Listener Feedback #177

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-428.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-428-lq.mp3

SHOW TEASE: It's time for Security Now!. Yes, we have security news. Steve Gibson has the latest. And then we'll answer questions, a lot of questions about this new CryptoLocker virus, coming up next on Security Now!. Steve's got the answers.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 428, recorded October 30th, 2013: Your questions, Steve's answers, #177.

It's time for Security Now!, the show that protects you and your loved ones online - your privacy, too - with this guy right here, the Explainer in Chief, Steven Tiberius Gibson. Hello, Mr. G.

Steve Gibson: Yo, Leo.

Leo: Yo, yo, yo.

Steve: We have a Q&A finally. Finally the universe has allowed us to actually respond to listener questions, although we've actually been doing that all along because our listeners sort of guide what we talk about based on what they're interested in. But we're incrementing the Q&A counter officially to 177.

Leo: So we're back on mod 1.

Steve: I don't know what mod we're on. But we're - even episodes are now Q&As,

until...

Leo: Oh, this is an even episode. So we're mod 0.

Steve: I think we are. I don't know.

Leo: I don't know.

Steve: Yeah, we're even parity.

Leo: Hey, a programming note before we get to - we've got security news. We have questions and answers. But we are...

Steve: Don't panic, anyone, though, because it's for 2013.

Leo: This is not till next...

Steve: Oh, wait. No, 2014.

Leo: Yeah, you and I both are finally figuring out that the year is now 2013.

Steve: Can you believe tomorrow's Halloween? It doesn't even feel like tomorrow's Halloween to me.

Leo: Happy New Year. I don't - it's still, you know, New Year's Day.

Steve: Completely out of touch.

Leo: So can you believe, first of all, that we're going into 2014. Now, here's a little tip for you youngsters. When you get old, and you remember years like 1982 vividly...

Steve: Fondly.

Leo: ...as an adult...

Steve: Or '73 when you graduated from high school.

Leo: A good year, '73. Those were the days, my friend. When you say "2014," it sounds like you're living in the future. Right, John? John says so, too. So we're going to 2014. As of, now...

Steve: The 6th.

Leo: The 6th because, yeah, January 6, 2014, this show is moving. Don't panic. I know that you may have conflicts. That's why we're telling you now so you can rearrange your life to fit our new time. We are moving the show. A number of shows are moving because - and I'll explain why. It's not Steve, it's me. It's not you, it's me.

Steve: Yeah.

Leo: I wanted to get two days off in a row. I haven't had that in, like, a long time. I wanted, in effect, a weekend. I can't, I always work weekends, but at least I can get a Thursday and a Friday off. So we're moving shows around so that I will be working now Saturday through Wednesday will be my five-day week. And so in order to do that, Steve has very kindly agreed to juggle his schedule a little bit. The full schedule's on our blog, inside.twit.tv. Security Now! will now be Tuesdays at 1:00 p.m. Pacific, that's 4:00 p.m. Eastern time, that's 21:00 UTC, starting January 6th.

Steve: And it's good for me. One of the - when I was talking to Lisa about this, she was initially proposing Monday. And for me that was a problem because I often do so much prep for the podcast that that would have sort of messed up my Sunday because I would be worrying about the Monday podcast on a Sunday.

Leo: Yeah, I didn't want to do that, yeah.

Steve: And so, anyway, by putting me to Tuesday at 1:00, it gives me, essentially, all of Tuesday up until the podcast. So I get two more hours on the day of the podcast.

Leo: Oh, good. Oh, good.

Steve: And so I think what I'll end up doing is just, I mean, I worked on the podcast all this morning, and because it was a Q&A, I figured, okay, I can get it all done in just one day. But sometimes I start the day before. Certainly when I'm doing new heavy content stuff I'm researching it often for days leading up to the podcast. So this is good for me. So 1:00 p.m. Pacific time on Tuesday. So a day earlier and two hours later.

Leo: And there are a few other shows moving. You can see the entire schedule, as I said, at inside.twit.tv. None of this happens till next year, till 2014. And the other advantage, if you don't watch live, you'll get the show a day earlier for download.

You'll get it now on Tuesday afternoon or Tuesday evening instead of Wednesday afternoon or evening. Yes, the Google calendar will adjust, of course. If you download or subscribe to our calendar at TWiT.tv, it will automatically adjust for you. Most of the shows are not changing. Tech News Today is not moving. TWiT's not moving. The Tech Guy is not moving. But a few of the weekday shows are moving around a little bit. And almost all just my shows. But thank you for being - accommodating that. And I apologize to anybody that that's messing with your schedule. We don't like to do this, and we won't do it again, but having Thursday and Friday off will be a boon for me.

Steve: And really you don't do it often. I think we've made one change to me in eight or nine years, so...

Leo: Well, I know people want consistency. And there's no reason to change it willy-nilly. But we want to have it. If you go to January 6th on the Google calendar, it actually apparently is already changed. Thank you, Replicant. So, that out of the...

Steve: With that bit of programming note...

Leo: Yes. What are we doing today?

Steve: We have a Q&A. We've got eight questions because I try to balance the length with the question count, and a lot of this is retrospective to last week, following up on various topics from last week. Lots of interest in CryptoLocker, of course, which we talked about also last week. I've got feedback from people who have been infected and recovered, recovery stories. There are remediation tools. There's a great page with great information. I was tweeting a lot as I was putting things together so that I would get this out into my Twitter feed. So just lots of great stuff to talk about.

Leo: That is very timely. And I'm glad to hear there is remediation.

Steve: Yeah.

Leo: Steve talked about this, of course, last week. We had him on the radio show because we wanted to unwashed masses to hear this. I'm sorry, I shouldn't say that while you're having a cup of coffee. Almost got you...

Steve: I didn't spit it out. I know you well enough to know...

Leo: You knew it was coming. And then we also put it on TWiT. So I think we did our best to get the word out. And I hope we've succeeded on that. Anyway, let us, you know, I just - it makes me - I swell with pride to see people who have - and you have this experience, I'm sure, people come up to you all the time and say, "I

watched you, and I got inspired, and I got into the business." We have classrooms that use Security Now! for curricula.

Steve: Yeah.

Leo: We have people come up all - and I still - people come up and say, "Look at me." I say, "Yeah? Okay." "I've lost 50 pounds thanks to Steve." So it's weight loss and security.

Steve: We got you covered.

Leo: We got you covered. So what's new in security news?

Steve: We're going to keep you alive longer, and we're going to make sure you're safe while you're...

Leo: Yeah, we can't afford to lose any fans. We want you all to live a long, long time.

Steve: So I picked up on a little tidbit that somehow escaped me until I was doing some background research on yesterday's release of v25 of Firefox. Somehow I had missed the fact that they update Firefox every 42 days.

Leo: That's funny.

Steve: Isn't that hysterical? I love that.

Leo: Geeks, you gotta love 'em.

Steve: Uh-huh. And of course everybody knows what 42 is. That's just not a random number. That's an important number within our culture.

Leo: Absolutely.

Steve: And so what this means is that they're constantly moving the code forward. And essentially they do a stable drop of where they are every 42 days, increment the major version number, in this case from 24 to 25, and say here's what's new in 25. Now, in this case there's one interesting set of improvements that our listeners will really care about a lot. They fleshed out the Web Audio API. Basically they're sort of continuing to move Firefox forward in standards, just like the big web standards. So the Web Audio API is now complete. And apparently that is of most significant importance to gamers. This

allows a fully web browser-based, real-time audio gaming level experience, just using the native browser, with no third-party plugins or extra, outside-the-browser paraphernalia required. So that's one thing.

Also, I had noticed that the Find window, when you want to find text on a page, that when you change tabs, the Find window stays, which I guess is useful to some people who want to find the same thing across pages. But the Mozilla folks felt that that wasn't the typical case, so now Find is no longer shared among pages. Oh, and then also, if you've been gone for, like, if you've stopped using Firefox for months, and then you come back to it, it now knows that. And it says, oh, welcome back. And it assumes either you've been on a long vacation or you went off, I hope not to Internet Explorer, maybe to Google or Chrome or Opera, who knows where. But anyway, for whatever reason, you've fired Firefox up again after some length of time away. And so it greets you, says welcome back, and offers to re-import another browser's history and settings into itself in case maybe you've made changes wherever you were, you've made changes and you want to update Firefox to make it the latest and greatest.

The feature that I think is most interesting is that v25 - which anyone can get just by opening up Firefox and going Help > About. And when you open up the About box, that seems to trigger its self-check. And it says, oh, and then immediately starts downloading 25 if you were on 24 or earlier. They have made more of the critical security information available to plugins. And, for example, there's a plugin called Calomel, C-a-l-o-m-e-l. It's called Calomel SSL Validation. And they posted on their blog relative to, or in the updates for their add-on, relative to their Calomel SSL Validation add-on for Firefox, under Update No. 2 they said: "Firefox 25 now allows the add-on to query the full cipher suite. We have added the ability to grade the connection on each part of the cipher including key exchange, signature, bulk cipher, and message authentication code." So Firefox 25 gives them visibility into the fully granular handshake and crypto status of your connection to the server. And so they said: "We also check and grade the cipher if it supports Perfect Forward Secrecy (PFS)."

