reading it, this lock/unlock thing made sense to you. It felt - you were more comfortable with it.

Leo: You just do it because it gives you...

Steve: Yes, I think from a psychological...

Leo: People aren't going to adopt it from a psychological point of view. People don't understand the math.

Steve: I think that's the case. From a psychological standpoint, it's just - it unnerves people that there isn't a separate username and password. We like username and password, rather than just a really monster long password that is both.

Leo: The BitTorrent Sync guys are just obviously too attached to the cleverness and elegance of their solution and not recognizing that normal humans might just want

something else. But you raised a very interesting point, which is it does send a signal: There is something here. It's locked.

Steve: Yes, yes.

Leo: So that, I mean, I think it makes it less secure. I think that that's the truth of it.

Steve: Yes. And the fact is, how do you do this without any central management? That's the problem. The reason username and password works is you're always - there's a central manager. And we know how well that works.

Leo: Yeah, yeah.

Steve: Because, I mean, how many passwords are being blown by a hash...

Leo: Do you think that this could be a system used more widely? I think that people, look, people don't understand probability. So it's going to be something that bothers people. There's no way around that, even if they understand the math, and even if the entropy is very, very good indeed.

Steve: I actually agree that, I mean, okay. Am I using it? No.

Leo: Oh. Why not? Because you haven't vetted the protocol, yeah, okay.

Steve: I haven't vetted the protocol. We have to have the protocol vetted. But the notion of sharing TrueCrypt volumes, now, that makes a lot of sense. Share that rather than naked files. If you're not that concerned about security, or you're only sharing your cat videos, then fine. Just put them up there. But if you've got the keys to the kingdom, pre-encrypt them. Pre-Internet Encryption, PIE, is an acronym we've been using here for years. And I would say that makes sense. Use this as your glue, but don't trust it for your security.

Leo: Yeah. Adrian Justice in Phillip Island, Australia - another Australian - shares his experience with advertising plugins: Steven and Leo, thanks for all the effort you put into producing a fantastic podcast each week. I was put onto the show by my dad during my final year of high school - what a smart dad - which led me to study security at a university level, courses that reference Security Now! almost on a weekly basis - all right - whilst working at my local computer store.

A few months ago a customer came into the shop with their laptop, complaining about advertising on the Internet. We explained to them, hey, this is how Internet-based businesses make money. That was fine until they mentioned that our own site

contained advertising, which, by the way, is not true. Our site's always been free of advertising. On review of the laptop we noticed hyperlinks embedded in the body of the page - we talked, we had somebody with this problem last - couple of weeks ago.

Steve: Yup.

Leo: Which, when hovered over, displayed a popup with advertising for products related to the highlighted word, as described by a listener in SN-405. After browsing around to other reputable sites, even Google, we found similar links everywhere.

We managed to narrow the cause down to a plugin in Firefox, which was, by the way, the only affected browser on the system. When we removed the plugin - I don't recall the name, sorry - the mysterious advertisements disappeared. We have since seen similar plugins for Chrome. Thanks again for the great podcast. Adrian Justice, Phillip Island, Australia.

Steve: So I appreciated that because we were hypothesizing a malware installation, and this confirms it. We didn't know for sure. We knew that there were sites that, from our own experience, that were using links, like they were hosting ads themselves in that fashion, which I find really annoying, and you've indicated you had the same feelings. But clearly there is malware which can do this, too. So that is, I think, what was affecting the Chrome user whose question we talked about two weeks ago. Adrian confirms that he saw it in Firefox and in Chrome. So it is something icky that you can pick up in your browser.

Leo: Yeah. And it might not be you got infected. It might be you installed, I don't know, Java, and along with it, because with Oracle now it encourages...

Steve: The spiffy search bar.

Leo: Yeah, I think they install Ask Toolbar.

Steve: Yes, Ask, yes.

Leo: That, whenever you install that shareware, and it quickly went by that they, yeah, we're also going to install a very handy little tool that'll let you - I think I've even seen it as a, not as malware, but as a, you know, like an ad plugin. Ads Plus browser plugin, somebody said. Maybe that's it. Ads Plus is the software that websites use.

Steve: Oh, no kidding. Ads Plus.

Leo: So maybe they distribute a plugin.

Steve: Wow.

