Listener Feedback #173

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-417.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-417-lq.mp3

SHOW TEASE: Time for Security Now!. Yes, there's another update from Microsoft. There's problems on the 'Net. There's no need to fear. Steve Gibson is here, protecting your security for eight solid years. Security Now! is next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 417, recorded August 14th, 2013: Your questions, Steve's answers, #173.

It's time for Security Now!, the show that covers your security, your privacy, your deep, most darkest fears and needs. And here he is, Mr. Fears & Needs himself, Steven "Tiberius" Gibson. Hello, Mister....

Steve Gibson: If you weren't sure what you had to be worried about at the beginning...

Leo: We'll find it.

Steve: ...you'll have all the details by the end.

Leo: We'll find something for you to worry about before this show is over. I worry about that. Actually, that's what I worry about. I don't want to make this show be something that people go, "Oh, what new, what fresh hell is this?"

Steve: No, I actually think we do a good job. And I hear from listeners who confirm their feelings that we do a good job of keeping this balanced. We're not the Hysteria Now!

show.

Leo: No, no.

Steve: I mean, I'm often very skeptical about some of these early things. Like I was the last one to agree, okay, maybe Stuxnet really did come from the government. It was like, I don't know, let's just wait. We're still grasping, we're still guessing, blah blah blah. And as it finally began to come out, it was like, well, it does really seem like a little joint effort between the U.S. and Israel, so maybe. But, so, yeah, I think, I mean, our anchor is technology.

Leo: Yes.

Steve: And so, yes, we will talk about the consequences of the technology. But that's not what this show is about.

Leo: No.

Steve: It's about technology.

Leo: And Leo revealing his credit card numbers.

Steve: That's our focus.

Leo: You know I did that.

Steve: And speaking - I know, last - yeah. Well, let's remind everyone again, Leo, so they can go back and scroll...

Leo: Well, no, I already canceled the card.

Steve: Okay.

Leo: In fact, I should have a new one by now, shouldn't I.

Steve: It's a great number to use now because it's invalid, and it's not all fives or something really lame like that.

Leo: Oh, you mean, like, when I have to give a credit card on the air. Yeah.

Steve: Yeah.

Leo: From now on I'll use that.

Steve: In fact, show it, and everyone's going to go [gasp]. But, you know, it's safe now.

Leo: It's safe.

Steve: I hope. I hope the cancellation order was well propagated through the entire system.

Leo: Yes. I hope so, too.

Steve: This is a special podcast.

Leo: Well, it's always been a special podcast.

Steve: Well, this is a particular one. How's that?

Leo: Okay.

Steve: Sharp-eyed Elaine noted a couple weeks ago that August 18th of 2005 was the date of Podcast No. 1.

Leo: Holy cow. That long ago.

Steve: Here we are, on the 14th of August. So between this podcast and the next podcast we celebrate an anniversary.

Leo: That's cool.

Steve: Meaning this is the final podcast - I can't even pronounce it anymore, padcast - the final podcast of our...

Leo: Well, you didn't get the memo that we don't call it "podcast." That went out in 2006. But that's okay.

Steve: Yeah. I'm-I'm-I'm old.

Leo: [Laughing] No, no. Call it a podcast.

Steve: Year Eight now.

Leo: Year Eight.

Steve: So next week starts our ninth year. Yeah.

Leo: When we started this show, Steve had hair, and mine was brown.

Steve: He didn't even have a ball.

Leo: We didn't even have a wall.

Steve: You didn't even have a ball to bounce on.

Leo: Oh, a ball, no. I barely had a microphone.

Steve: You were upstairs, crouched over, where the attic was...

Leo: That's right. I had to sit like this with my head tilted the whole time because the roof was coming down on me.

Steve: And you'd sort of crowd people into your little den and say, okay, talk now.

Leo: You know what's gratifying, sometimes shows, superannuated shows like this start to wear out. This show has not - far from worn out, it has grown consistently.

Steve: I'm an expert on that phenomenon because, for example, "Dexter," I'm dragging myself through this final season. It just - it's dead. So it's uninteresting, it's just like, oh...

Leo: And that's, what Season 6, 7? It's not even that far along.

Steve: No. And, but I mean, many - well, and "Galactica." Wow, kickass couple first years. Then they just kind of went, I mean, they were literally adrift with the writing because, you know, there's very much often an arc. And you see this, where the show takes off. It's successful. Now it's collected a huge audience and a huge advertising base. They can't stop. They just - they're unable to. One of the things I appreciate, somehow,

for some reason, "Star Trek" always stops before it becomes really bad. Even the "Next Generation."

Leo: Well, that's the tradition. It got canceled before it was even born, practically.

Steve: Yeah, but "Next Generation," seven seasons, thank you very much. And that's like, wait, I mean, and we don't have anything like that now. There's, like, nothing like a really good sci-fi series on. We've got a bunch of low-budget, walking around in the weeds shows, with every so often something flies overhead. It's like, okay.