Leo: You know what Calomel is; right?

Steve: No.

Leo: It's a fungicide and insecticide. Mercury chloride is called "calomel." Whoa.

Steve: Okay.

Leo: It's good, it's actually a great name.

Steve: So, yeah. So if you get 0.64, their version 0.64 for Firefox 25, you get this extra stuff that Firefox 25 now offers. And I think that's cool. That'd certainly be of interest to our users. One thing they did that I'm a little curious about is they said in their notes that resetting Firefox, which I assume means restarting, no longer clears browsing session. And they said that - so I'm assuming that that means that session cookies span resets. Which is - I guess that means that closing the tab is now what causes session cookies to be removed. But closing the browser and restarting it, which reloads tabs, apparently now in v25 deliberately retains session cookies.

So I guess that's okay as long as people understand that. That does represent sort of a stretch, but I can see where, from a usability standpoint, they wouldn't - so the idea would be that, like, it wouldn't log you out of all of your ongoing sessions if you closed Firefox and restarted it immediately, or reset Firefox, whatever that means, as opposed to manually closing a tab, closing a window, which then would clear the session cookies for that session. So it's like, okay, that's an interesting change.

Also, what we've had on the desktop since v23 of Firefox, Android now gets, and that is guest browsing support in Android. So people who are for whatever reason not using Chrome, which would seem to be the default browser in Android, if you are using Firefox, then now there's guest browsing where you can prevent anyone who's borrowing your tablet from seeing anything about your browser history. It locks that and creates a brand new personal state for the browser which the guest then uses. And when that's closed, everything, all of that is flushed, and your default browser state is restored. So that's there. Oh, and also mixed content blocking. We've had that for quite a while on Firefox, and now Android also has that, where you'll be alerted if there's any sort of mixed content games being played.

Leo: You mean reset or restart?

Steve: Okay, what is reset? Is there a reset Firefox?

Leo: I don't know. The chatroom is asking that. I think most browsers have a kind of reset, clear everything. I don't know what Firefox might call it.

Steve: Yeah, I don't...

Leo: But you're saying "restart," is what you're saying.

Steve: Yeah, I'm assuming that if you just close it and then restart it, it does come back with all the tabs. And apparently now session cookies, which are typically how sessions live, you won't be logged out of all of the sessions that you were logged into across a restart of Firefox, whereas before you were.

Leo: The chatroom tells me that there is a - the way to reset in Firefox, and this is actually a very handy thing to know, is if you go to about:support, there's a big button that basically says go back to your initial installed state.

Steve: What?

Leo: Yeah.

Steve: No, that can't be what they mean.

Leo: Reset Firefox to its default state. If you're having major problems which you can't resolve, start fresh with only your essential information. Oh, I guess it does preserve some information. That's in about:support. That's a handy thing to have. But that's not germane to the...

Steve: Yeah, that seems, like, aggressive, yeah.

Leo: That's if you've got a real - there's a plugin...

Steve: Somebody's really gone wonk...

Leo: ...crashing you or whatever, yeah.

Steve: Yeah. So Bad Idea of the Week, Leo. Now, maybe of the year.

Leo: Ooh, this must be really bad.

Steve: This generated so much upheaval among our listeners. And you probably could guess what this is, or you'll maybe agree, or it must have crossed your radar. LinkedIn has decided that they want something called - they want to offer a new service called Intro. With LinkedIn Intro, you deliberately let them proxy all of your email. It's just unbelievable.

Leo: So you send your email to LinkedIn?

Steve: No. You give them all of your login information so they pull all of your email for you.

Leo: I know it's a bad idea, but I do that myself with TripIt, for instance, and a number of places. I allow them access to Gmail so that they can look for reservation information and stuff.

Steve: Okay. Well, in this case...

Leo: It's a terrible idea if you don't want them to get your email.

Steve: Oh, well, I mean, it's - actually, it turns out it can officially break attorney-client privilege.

Leo: Oh, yeah, sure.

Steve: I mean, it, like, does all kinds of bad things.

Leo: Yeah, don't do it if you're an attorney.

Steve: So then you get - you then pull your email from them.

Leo: Oh, no, I don't do that.

Steve: Okay. But that's what this does. They modify your email. When they recognize people within LinkedIn that are sending you email, they add their content to your email, saying, oh, this is this person.

Leo: Here's what we know about them, yeah.

Steve: So they introduce you to people who are sending you email that you might not already know. It's like, oh, wow.

Leo: There are ways to do that without doing it in such a draconian solution. There's plugins for Chrome, for instance, Gmail plugins that will add contact information as you're looking at an email, things like that that don't require you to send your emails to another...

Steve: Yup, and this routes your email through them.

Leo: That's a terrible way to do that.

Steve: Well, and consider also that they lost 6.5 million LinkedIn accounts not long ago. I mean, their security has already shown some problems. And so, oh, yeah, I'm going to route my mail through them. They're storing it because it's a store-and-forward. So they're going to store your email on their servers, and then modify it to add their content so that - and build this as a service to you. It's like, yeah. This really sounds like a good idea.

Leo: A lot of people will do it. A lot of people will do that.

Steve: Not our listeners.

Leo: No.

Steve: No. So anyway, wow. And everyone saw this and started tweeting me, like, Steve, have you seen this? It's like, okay.

So CryptoLocker follow-up. We talked about it at length finally last week. I got a tweet from a Rob Pickering Monday, who came into work and was greeted with the news that one of the execs in his apparently rather major corporation got CryptoLockered over the weekend.

Leo: Oh, dear. Oh, dear.

Steve: And so Monday morning it was, um, I have something on the screen. And Rob had already heard last week's podcast. So he said...

Leo: Oh, even worse. He knew what he was looking at.

Steve: Yeah.

Leo: Oh, the feeling in the pit of your stomach when you see that.

Steve: And he said, "Read me exactly what it's saying." And so it was verbatim the beginning of that sort of broken English that I shared with our listeners last week. And he did have that sinking feeling. And he said, "Okay, don't touch anything. We'll see what we can do." So he started tweeting to me. And he ended up putting up a really interesting first-person narrative experience blog posting. Unfortunately, when I tweeted that, of course, it crashed his server because so many people were interested in tracking it down. I had him produce a PDF of the page which I then hosted so that everyone could get the PDF from me.

So for anyone who's interested, this is in my Twitter stream. And remember, you can always find my Twitter stream, you can obviously go to Twitter.com/SGgrc. But then there's that neat guy that's aggregating my stream for me, and he's at bit.ly/SGgrc. And that'll bounce you over to his page, where you can easily find those tweets, where I have links to both Rob's original blog post, which he has updated since, and the PDF that I had him make for me so I could host it with my bandwidth, which is hard to crash. So the good news is 100% recovery. They paid the ransom. They got the key. It began doing the work. And all the files came back.

Leo: Well, that's sort of good news. I mean, they're out 300 bucks.

Steve: Yeah, but they had files that they needed that weren't backed up anywhere.

Leo: I don't know if that's the good news. They gave 300 bucks to a bad guy. It's like, "Good news: I got mugged, but I'm not dead."

Steve: Well, and so we hadn't seen - from everything I'd seen online, there were mixed results, but no affirmative full recovery report. And we were sort of chuckling, you and I, that it didn't look like the bad guys had spent as much time perfecting the recovery, the decryption, that they had the encryption, which of course was understandable, I guess. But at the same time, if this thing developed the reputation of not giving your files back after you paid your $300, then people would stop paying the $300. So anyway, it does successfully decrypt.

Leo: As long as law enforcement hasn't shut down the server with the keys.

Steve: True. True. And that has been happening also. Another listener, Tony Casazza, I guess, C-a-s-a-z-z-a, he tweeted earlier this morning, "My client just called up with CryptoLocker virus. They are paying the ransom. Cross my fingers it works." And then a bit later he wrote - I'd sent back to him, I said, "Good luck, as far as we know it does." And he says, "Thanks for the reply. Wait. Just got message payment activated. Decrypting files. Holding my breath." So the bad news is these guys are making a ton of money. As you said, Leo, I mean, it's a mixed blessing. They are making a ton of money. And this is why it was immediately clear to me last week that this was the new normal. I mean, this was what we're going to see.

Leo: Well, I just hope awareness of this spreads as fast as possible. That's why I put you on every venue I had, because if people back up, then they don't have to give 300 bucks to these guys. And I really think that giving them 300 bucks is not the ideal outcome because it just, as you point out, encourages it.

Steve: It's going to encourage it, yeah. But on an individual level, what choice do they have?

Leo: No, I understand. That's why be proactive.