Leo: Oliver Stengele in Heidelberg, Germany - gosh, I love the international nature of our audience. I just love that. I come to you with a disturbing topic from the battlefield between technology and politics: 'Net Neutrality. A few weeks ago Deutsche Telekom published their plan to throttle the bandwidth of DSL connections after a subscriber's preset monthly volume has been exceeded. Oh, yeah. You may recognize this from your 3G data plan. However, a few select services like their own IPTV or certain music streaming services would be excluded. Ah. That volume wouldn't count towards the monthly cap. Their bandwidth would remain unthrottled no matter what. This, of course, violates the concept of 'Net Neutrality and either forces volume-intensive services to broker deals with Deutsche Telekom or to suffer and wither. The resistance to these plans already is underway with an ePetition to the German Bundestag which reached the quorum of 50,000 signatures in only three days.

Steve: Good.

Leo: Yeah. The ePetition remains open for signatures from German citizens until June 18th. That's good. That means people are aware of the issue. I think Neelie Kroes, who is the privacy minister for the EU, has also just in the last couple of days proposed regulation, EU regulations to protect 'Net Neutrality. So there's certainly awareness about this issue.

Steve: And it's growing, and it's good. The one thing I wanted to comment is that when he mentioned that, for example, their own IPTV services would be excluded, one thing that typical users don't appreciate, only because they've never been in the posture and the business position of an ISP, is that not all traffic is priced the same.

Leo: Right.

Steve: That is, an ISP's own traffic does not cost the ISP anything because ISPs typically pay for transit across their boundary. So external services are creating bandwidth that they're - and, see, the ISP is buying bandwidth from a Tier 1 provider. And so, depending upon their relationship with the Tier 1 provider, if they're able to say, well, we're only going to need this much bandwidth in aggregate for all of our uses in a month, the bandwidth that they source themselves is free to them; whereas the bandwidth that their users want from outside their bounds is not free to them. So there is that. I'm not, certainly I'm not defending the lack of 'Net Neutrality. I really think we need it. But underlying this is an economic aspect that the bandwidth is not the same whether it comes from the ISP or from extra-ISP sources. Endogenous or exogenous.

Leo: Actually the Neelie Kroes proposed regulation, in fact it addresses this

specifically. Thank you to Nerve, who sent me this article from ZDNet yesterday. Online throttling and site-blocking will be outlawed in Europe under a 'Net Neutrality plan.

Steve: Nice.

Leo: So they are addressing this.

Steve: Nice. So they'll just have to - the ISP will have to factor it into their pricing model.

Leo: Yeah.

Steve: And no longer say, oh, well, we're going to allow these and not those.

Leo: I think the real issue - you're absolutely right, there is a real cost to stuff that comes outside their network versus stuff in their network. The real issue is it's just a great temptation for an ISP then to use that as a way to promote their own business at the cost of a business like ours.

Steve: You're right.

Leo: Because we sit on the other side of that wall.

Steve: Yes. Huge temptation.

Leo: And you set those caps low enough, suddenly, oh, well, I guess I'll just watch TV from my Deutsche Telekom account, or I'll listen to music from Deutsche Telekom. And so it does in fact impact outside businesses. And that's the whole point of 'Net Neutrality.

Steve: And the fact is in many environments there is not much choice of ISP.

Leo: Absolutely. Certainly here in the U.S.

Steve: I have no choice, yes, I have no one to use but Cox for my cable modem. I have no choice whatsoever. And so that's the problem is that, if you don't, if there's no competition among providers, then they have a captive market that they can screw with any way they choose to.

Leo: The waters are muddied because, unfortunately, and it's certainly true in the U.S., and apparently as well in Germany, the Internet service providers are not pure utilities providing you with a pipe to the outside world. They are businesses. They're Comcast, you know, or Cox, which primary business is selling content. So that's the problem. You have to kind of say to these pipes, hey, if you're going to be a pipe company, at least that part of your business, you cannot favor the other part of your business.

Steve: Leave the pipe alone.

Leo: Right. The pipe's got to be neutral.

Steve: It's got to be a content-neutral pipe.

Leo: Right. And that's where it gets very complicated. Because you're making - the argument you just made is exactly what these ISPs say. But it costs us more to give a treat to your viewers than it does for us to show them the German programming.

Nick Donnelly, our last question. He's in London, although - actually he's a Londoner in Saigon.

Steve: And I think we have to have heard from him recently because that seems familiar.