Steve: Yup.

Leo: Back it up.

Steve: Yup.

Leo: And how come he didn't have a backup?

Steve: Well, you'd have to ask him.

Leo: This is a business, and you don't have backups?

Steve: Well, this was the executive's personal machine at home on the weekend.

Leo: Oh, it's the nitwit executive. Oh, yeah. That's the problem with, you know, executives. Yeah.

Steve: Yeah, those darn...

Leo: I'm sure the business was well backed up and wouldn't have a problem here.

Steve: No doubt, no doubt.

Leo: In fact, in a way that's Darwinian. Executives should have to pay $300 just for being executives.

Steve: Darwinian. I did, I have also heard of instances where someone in a corporation had the shared drive mapped to a drive letter, and it encrypted the corporate drive.

Leo: Oh. That's what we were worried about.

Steve: Yes. We've had confirmation that it is going after drive letters. And so it will enumerate the drives and go look for anything out, any enumerated drives on the system. So it did reach into a shared server and encrypted those documents.

Leo: So be careful. Back up. Please. I beg of you.

Steve: Well, and the issue of hot and cold backup, then, of course becomes very germane because - so you need versioning backup, where the versions are deep enough that you will recognize the problem and still have backups that predate the moment of encryption and when your backup snapshot occurred.

Leo: I mean, this isn't a hard thing to do. Both Macintosh and Windows have versioning backups available, Time Machine and I forget what Microsoft calls it, folder thingamabob.

Steve: They're snapshots.

Leo: Yeah. So you absolutely can do this without any expense or really even much

trouble. But do it.

Steve: Yeah. So two Snowden updates. One is a few days old, well, okay, Monday. And this just sort of crossed my view, and I thought, well, this is sort of sad, and that was - this is via Reuters that reported that British Prime Minister David Cameron said on Monday his government was likely to act to stop newspapers from publishing what he called "damaging leaks" from former U.S. intelligence operative Edward Snowden unless they began to behave more responsibly.

Leo: This is why we need WikiLeaks.

Steve: I know. Quoting him, he said: "'If they don't demonstrate some social responsibility, it will be very difficult for government to stand back and not to act,' Cameron told Parliament, saying Britain's Guardian newspaper had 'gone on' to print damaging material after initially agreeing to destroy other sensitive data." So, wow.

Leo: [Sighing]

Steve: And then this morning's news. There's a link that I have in the show notes, Leo, if you want to click it and bring up a picture because this Washington Post article, which copies something that the Guardian had posted - I assume it was in the Guardian. Maybe I'm not so sure now. But the Washington Post did a picture of today's most recent slide, courtesy of Edward Snowden [wapo.st/HuOzL9].

Leo: Now, I have to warn you, if you are a government worker...

Steve: Oh, right.

Leo: That what I am about to do will force you to burn your computer and hand in your badge or whatever it is that you have to do. Because if I show this classified slide...

Steve: On a non-classified computer...

Leo: ...on a non-classified computer, you've got to tell your boss. So turn off the podcast now. Or get a better job. Think about the private sector.

Steve: So what this slide shows...

Leo: This doesn't look like a slide. This looks like a Post-it note.

Steve: [Laughing] Well, it is yellow.

Leo: It's a Post-it note. It's yellow and handwritten.

Steve: So this shows, on the left is the public Internet cloud with all of the regular things out there, showing SSL encrypted links going to something called a...

Leo: This is the worst - if this is a PowerPoint slide, we are in more trouble than I thought.

Steve: It's also got a smiley face on it. So it is very...

Leo: This is so depressing. There's a smiley face.

Steve: So this shows all of that and something called a "GFE Box," which stands for the Google Front End. And then behind the GFE, the Google Front End, is another cloud showing Google datacenters exchanging data not encrypted. And what we now know is that the NSA - and there's a name for this program that the story discusses. There is another part of the program is the NSA deliberately tapping Google's cloud communications, which have been decrypted by the Google Front End and are in the clear.

Leo: This is where the smiley face appears. It's right under the GFE: "SSL added and removed here," smiley face. This, I don't - I'm sorry. This doesn't - it feels not credible to me, like this is - the NSA would do this? Like this Post-it note with a smiley face?

Steve: Well, they're not known for their graphics. Their prior slides were not award-winning in terms of their design. So...

Leo: This is the most ghetto slide I've ever seen.

Steve: Well, the bad news is, I mean, it makes sense. The way SSL operates, one of the things you often do is you run - a major SSL provider will have accelerators on their border, so-called "SSL accelerators." They're hardware assisted, performing all of the crypto work. And so the SSL communication is point to point between the SSL accelerator and the user. And then inside that you have a non-SSL encrypted connection. It is decrypted by the accelerator because the accelerator is tuned specifically, often with strong hardware crypto technology, to deal with the bandwidth and the extra SSL handshaking. And then inside you don't have that. So it entirely makes sense that at some point this is what was going on. And the slide tells us that the NSA was deliberately tapping, essentially in the cloud. That is, as this data, which is private Google IPs and point-to-point, but it does, in order to go from one datacenter to the next, it's traversing the public Internet, even though it's private IP to private IP. The NSA knew that. They knew it was decrypted, and they arranged to tap it.

Leo: The tool is called "Muscular."

Steve: Uh-huh.

Leo: And the reason the British don't like these revelations is because it's operated jointly with GCHQ, the British spy agency. So...

Steve: Yeah, the British equivalent of our...

Leo: Yeah, NSA, yeah. So that's why David Cameron's so peeved.

Steve: Yeah. So more from - more details.

Leo: And judging - this feels credible. I mean, I've got to say the Post-it...

Steve: It does.

Leo: ...doesn't feel credible. But the information therein is perfectly reasonable.

Steve: Yeah, yeah.

Leo: Yeah. And if they weren't doing it, they're probably thinking about doing it now.

Steve: So a little quick instant messaging follow-up. I talked about the BlackBerry Messenger and its phenomenal number of downloads since it was released. It was, what was it, 10 million in the first day?

Leo: Yeah. Downloaded. I wonder if used. But anyway, that's - I downloaded it, and as soon as I looked at it I went, this is horrible.

Steve: Well, and now we're at 20 million in one week. And Boy Genius Reports did a follow-up where they showed that, not only was it 20 million in the first week, but they had surprisingly held their position among the very top iOS and Android downloads throughout that entire week. Boy Genius said that many times something will spike, and you'll see it in the top ten for a day, then it immediately drops back down. BBM, the BlackBerry Messenger, has held its position for seven days, which they said was really unprecedented, I mean, that it had that kind of staying power.

So and I did install it, like you. It happened that our podcast friend, Simon Zerafa, who often tweets, I happened to see him. He tweeted something, and I sent him a message with my BBM ID. And so we sort of - we played with BlackBerry Messenger a little bit for

10 minutes. And it was like, eh, okay, well, you know. Other people explained that the reason it was so powerful was it had good group messaging features. Apparently that's one of the strengths...

Leo: So does every other - so does WhatsApp and everything else. This is the '90s are calling and they want your messenger back. I don't think this is state of the art by any means. The real reason people are downloading it is because they still know people, that's how they communicate with them on BBM because you need their BBM number. I mean, it doesn't even go by name, it goes by PIN, which is...

Steve: Right. You need their PIN. And the thing that I wanted to do, which is why I brought it up initially last week, was to disabuse people of the belief that it was somehow really strong security. It's not. So I wanted to let people know, yes, from everything I've seen, Threema, T-h-r-e-e-m-a, that we also discussed last week, is really strong. And I have also played with it. And I don't have a pressing need for point-to-point encryption. I'm happy with iMessage on my new iPhone. But if I do need really strong, point-to-point encryption, Threema would be, I think, my app of choice. There are alternatives, but Threema really looks like they did it right.

Leo: So many people have Threema'd me now because of this, and I have responded. I've kind of done the same thing I did with PGP, which is, yup, your Threema's working. We are connected. You and I are connected via Threema, but we haven't yet exchanged QR codes. We have to do that in person over a glass of fine Cabernet.

Steve: Right. I think I associate it with my email address.

Leo: That's right.

Steve: And since you have my email address in your account, it said, oh, somebody you know is using Threema, and then it was able to connect you.

Leo: You know what's nice, though, Threema, like BBM, but for privacy reasons, doesn't associate it with a name in many cases. So when I get a Threema from somebody...

Steve: Correct.

Leo: ...it's just a number. It's an ID number.

Steve: And you're able to give them a - you're able to assign that account your own nickname. And it suggests that you not use your real name, but rather that you use a handle that you're comfortable with somebody else seeing.

Leo: Is this a TNO solution, though, really? It's not.

Steve: It absolutely is.

Leo: It is.

Steve: Yes, yes, yes. Absolutely. I meant to do - since I talked about it last week, I ran across much more detailed information about their cryptography. I mean, for example, they're using the same elliptic curve stuff, they chose exactly the same stuff I chose for SQRL. These guys said this is the right one. And so it's like, whoa.

Leo: And it's done on your device. It's not done on their server. Nothing is stored on their server unencrypted. Nothing goes to their server unencrypted. It's like PGP. You encrypt it on your end, send it. They do hold it so that they can have a store-and-forward briefly.

Steve: For 14 days. But it's, yeah, so it uses Dan Bernstein's ECC, the same 25519 elliptic curve technology that I chose to use for SQRL, which has been looked at a lot. And as far as we know, I mean, it's completely NSA-proof. So your Threema client generates a public key pair. The private key never leaves you. The public key then is what you want to - the reason that they have these three dots is that you want to obtain a level of confidence that the public key belongs to who you really believe it does because authentication then is the challenge. After you've achieved privacy, you want to make sure you're not subjecting yourself to a man-in-the-middle attack by having someone - someone gives you their public key. You give them yours, thinking that they are somebody else. And then they turn around and give theirs to the other person and establish a man-in-the-middle position.

So that's why there's this red, orange, and green three dots is the level of certainty. And so, for example, you and I would have orange level, two dots, because we used our email address books to identify each other more than just exchanging the public key itself. And when we meet we can aim our phones at each other. They will then do a first-person, phone-to-phone public key exchange, and that will bring us up to green level, which is we're absolutely sure that we have each other's public keys. And so, yeah, I'm very, very pleased with Threema. I think...

Leo: It's a neat idea. And it does - I don't - it doesn't do - maybe it does group. I haven't - but it does do multimedia, so you can send images and all that.

Steve: Yup. It's not group, it's just point to point.

Leo: Just point to point. That makes sense. You couldn't do group, probably.

Steve: Be more tricky to do that.

Leo: More tricky, yeah. Very nice. Good. I've been using it. Put it on my front page.

Steve: Yeah. So it's there for...

Leo: Now, should I hold up my QR code and put it on camera and let everybody take it?

Steve: You know, I was tempted to post mine on, like, on my own website just because it's like, hey, here's my QR code.

Leo: Why not, yeah.

Steve: And that would allow everyone to get green dots, which is sort of nice. And so...

Leo: Is there any reason not to do that?

Steve: For me, you would want to be on SSL, and of course GRC is a hundred percent SSL, because then the real, the security kneejerk people would say, wait a minute, a man-in-the-middle attack could have changed that image, and you wouldn't know that it was real. But, yes, you could hold it up, like on the podcast right now, on the video, and there it would be. So anyone whose phone was able to scan that...

Leo: It's my public key.

Steve: It's your public key. That's all it is.

Leo: So the only negative to this would be that then everybody would know my Threema code, not just my friends.

Steve: Correct. And so you could get spammed. Anyone could send you stuff on Threema.

Leo: Well, anybody who watches Security Now! is my friend.

Steve: That's right.

Leo: Right? So there is my Threema QR code, right there. I'll just hold that there for a second. You don't need it for very long, you just do a screen grab. I think that's good enough resolution. I'm really amazed by the - we've talked about this before,

how much redundancy and how effective QR codes actually are.

Steve: Yup. They're very reliable, varying levels of error correction. It uses strong error correction because in many situations, like where there might be a poster, the poster could be physically damaged. Sometimes people will even put logos in the middle of the QR code, which completely violates the encoding.

Leo: But there's so much redundancy, it...

Steve: There's so much error correction that it'll just error correct right around the weird little logo in the middle. So I think that's cool.

Leo: I do, too.

Steve: Well, and speaking of QR codes, we have officially renamed SQRL. It's still...

Leo: What?

Steve: No, no, it's still SQRL. But it stands for Secure Quick Reliable Login.

Leo: You've retronymed it.

Steve: We've retronymed it, yes. The problem was too many people were thinking all it was, was QR codes. And it's evolved way past that so that you don't need a smartphone, you don't need - it's like, well, how do I log in on my phone? Well, you just tap the QR code. How do I log in on my computer? You just click on the QR code. You don't have to scan it with your phone. And so we decided we would, I mean, nothing else has changed.

Leo: I like that, Secure Quick Reliable Logins. I like it.

Steve: Login, yeah. It's funny because I just changed the title on the web pages yesterday, and when I looked at it for the first time, I thought, that really works, I like that. So we have a person in our newsgroup, Monty, who said, you know - and he's been out browsing around the 'Net, seeing what other people are saying. And he says everyone's getting tangled up in the QR code part. They're saying I don't have a phone, or I don't like QR codes and blah blah blah.

Leo: Right, right. I think that's appropriate.

Steve: Okay. Let's back away from QR codes and just say Secure - because it is secure, quick, and reliable. Login.

Leo: Good. I like it. Hey, before we get to your miscellany...

Steve: Okay.

Leo: Before we get to the Gordon Shumway project. Because I learned something from this. This is good. I like it. I was kind of - I misunderstood really what Gordon Shumway stood for.

Steve: So I did want to follow up a little bit on my discussion last week just briefly of SQRL's new, what we call ID Lock.

Leo: Oh, okay, good, yeah.

Steve: Identification Lock. I had just released it - remember I'd spent a couple hours at Starbucks and figured out a protocol. And I just put the page up. And I'm not going to try to describe it on the podcast because it's tricky. What I wrote was, I said - and this was on the ID Lock page, so it's completely documented in the SQRL pages at GRC. And I started by saying, "The Identity Lock protocol is admittedly a bit tricky. It needs to be more complex than SQRL's comparatively straightforward identification protocol because its requirements are more complex. While operating, it must be able to generate and provide something to every web server so that its identity can later be proven. But what it generates and provides to each web server cannot in any way identify it to the server since the SQRL system provides strong anonymity guarantees to prevent web servers from having anything they might compare to identify and track users.

And on top of that, since it must be truly hacker-proof, the system that generates this identity-proving information must not itself be able to prove its own identity. Otherwise, a compromised or hacked SQRL client could be used to maliciously prove its identity in order to unlock and alter a user's website identification. So we need to be able to provide anonymous identity proof without being able to prove our identity."

Leo: [Laughing]

Steve: And that's what I did.

Leo: Okay. That's confusing.

Steve: And so, well, no, I mean, it is. And people in the newsgroup have, like, have studied the protocol and understood it because it's not like it's super voodoo. It's not that complicated. But it's just a little too cumbersome for me to describe verbally. But I wanted to invite our listeners who are curious to go check out the Identity Lock page [grc.com/sqrl/idlock.htm]. I just finished a rewrite late last night because the way it sort of evolved, it ended up being clunky. So I went through, and I cleaned it up and unified the naming that I'd used, and it's clearer now than it was.

But it's pretty nifty because the cool thing is, as you're using SQRL just during the day, and you're associating your SQRL ID to new websites, the SQRL client is at the same time providing information which locks your identity so that, if the worst happened, and someone were ever to hack your SQRL client, they could not change your identity. They couldn't lock you out of your accounts.

And what that also means is, if you discovered that someone had apparently been logging in as you, which is what could happen if they somehow hacked your SQRL password and master key, if they got a hold of that, then you can, by then loading this Identity Unlock key, which is always offline, no part of it lives in your SQRL client, but you get this out of your drawer where you've been saving it. Then you're able to preemptively change your identity and essentially take it back from bad guys that may have gotten it. So you are able to take back your identity if it were ever to escape. And because that ability does not live in the client, bad guys can't do that. So we really made some great progress with this.

Leo: Yeah, that's good, yeah.

Steve: I think it's going to happen. So, Shumway.

Leo: So thrilled.

Steve: Remember last week I was just, like, Leo, why does this sound so familiar? Why? I couldn't figure out what it, I mean, like, Shumway, why is that - I felt like it was current.

Leo: Right.

Steve: Well, the mystery was solved, thanks to people who listen to the show and listen to me and know the things I'm doing and watching. But it turns out, first of all, where Mozilla came up with Shumway, remember that this Mozilla Shumway Project was their codename for their project to build a native JavaScript-based Flash VM. They were going to basically host a Flash Virtual Machine, run Flash files without needing to load Flash, the Flash plugin, in the same way that they now, for example, are able to give us PDFs reading natively in the browser without needing to load an external PDF plugin. So that was Shumway. So it turns out, thanks to a bunch of people who tweeted, that Gordon Shumway is the - I guess was Alf?

Leo: Right. And we said that [SN-427]. Maybe you didn't hear me.

Steve: I didn't know that.

Leo: We said that in the - because the chat room came up with that one.

Steve: Oh. And then I guess Flash Gordon inspired the naming of Gordon.

Leo: Shumway. Of Alf. Because Alf...

Steve: So you have Flash Gordon, and that's where the Flash comes from, and then Gordon Shumway. So they're, like, two of these weird references linked together to get to it. But the reason it was so familiar to me was Julia Shumway is one of the characters in "Under the Dome," which I read the book, and then I...

Leo: That's where you'd heard it, yeah, yeah.