Leo: Yeah, it does. He might have been in the studio, actually. Anyway, Steve, thanks for the explanation on the BitTorrent sharing service not being brute-forceable. I'm getting more excited about the potential of BitTorrent Sync all the time. I also heard your piece on the Marks & Spencer customer having one of their cards debited by the supermarket even though they'd never taken it out of their bag. While this is inconvenient, isn't the bigger horror here that someone malicious with a contactless payment reader could walk around a street stealing hundreds of card numbers in a couple of hours? Even if it's a low limit, the fact it can be read at all at such a long distance and doesn't always require a PIN must make this payment format largely untenable from a security standpoint. Here's hoping neither you or Leo have a stroke on this week's show. Thank you. I think so far...

Steve: We've made it to Question 10. There's been no slurring or blurring of words. So I think we're in a good shape so far.

Leo: We've survived.

Steve: Yes. And I think Nick is exactly right. I mean, it is a - it's horrifying. We have evidence from that report that cards were debited before the user entered the PIN for a different card. So even if the PIN were the same, the debiting preceded any action that they took, which absolutely says you've got - you have NFC, near field communications,

embedded cards that will function at sidewalk passersby distance.

Leo: Yeah, that's not good. That's not good.

Steve: And that is horrifying.

Leo: Yeah.

Steve: So, Nick, thank you for bringing that up. I should have said it myself. But I was so caught up in just reading the story that I didn't add that. But absolutely, I mean, that is - people will remember that I was advocating a brief microwaving treatment of your card. I'm not sure that you want to do that.

Leo: They pop.

Steve: But send it back to your provider and say, no, send me one without this fancy...

Leo: This is why these smart cards have never made it in the U.S.

Steve: Yeah. It's not good.

Leo: But all they have to do is require a PIN for all transactions, and you're done. Right?

Steve: I don't like that, Leo, because, I mean, I don't want any - just why can't we just have little gold contacts where you just stick the card on a reader or something?

Leo: I see, yeah.

Steve: I know how magic radio is. Radio is just bad. We don't even - we don't yet know how the bad guys are opening those car doors, but it seems to be some radio-like - it's either high-power radio or high-power magnetic, which is confusing the car's network, I think, and saying, oh, look, I'm supposed to open now.

Leo: Radio is dangerous.

Steve: I can't wait till we find out. Radio? Radio, look at, I mean, how many times are we talking about security aspects relating to radio? It's just scary. Lord knows Google got into trouble with radio.

Leo: [Laughing] Steve Gibson is the Explainer in Chief. He's at GRC.com. Go there. And he didn't mention it, but do buy SpinRite, the world's best hard drive and maintenance utility, great for recovery, too. GRC.com. While you're there, lots of free stuff like ShieldsUP!, Don't Shoot The Messenger, Unplug N' Pray, Password Haystacks, so many great utilities, and lots of great conversation. If you have a question for future episodes, GRC.com/feedback is the feedback form. Don't email Steve. GRC.com/feedback. He won't even see your email. He obfuscates it.

Steve: I don't have email.

Leo: He doesn't have email. So just - but you make it very easy, GRC.com/feedback. He also has 16Kb versions of the audio of this show for people with bandwidth limits. He also has transcriptions that he pays for. Elaine Farris does a great job with those. So you can read along as you listen. We have bigger audio files, higher quality audio files, and video available at our site on demand, TWiT.tv/sn. Or you can always watch live. I mean, it's fun to have people watch live. We pay attention to the chatroom. You can do that by watching Wednesdays, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 19:00 UTC, on TWiT.tv. That's our website for the live streaming. That's it for this week, Steve. Have a wonderful week.

Steve: I'm not sure what's up for next week. I've got a whole bunch of topics, and we'll see if maybe something will come up in the meantime. Otherwise we'll grab a topic which is needing some attention. And that'll be what we talk about next week.

Leo: And there's sure to be one, so tune in.

Steve: Oh, yeah.

Leo: Each and every week. And thank to all the professors and educators and teachers who use Security Now! in their classroom, in their curriculum.

Steve: Yeah, really.

Leo: I think that's great. I just - it makes us feel really, really good to know that we're this kind of value to people. That's the mission. So I'm glad - mission accomplished, Steve.

Steve: 407 episodes and counting. 408 next week.

Leo: What a body of work you've created.

Steve: We've done it.

Leo: Yeah, it's nice. Thanks, Steve.

Steve: Thanks, Leo. Bye.