Steve: Yes. That's why it was so familiar to me was just, like, Shumway. What have we been talking about recently that is Shumway? And it was Julia Shumway, who's one of the characters in "Under the Dome." So that's what that mystery was. And now, Leo...

Leo: I just got a Threema from somebody who says, "Thank you. I work for a group of doctors, and now they can text each other."

Steve: Ah, they really can.

Leo: "It's HIPAA compliant..."

Steve: Yes.

Leo: "...since all messages are encrypted. This is going to make us more secure for the new 2014 regulations."

Steve: Yes.

Leo: That's great.

Steve: I mean, it is absolutely secure. Those guys did it right. And they've freely talked about how they're doing it, which you have to these days. Leo, there's - I had a big change in my life.

Leo: Steve, Steve, Steve, you cannot get married again. It's just - go ahead.

Steve: Fortunately, there's no sign of that happening. Jenny is as uninterested as I am.

Leo: I love Jenny. She's great.

Steve: She is.

Leo: You two are a very good couple. You kind of remind me of Lisa and me. There's just - it's just a great relationship.

Steve: She had never seen "Gremlins," so we watched "Gremlins." And, first of all, when she saw that it was Steven Spielberg, she says, oh. That helped her a lot because she was a little skeptical. And but then she knew there would be a story, and she really enjoyed it. She's anxious to see, and we will be seeing, "Ender's Game" on Friday. I mean, so, yeah, there's a lot of great overlap between us. And also the fact that we're happy as we are. No. The big change for me...

Leo: Okay, wait a minute, let me guess. You're not switching to tea. You got an iPhone? Or is that an Android?

Steve: No I switched.

Leo: What is that?

Steve: It's an iPhone, and I've switched.

Leo: Well, for you, I think that - you got the 5s with the fingerprint; right? I think that's a good...

Steve: I did. The problem was I could never make the change because I liked BlackBerry's keyboard and messaging. But I have to say that the keyboard-aware correction on the iPhone...

Leo: It's pretty good, yeah.

Steve: ...is excellent.

Leo: You have to - it takes a little while because you have to learn to trust it. So if you just type, even though you know you're typing inaccurately, and it somehow knows.

Steve: Well, and it should, because it should be able to see the letter proximity and use adjacent keys as hints for the spell corrector. And I believe they really did it right. But I contacted Verizon a couple days ago, and I said, okay, I want to exchange these phone numbers.

Leo: Oh. That's a big switch. That's a...

Steve: Oh, Leo, I did not do it cavalierly.

Leo: You should have at least gotten a Google voice number and...

Steve: For a while I was carrying both of them. I thought I needed a crossover period. So my right front pocket was a little heavy for a while. But now - and I actually weighed them both, and the iPhone weighs less than the BlackBerry. So I'm a little bit lighter, and I'm very happy so far. I've just - yeah. Oh, and I did go into Verizon and looked at the iPad Mini. Even though it's the old one, it's still going to be the size. I think that may be the one, Leo.

Leo: Yeah. I can't decide. The reviews for the Air are now coming out because they seeded the big names. And very positive. It's 80% faster than the previous version, which was very fast, this new A7. And it's smaller. So I think, well, the problem is you don't - you could go in and play with an Air starting Friday. So maybe that's what you should do.

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

Leo: And then, if you say, no, that's still a little big, then hold off. We still don't have a ship date for the Mini with retina.

Steve: I know. But the Mini, it's like enough bigger than the iPhone that you can actually do real work on it, I think. I mean, you can really easily...

Leo: Oh, totally. Oh, totally.

Steve: ...really read web, well, I mean, it's the same resolution as the larger pad.

Leo: Right. Just shrunk down a little, yeah.

Steve: Just smaller, yeah. That may be the one. So, okay. Now this is...

Leo: You're going all-Apple, dude.

Steve: I am. And things are, like, syncing. It's amazing. Like it knows what my tabs are on different - it's like, I'm getting all this cloud benefit. So, yeah.

Leo: See, it really is 2013 now.

Steve: Beginning to happen. So this is an odd - I ran across this from Justin in Lacey, Washington, and the subject line caught my eye when I was going through the mailbag this morning. It said: "SpinRite helps to uncover lazy employees." And I thought, what?

Leo: [Laughing] Never thought of using it for that.

Steve: Well, he wrote: "Several employees were given a stack of hard drives to wipe with a company-approved wiping software for disposal. I decided to run SpinRite on some of them. I am not sure exactly what the wiping process entails, but the end result I know is that the same ASCII character is repeated across the entire hard drive. While running SpinRite and peering into the drive through SpinRite's real-time analysis window, several drives came up showing me data other than what I knew I should see on a wiped drive: recognizable file information, filenames, corporate data, et cetera. And since each drive was assigned to employees by hard drive serial number, it was easy to track down the person who was simply deleting the partition table and calling the drive 'wiped'."

Leo: No, no, no.

Steve: We've never talked about this. But in SpinRite 5 there used to be a large area of the real-time analysis window or screen that had a bunch of data that became obsolete in SpinRite 5. So I thought, hmm. What am I going to put in there? And I thought, well, I'll just show the drive data. And so it's really - it's actually kind of fascinating because you can watch this screen while SpinRite's running, and things you recognize go flashing by. I mean, it's showing you...

Leo: Ooh, that's not good, yeah. That's a little scary.

Steve: It's showing you what's in the drive. And, I mean, it's not decrypting or anything. It's just showing you what it's reading. And so I thought this was really an interesting hack for SpinRite that had never occurred to me before, is if you want to verify that drive-wiping worked, you can run SpinRite on it and just stare at that little - stare into the drive through the window and see if you see filenames and data and stuff that's not wiped or encrypted. And so that was a kind of a cool use for SpinRite that had never occurred to me.

Leo: Well, there you go. Isn't that good news. A great way to see what's on that drive. All right. Are you ready? Got questions. You got answers; right?

Steve: Yes, you betcha.

Leo: Launch right into it here with Question #1 in our listener-driven potpourri.

From - you got me excited a little bit for a moment. John Sellitti in Venice, Florida wants positive VPN proof. Okay, he says, I'm convinced I need a VPN. But how do I know if it's working? Steve and Leo, you sold me on proXPN. Good. I travel a great deal, and I use the scary unsecured hotel wireless.

Steve: Ooh.

Leo: You know what's fun, a little fun trick, if you're...

Steve: That's got to be the worst, Leo.

Leo: If you're on a Macintosh, and you do that, you'll see all the other people on Macintoshes. You'll see their iTunes shares. It's really fun. All their iTunes libraries just pop right up.

Steve: Oh. Oh [laughing].

Leo: You can't, I mean, you can't steal their music - usually. Depends how they've set it up, of course. I signed up for proXPN, used the offer code SN20. I use it with my laptop and my Nexus 7 tablet. I can confirm that my IP changes after connecting to proXPN. But here's my question: How do I know the VPN is doing its job? How do I know my traffic is encrypted? Surely there's a cool test on GRC.com.

Steve: Okay. So that's a great question. For a belt-and-suspenders person who, I mean, first of all, if you recognize how scary that environment is, exactly the scenario you talked about, Leo - and remember in the old days, before personal firewalls and before anyone understood about Windows filesharing, people's C: drives were out on the Internet. I mean, that what - that prompted me to do ShieldsUP! was to show people, uh, I can see your C: drive, guy. So you should take some precautions. So his question is, how does he know it's truly encrypted? And unfortunately, there is not a cool test at GRC because GRC will see the outside-the-tunnel traffic after the tunnel has been decrypted, just prior to emerging on the Internet. So what you need is you need some kind of what's called "packet capture" software.

Now, on a desktop machine, like on Windows or a Mac, Wireshark is, like, the standard in packet capture, relatively easy to use. And what you would do is you would run Wireshark, tell it to monitor the traffic on your NIC, on the Network Interface Card or controller on your actual Internet interface. And just you can - you start it doing that, and then doing unencrypted things like go check your mail. You'll probably see your mail go by right there in the clear. And then, if you bring up the VPN tunnel and are monitoring your network interface, and do the same thing, you should see it just looking like gibberish. It will just be, I mean, looking like cartoon-character cussing, just absolute nonsense, nothing at all intelligible. It'll completely disappear in the encrypted tunnel. And there's something called Android PCAP and also tPacketCapture are two Android tools, if you want to do the same sort of thing on your Nexus 7.

So you definitely can, if you're curious, do a before and after, with and without the

encryption tunnel running. And then you could also do other things, like you could, if your network was set up on a hub, you could run this on a hub where you could see the other computers' traffic and capture it in a third-party situation.

So you can use packet capture in a number of ways. But probably the easiest is to run it on the same machine where you've got the VPN running, and then look at the interface, not the VPN's interface, because it'll create a virtual network interface card which you connect to. But you want to look at the physical NIC on the network, and you'll see the before and after change. It's dramatic when the tunnel is up and running. And it's really a cool experiment to run, by the way. I've done it a bunch.

Leo: Everybody needs a packet sniffer in their...

Steve: Yeah, in their bag of tricks.

Leo: Always a good thing to have.

Steve: Yeah. Oh, and, boy, go to Starbucks, and it's frightening. Oh, boy.

Leo: So did they - it was Wireshark, and now it's...

Steve: It used to be, oh...

Leo: Or is the new name Wireshark? Because...

Steve: The new name is Wireshark.

Leo: Oh, okay, good.

Steve: And I can't remember what it used to be.

Leo: But it's free. It's open source. It's really handy.

Steve: Yeah. And it is THE tool. In fact, it's based on the original, I think it's called - was it NPcap? I think it was called NPcap, which was a beautiful open source...

Leo: Oh, used to be Ethereal.

Steve: Ethereal, exactly right.

Leo: Yeah, yeah.

Steve: Yup. So, and that was based on the NPcap library, which is what I originally used to build ShieldsUP! in order to add low-level packet capture...

Leo: Oh, neat.

Steve: ...to Windows. I later wrote my own network interface capture at the low level because there was more stuff I wanted to do. But it's a great packet capture library and has been ported to all platforms.

Leo: Do you ever use NMAP?

Steve: I'm aware of it.

Leo: That's kind of more of a pen testing or...

Steve: I just never really had a need for it, yeah.

Leo: Yeah, or a protocol. It's another - it's essentially a security scanner that's also free and open source.

Steve: And also has a strong scripting background. So you can do, like for example, someone did mention the other day that there was an NMAP scanner script for, like, open webcams or something that we'd just talked about. Oh, no, it was a vulnerability in the D-Link router that we discussed where, if you set the user agent to a certain string backwards, then it was able to do unauthenticated access to the user. And so someone quickly whipped up an NMAP script that would just find them for you on the Internet.

Leo: That's great.

Steve: It's like, oh, thank you very much.

Leo: And, by the way, the good news is we now know that NMAP will still be in use in 2154 because, when they hack Matt Damon's brain in "Elysium," if you look up close at the screen shot, it says "Starting NMAP 13." [Laughing] That's - somebody, whoever did their screens for "Elysium," knew what he was doing.

Steve: Yeah, they had some good techies, yeah.

Leo: I love that. Question 2, shall I move on?

Steve: Yes.

Leo: This comes from John Vandiver in Smithfield, Virginia, home of the fine Smithfield ham. Steve and Leo, I thought you might be interested in this site, Livingto100.com. You fill out a questionnaire, it gives you life expectancy. Thought you might want to try it out now that you're so healthy. I'm going to live to 97. I thought I could retire at 72, but I may have to launch a new career. Jim from Smithfield, Virginia. I guarantee you he doesn't eat a lot of Smithfield hams if he's going to live to 97.

Steve: Yeah. So, okay. First, so, well, it would be. Well, it can be. First of all, I tweeted it, and immediately found out from a good friend of mine that they want your email address. Then other people said that there's no verification at all, and so you can just type random gibberish for your email address.

Leo: Oh, good, right. So that's a good start.

Steve: And I have not tried it. I can't vouch for its accuracy. But I thought that our listeners might find it interesting: Livingto100.com. And I don't know what they're trying to sell you, or what the deal is, but - and it does seem to be giving people a lot of encouragement because I had, in the feedback that I've seen, everyone seems to be in their 90s. So either we've got an unusually healthy...

Leo: Oh, wait'll I fill it out, dude. What did you get?

Steve: Tell the truth.

Leo: What did you get?

Steve: Oh, I haven't - I just found out about it this morning, and I've been working on the podcast all morning, so I've had no time to do it. I didn't want to get myself involved where I thought, well, I might be late for getting all my notes together.

Leo: Check all that you feel currently stressful. This is good, yeah. This is good.

Steve: So don't worry about having to give it a real email address. You can just make anything up that you want to.

Leo: They didn't ask me for email. Maybe they ask at the end.

Steve: They do at the end, apparently.

Leo: So they can mail you with your results.

Steve: They bait you, yeah.

Leo: Jamie Brand in Burnaby, British Columbia, Canada wonders about a possible way around CryptoLocker. I'm curious, says Jamie, if you happened to have whole drive encryption turned on with TrueCrypt, would CryptoLocker be able to hijack your data? Would it prevent them from encrypting it as it would already be locked, per se? Or would it just be an onion router situation where it would encrypt the encrypted information and you'd still be screwed? Love to know your thoughts. Also, why isn't Security Now! called This Week in Security Tech, TWiST? It has a nice ring to it. Love your show, hopefully I can get your feedback. Jamie.

Steve: So the bad news is, if a system gets infected that is whole drive encrypted, then CryptoLocker is running on and in the drive and can see all of your files and encrypt them. So unfortunately it is like the onion router. It is double-encrypted, which is definitely not what you want. You only want it encrypted by TrueCrypt and not anything else. If this was a drive offline, then it could not encrypt it. I'm assuming that the file extension that TrueCrypt uses is not among those which CryptoLocker encrypts. Normally it just goes for things that are videos and documents of various sorts that it finds in your documents file. So I don't remember what the file extension is for a TrueCrypt container, probably not on CryptoLocker's list because it would feel it was a waste of time, although it could certainly damage you if it did that. But, so, yes, unfortunately, and a number of people asked this, so I wanted to answer the question, whole drive encryption of a mounted drive won't protect you.

One thing that will, toward the end, the last question in our list, is some interesting prevention suggestions. But someone asked about a virtual machine. And that would protect you as long as the virtual machine couldn't see out into any of your other important files. So if you ran email in a VM-style virtual machine, it would be blinded to what else was there. And if that got infected from clicking a link in email, then you'd be okay. Just FYI. That's probably the strongest prevention I can think of. We'll have some that we'll, as I said, we'll talk about here in a second, which is good. But as you and I talked about on the weekend, Leo, the problem is it's a little bit in the cat-and-mouse category. Once this becomes popular, the authors could work their way around it. So it's not as strong as putting your email in a virtual machine, which is really robust protection.

Leo: Steve Gibson, Leo Laporte. We're answering questions from our vast and brilliant, if you don't mind me sucking up a bit, listening audience. Chris McCormack...

Steve: We have great listeners.

Leo: Yeah, I do, I really like them because they just - they ask great questions. I'm sure you enjoy this. Chris had a thought about malicious encryption: While you were

discussing the recent trend of malicious encryption - in other words, CryptoLocker, the first of many I'm sure - an idea formed in my head. If you were to back up a static, never-changing file from your computer to a secure backup, could you use this file to determine the key used to encrypt the recently encrypted version of the file on your hard drive after the attack? In other words, kind of figure out what the encryption was to reverse it? Seems it would be trivial once the algorithms used by the attack are determined. Love the show.

Steve: Well, so that's interesting. We've never talked much about cryptanalysis. We've touched on it here and there. But essentially what Chris is talking about is a huge area of cryptanalysis, and it's got some well-understood terms, a known plaintext attack, and in some cases a chosen plaintext attack. The idea is that the question is, if you knew what the unencrypted data was, that is, the plaintext, so known plaintext, can you learn anything useful in, like, what the key is that was used to encrypt that known plaintext, because presumably you already have the encrypted text. And then a slight variation on that is the so-called "chosen plaintext attack." And that's a situation where the person trying to crack the encryption is somehow able to put their own tests in and see what the plaintext they choose is turned into, and that gives them in some cases more control.

Well, the good news is, well, the good news for most of us who want strong encryption is that AES, and any modern cipher, I mean, the so-called "known plaintext" and "chosen plaintext" attacks are, like, the basis of cryptography. So any recent cipher will absolutely not leak information about, like, the encryption key used, even if someone trying to learn what that was had both the plaintext and the encrypted ciphertext at their disposal, which is what Chris is suggesting. So modern ciphers are completely immune to that.

A perfect example of this being done is a, for example, we've talked about this often also, a simple stream cipher using XOR to merge the plaintext with the pseudorandom stream. Remember, if we have a pseudorandom stream of bits, and we take plaintext, and we XOR those two, even though it's a little counterintuitive, what you get is really good crypto, except it is absolutely vulnerable to, for example, a known plaintext attack. Because if you took that ciphertext, and you XORed it with the plaintext, you get back the pseudorandom stream, that is, you get back the key stream that was used for doing the XOR.

So XOR is an example of it's a little fragile. If you use it very carefully, just right, it's secure. But you can't ever use the same stream twice, or that opens you to an attack because it is so easily reversible. Whereas something like a modern cipher, like Rijndael used, which was chosen for AES, the Advanced Encryption Standard, is not subject to this kind of known plaintext or chosen plaintext attack. But great question. Several people asked it, too.

Leo: Phil in Leicester, U.K. wanted to check-in for your recommendations: First, big fan of the show. I've learned about security over the years through the podcast and your superb free tools, Steve. Thank you for doing this for the community. Given the ever-increasing need to protect our computers, I was just wondering if you could recommend any good free firewall and virus/antimalware protection software. My apologies if you've already covered this and I've missed it. I'm currently using Microsoft's Security Essentials with the built-in Windows 7 Firewall and Malwarebytes, but I'd like to know if there are any free alternatives. Once again,

many thanks.

Steve: And I'm using the same thing. I have never been a big user of third-party AV stuff. And Windows Firewall provides good, unsolicited, incoming protection. So, and of course I'm also behind all kinds of layers of NATs and routers and things. So I've got good security. But I just thought it was an interesting question. I know that our listeners would be interested, Leo, if you've got any favorites.

Leo: Well, we've had for many years a sponsor, ESET, which I think is excellent. Kaspersky, a lot of people say very good things about that. My kind of - most of the security people I know don't really take any extra steps, A, because they believe, and I think they're absolutely right, that really behavior is the biggest issue. And so even - in fact, as we know with CryptoLocker, even if you've got the best antivirus, if you don't behave well on the 'Net, even inadvertently, it doesn't matter; right? So I think a false reliance on antivirus is risky because it's not going to protect you if you're clicking links and opening attachments and, hey, let's see what this is. You're going to get bit.

Steve: Yup.

Leo: I think that, absolutely, Security Essentials, while not even close to the best antivirus out there, is probably adequate. In fact, Microsoft's own monthly check with its malware removal tool is a good start. In fact, you already have it if you have Windows. We've talked about this, I'm sure. You click Start > Run > mrt, you could do - it doesn't normally do a thorough scan, but you can coerce it to do a thorough scan. That's not a bad idea. It's not an antivirus. It's not proactive. But it will - it's a great way to see if there's something on your system. And Microsoft does, I think, proactively remove some of the better-known malware issues. I think Windows Firewall is fine. The issue, as we've said before, is it's a one-way firewall, does not protect you against outbound attack. But it's great against protecting your systems against other systems that are on your network, if somebody comes in and plugs in an infected - yeah.

Steve: The thing that annoys me a little bit about it is that it is prone to software in your machine bringing down ports, or opening things into them.

Leo: It allows it.

Steve: And so, yeah. And so that was the tradeoff Microsoft had to make for ease of use, which is why you really want to be behind a NAT router. And of course I think everybody is.

Leo: Everybody is. And, yeah, and that is, of course, a must have. And that's a - but if you've got that, I think you really have got a very effective firewall because it's just dumb. I can't imagine anybody who listens to this show sits a computer out on

the public Internet without a router because that would be not advisable.

Steve: I almost fell victim to a phishing email the other day and had to scold myself. It came in, looked like it was from PayPal. I use PayPal a lot. And it said, "Just confirming we're adding another email address to your account." And it's like, oh, what? And I take every precaution all of our users know we should take. But there's always that how did maybe something happen? Maybe somebody got in; maybe this is legitimate. And, I mean, I was, like, reaching for the mouse. And I said, oh, oh, oh, oh. And sure enough, I went over into my inbox and pulled the raw ASCII, and the whole thing was malicious. It was just - and the links were masked. It really is a problem that email - I'm still using an old Eudora client. I don't know if other email clients are better. But I cannot see what is behind an email link. It will not show me the domain it refers to. And so it's really annoying. I mean, it's just - it's really trouble-prone.

Leo: Well, I don't use HTML email. I turn it off. And I really wish people wouldn't use it. I think it's terrible. Didn't you block HTML email for a long time?

Steve: For a long time. I said, eh, that's not real email.

Leo: But the problem is everybody uses it.

Steve: It's now, yeah, exactly.

Leo: It's by far the majority of emails. Malwarebytes, a lot of people love Malwarebytes. I have very mixed feelings about that. I think it's also another case of a false sense of security. So if you - Microsoft Security Essentials, while not a great antivirus, nobody thinks it's a great antivirus, is okay. If you want to buy an antivirus as a form of protection, I do like ESET a lot. I think it's a really good antivirus. My best advice: Use a Mac. Because almost all of these attacks, including CryptoLocker, are aimed at Windows. It's not that the Mac is inherently more secure, although they've done some very good things to protect you. But it's just not a target. If you're using...

Steve: I love what Apple is doing, Leo.

Leo: If you're - yeah, yeah.

Steve: I'm really drifting in this direction.

Leo: If you're compelled to use Windows, then all of this is germane. Or Linux. Linux would be appropriate, too. Although you have to be more of an expert to secure Linux than you do on Windows or Mac. You really have to kind of know what you're doing.

Question 6, David Troxel in Maryland offers a heads-up about Match.com, a site neither of us uses or needs to, and its insecurity: Dear Steve, blah blah blah. I recently had an interesting occurrence that you should probably mention. I got a few emails from Match.com, with my wife standing next to me at the time. That's embarrassing. After looking and wondering for a few minutes, I concluded that someone, a female in her 40s, from the Midwest apparently, gave the wrong email address when updating her profile. Match does not send out the email with the link to make sure you did it right. Oh, I know this. And I'll tell you how I know.

Steve: [Groaning]

Leo: Match then emails me just about all her information - her screen name, her password - oh, you idiots.

Steve: I know.

Leo: And from listening to this podcast I know that means the passwords aren't encrypted on Match.com, so not even LastPass can save you. I also got her gender, zip code, and birth date. Oh, for crying out loud. I don't think anyone hijacked my email because I have text message two-factor ID, and I didn't get a text message. This looks like just some really poor security. With such a tech-centric following, I'm pretty sure someone listening to this show uses the Internet for dating purposes. They should know about this. Well, I do know that Match.com makes no attempt to validate email addresses because I get subscribed to Match.com regularly by pranksters [mirthless laughter]. But that's worse. That's a leak of information that is horrific.

Steve: Yes. This is a horrifying privacy leak. And so I wanted, I mean, I actually - Mark Thompson has used Match.com. Several decades ago I did, and met someone fun, and we dated for a while. So I was there once upon a time.

Leo: Yeah, it's a good service.

Steve: Boy, it's the No. 1, the No. 1 Internet dating service online. But with security this bad, I just wanted to make sure our listeners knew because I think David is right. There's no doubt that people who are hearing this are probably active users, and they need to be very careful with their email address and password going forth. Wow.

Leo: Yeah.

Steve: Really crazy that a site like that would be so lax with security. Because, I mean, it's the definition of personal information.

Leo: [Sighing] I mean, that's really enough to perpetrate identity theft, I think.

Steve: Oh, my goodness, yeah. And he could have clearly logged in as her and had complete access to everything she's able to do from her account.

Leo: Right. Mike Graham in Hopatcong, New Jersey - I don't know how you say that - wonders whether TrueCrypt is dead? It better not be. Hi, Steve. Based on your mention in a recent Security Now! episode, I checked out TrueCrypt. I take back what I said about our smart listeners.

Steve: Leo.

Leo: No. No, it's a simple and an easy mistake. To me, this site has all the earmarks of being dead. There's not been a release for over a year. The news page is similarly stale. I checked because I have a new laptop with Windows 8 and a UEFI BIOS, and TrueCrypt does not yet support this for full disk encryption. I was hoping you may have an in with the TrueCrypt developers. Mike. Love the show. Keep up the good work. TrueCrypt, is it dead?

Steve: No. But this raised an interesting point, and this is why I thought this was a worthwhile question, is that TrueCrypt is done. And that's why they haven't touched the page for so long. I mean, okay, now, yes, it apparently needs to be updated to support UEFI BIOS and so forth. But with a project like this - and of course I face this with SpinRite because SpinRite has sat, doing what it does, for 10 years because it did what it did perfectly. And I wasn't needing to update it continually because it was done. Yes, I will be working on it soon as I get SQRL put back to bed. I will be back to SpinRite 6.1, and I'm going to give everybody a free update, and support in the UEFI BIOS is one of the things on my list because the old-style partition table only has 32 bits, so it can't handle ridiculously large partitions, which are becoming increasingly prevalent.

But I guess I felt for the TrueCrypt developers, like this is all voluntary. It's all free. It's open source, fabulous software. We know that it's not dead because as we've been discussing, we're in the process of raising, well, we the community are in the process of raising money to do the first official audit of TrueCrypt so that everyone can know what it is. So, and this is a problem that you sometimes get into with free, open source software, is that it gets done, and then the world changes out from under it, and at some point people are going to have to come back and put in a substantial amount of effort in order to update it to new standards.

Leo: It's really because it's open source, and people do this in their spare time. It's for fun. It's not a paid project.

Steve: Yeah. And they did a fabulous job with TrueCrypt.

Leo: Yeah, yeah. And it does say, if you go to the site, updated October 11, 2013. I

mean, it's not like nothing's happening there. So if the main point is why hasn't the software been updated in six months, well, that's why. It doesn't really need to be. And I'm sure they're working on UEFI. Although, as you know, that's nontrivial.

Steve: It is nontrivial.

Leo: If you've relied on BIOS, you have to rewrite a lot of low-level stuff.

Steve: Yep.

Leo: Is it well documented? UEFI?

Steve: Oh, yeah. We have absolute all the information we need. It's a public open standard and becoming increasingly - one of the reasons I was able to put off, you know, I've been busy doing other things, and I was able to put that off is that we just weren't having many problems with people using UEFI because, for example, the Mac had moved there, but SpinRite was for the PC, and PCs were still staying BIOS-based. And so it wasn't becoming a problem. Now it's beginning to be a problem. So of course that has my, as we know, has my attention again.

Leo: Our last question coming up, I just want - a little programming note. If you didn't hear our interview with Ladar Levison last Wednesday, that is up now on Triangulation, TWiT.tv/tri. He's of course the creator of Lavabit. And he talks very candidly about what happened, why he decided he had to bring it down, what legal fight he's going on right now. And he mentioned something that we talked about before the show began, the new Dark Mail that he's doing in conjunction with Silent Circle. And that's exciting.

I asked Ladar, I said, come on, really, no email service can be secure because the nature of SMTP is that most of the time you're sending mail unencrypted. So few servers use encryption, it doesn't make any sense. And he agreed readily. He said, yeah, PGP or the like is the way, if you want secure email, you have to secure it on your side and give the guy on the other side the key. He said, but as Edward Snowden learned when he tried to get Glenn Greenwald to use it, and Ladar said, and even my lawyer, I said we've got to use PGP, and my lawyer couldn't figure it out. It's nontrivial, not easy to figure out. Our audience can figure it out, but normal people probably not. So I think that my sense is that his goal is to make that kind of encryption, just as Threema does, easy to implement in an email client. So we'll see. And of course Silent Circle is Phil Zimmermann, the guy who created PGP. So that's a good pairing.

Also, Triangulation today, I love this, we're going to interview Tom Standage. He wrote "The Victorian Internet," which was a great book. His newest is about social networks. It's called "Writing in the Wall: Social Media - The First 2,000 Years." And I think it's a great premise. It's the history of social networks from the agora in Greek times to coffeehouses in London in the 17th Century. Really a great - and then the rise in mass media, really a great subject. So that's coming up this afternoon.

Steve: And I have to say, Leo, that I received a number of tweets from people saying, Steve, you've got to go watch what Leo did with Ladar. So I had other people saying it was really a great Triangulation. And you were really up to speed, apparently. So I thought that was great.

Leo: Well, thanks to you, I mean, I knew what was going on because we'd talked about it. And I don't take any credit. I think the reason it was interesting was because Ladar was surprisingly upfront and frank, given his potential legal problems.

Steve: Given his limitations, yes.

Leo: Yeah. He didn't have a lawyer sitting next to him, just his dog. And he was great. I really enjoyed talking to him.

Steve: Neat.

Leo: Final question from Mr. Liquid Bread, Chris Phillips, who appropriately enough lives in Battle Creek, Michigan, home of Kellogg. He brings news of a CryptoLocker Prevention Kit": I ran across this packet of group policy changes, to prevent CryptoLocker from saving itself to your PC, on a Spiceworks forum. I've downloaded it, and me and my colleagues are still discussing whether to deploy this in our enterprise environment. Check it out and see if it's worth mentioning on your next Security Now! episode. He gives three links, four links if you include Steve's.

Steve: Actually, those are all mine. Yeah. So, first of all, this is what you and I talked about. There is something called CryptoPrevent. And that's - it's sort of a turnkey tool which will use Windows group policies to block CryptoLocker from doing what it wants to do. So this is a useful thing. I'm a little uncomfortable because it has a chance of triggering false positives, that is, your - the good news is CryptoLocker's behavior is a little odd in how it wants to install itself and run itself. And that can be used in order to block that behavior. The good news is that group policies are an absolutely well-documented, well-understood solution for, especially in a corporate environment, for managing PC behavior. But it's sort of a soft fix because CryptoLocker's future behavior could change so that in order - deliberately to work around the CryptoPrevent group policy fixes. However, for today, for now, it's a very clean and nice solution.

And so what I did was I tweeted a bunch of stuff, just before the podcast, so anybody who wanted to get the links could again go to bit.ly/SGgrc, or just check the SGgrc Twitter feed. And I created some bit.ly shortcuts: blockcl, prvntcl, and bleeping. The bleeping link, it's bit.ly/bleeping, is to absolutely the hands-down best page discussing CryptoLocker, talks about what it is...

Leo: That's a good site in general. BleepingComputer is really a good site, yeah.

Steve: Yes, BleepingComputer.com is great. And they've got a fabulous CryptoLocker page for anyone who wants to come up to speed. Oh, and that Spiceworks link that Chris put me onto, which is bit.ly/blockcl, I'm hosting their ZIP file on GRC, first, because I

didn't want to crash their server by tweeting it as I did crash Rob's the other day. And also because I verified the file is a legitimate ZIP before I opened it. I looked at it through a binary viewer to verify that it was a ZIP format and not executable myself. And then I opened it and looked at the files. It's beautiful because it's just a toolkit. And in fact I received some tweets back from corporate people who said, oh, thank you, thank you, this is just what we need for corporate deployment. So it doesn't do anything itself. It's very good documentation in PDFs, and the files that anyone who understood Windows group policy could use for establishing group policy settings that would absolutely lock CryptoLocker out of people's systems.

Leo: It is ironic that they send it out with a ZIP file containing what looks to be PDFs, which is exactly how...

Steve: I know.

Leo: ...CryptoLocker works. But okay.

Steve: So it's frightening. It's why I decided - I looked at it carefully myself and then hosted it on GRC.

Leo: Crazy. Crazy.

Steve: Yeah.

Leo: All right. Good.

Steve: So anyway, worrying, and this is the current big problem is CryptoLocker. As far as I've seen, the AV tools are still behind on this, and people are still getting themselves infected. So we really need to be careful with clicking on links.

Leo: We do, indeed. And the best way to be cautious is to stay up on what's going on. And if you listen to this show, you're miles ahead of everybody else. Steve Gibson keeps it all on the lowdown at GRC.com. That's his website, where you'll find SpinRite, the world's best hard drive maintenance utility. You gotta have it.

Steve: And allows you - you could peer into your hard drive with it.

Leo: Know if your employees are up to snuff.

Steve: Yup.

Leo: You can also get a lot of free stuff there, including 16Kb versions of this show for the bandwidth impaired, and full text transcriptions written by an actual human, the wonderful Elaine Farris. So you can read along as you listen to the show. We host full-quality audio and video of the show on our site, TWiT.tv/sn. And of course you can always subscribe. The podcast version's available almost everywhere you can get podcasts, including Stitcher and the like. We do this show currently, at least through the end of the year, on Wednesdays, 11:00 a.m. Pacific, 2:00 p.m. Eastern time. Next week, because of our change off summertime to standard time, we will be at - we move to GMT+8. So we'll be at 19:00 UTC, if you want to watch live. But if you don't, don't worry. Like I said, on-demand versions always available. Thank you, Steve.

Steve: Leo.

Leo: You're coming up for New Year's Eve, our special event.

Steve: Yup. I'm going to be with you at least for a while, while you're following users around the globe.

Leo: I'm going to spend the whole 24 hours. We start 4:00 a.m. New Year's Eve, end 4:00 a.m. New Year's Day. We are going to celebrate New Year's at least every hour, in a couple of cases every half hour, in every time zone, a countdown. And I hope, and in fact, if you're listening, I hope you'll participate, a viewer or a listener, in that time zone. You can sign up, there are many time zones unfilled, at TWiT.tv/nye. If you're in Papua, New Guinea, we need you.

Steve: I did ask to get late checkout the next day.

Leo: You're going to want it.

Steve: So that I can stay up with you for a while, Leo.

Leo: [Laughing] It's going to be a lot of fun. I've wanted to do this for years. Nobody would let me. 24 hours of New Year's from the TWiT Studios. All the shows will be on. All our people. We'll have bands. We'll have jammies.

Steve: Wow. You're going to be in your jammies?

Leo: No, I have been informed that I must wear a tuxedo the entire time.

Steve: Ah, there we go.

Leo: It's going to be fun. Thank you, Steve Gibson.

Steve: Thank you, Leo.

Leo: We'll see you next time. How do I say - how do you say "Papua"?

Steve: Oh, and by the way, no jury duty for me so far.

Leo: Oh, yeah. I forgot about that.

Steve: Not sure about tomorrow. But I've been watching it day by day. But nobody in the reserve group has been called. Apparently there are people who are not call-in. There are people who "you must show up" people. And so no one has been taken out of the call-in groups that I've been able to detect from looking at the website status. So I think I'm in the clear for this round.

Leo: Yeah. You did your duty. This Week in Google next. Thank you, Steve.