Leo: Well, I'm happy to say this show, far from it, has grown in audience. It grows very consistently. In fact, the last two years have been the most growth, I guess because of interest in what's going on in security, but also because of your excellent reporting on things like PRISM, where people really are hearing the straight story, and sometimes the story no one else is saying.

Steve: In fact, one of our, I can't remember how he described himself, anonymous and hiding from the government or something, in our mailbag that I ran across this morning was someone saying, how could you be so right about this stuff? And again, it's not that I am prescient, it's that it comes from technology. It was always clear we should not put unencrypted data in the cloud. And so that's where TNO came from, and PIE. I mean, these are just - it's come from the technology, and that's what we allow to, I mean, that's our main driver.

Leo: Well, just to show you, the show "State of Surveillance" that you did, where you talked about what PRISM must be - and, by the way, in time have proven very accurate - is the most downloaded show of Security Now!, I think, with well over a hundred thousand downloads.

Steve: Wow.

Leo: And I don't - that's not including your downloads or YouTube or any of the other sources. So that's...

Steve: Wow, so just from you guys.

Leo: Just from TWiT.

Steve: Wow.

Leo: So that's pretty good. Congratulations. And I have a feeling we're on a roll. Year Nine is going to be even more interesting.

Steve: Well, I think we've got the right mix. I have had some complaints from people who say, oh, it just turned into a gossip podcast. And it's like, whoa, whoa, wait a minute. I think it's far from that. I think that maybe we were a little too tech-y and not enough conversation. And so in the last couple years we have, I think, evolved this into a little more discussion. And I think, when I look at the listenership that your main TWiT podcast has, and what technical details it brings...

Leo: No, it's more of a gabfest, yeah.

Steve: Yeah. And I think people want entertainment, Leo. I mean, yes, technology, that'll never - because that's who I am.

Leo: Gotta have both. Well, we've got to have both.

Steve: That's what interests me.

Leo: It's informed entertainment. How about that?

Steve: Yeah.

Leo: And in your case, really, you are easily - this is easily the geekiest show we do. And should be.

Steve: Oh, and baby, get ready, because we're about to dive into email encryption. And there's a reason no one's using it. So we're going to tackle that in the coming weeks. And as an example...

Leo: Good, good. But a Q&A this week, yes.

Steve: Yes, Q&A this week. So here we are on the 14th, the Second Tuesday of the Month, Patch Tuesday. No huge news. But as always, it's get your machines updated. It's probably more important now than ever because the bad guys are getting smarter about reverse-engineering what's happened. Brian Krebs did some nice reporting about this month's patches, so I'm just, rather than duplicating his research, I'm going to share the top of his blog posting from a day ago.

He said: "Microsoft has issued security updates to fix at least 23 distinct vulnerabilities in its Windows operating systems and other software. Three of the patch bundles released today," so, yeah, he did this, he did blog yesterday, "address flaws rated 'critical,' meaning that malware or miscreants can use them to break into Windows PCs without any help from users.

"Leading the critical updates is a cumulative patch for Internet Explorer that affects every version of the browser on nearly all supported versions of Windows." So all versions of IE. "In its advisory, Microsoft warns it is highly likely that attackers will soon develop

exploit code to attack the flaws addressed in the patch." So even Microsoft gets it now, that when they patch something, it's possible to figure out what they changed and then look at the unpatched versions and go, oh, we know how to leverage that. So, unfortunately, that's a cat-and-mouse game there's nothing we can do to fix.

"Indeed, according to Ross Barrett," continuing to quote Brian, "manager of security engineering at Rapid7, the IE patch addresses a vulnerability first demonstrated at the Pwn2Own contest at the CanSecWest conference in March of this year." So this was responsibly disclosed. The guys who came up with this got a Pwn2Own award. Microsoft then, that was March, here we are in July or August. So it's like, okay, well, they weren't in a big hurry to fix this, but they have. Now it's possible to reverse-engineer it from Microsoft's fix. So, important to do.

Second most important critical update is a so-called "browse-and-get-owned font vulnerability." And we've talked about that already. This affects users on Windows XP and Server 2003. And this is, you know, we were discussing this just in the last couple weeks, Leo, where the fact that the rendering engine isn't bulletproof, you can even have something as passive as a font file, which a browser will dutifully load in order to properly render the font that your web page asks for. That can take over your machine with you not having to deliberately do anything. And final, and then the final of the three, tackles several flaws in Microsoft Exchange that stem from a third-party component from Oracle called Outside In."

So Microsoft's fixing those three critical ones. And then the important ones are your typical local privilege elevation where somebody at the machine who did not, for example, have administrative rights, could elevate themselves to do so. And that's not good because you could have, like, locally installed software that is malicious, and the nave user doesn't realize that's happening. So, as always, update Windows. When I fired up my Win7 machine in order to run Skype to do the podcast, I got, oh, you have updates. It's like, yes, that's correct.

We seem to always have these news breaks on Thursday, the day after the podcast has been recorded. So we're reporting things which are, well, technically as stale as they could be. Or I guess if they happened Wednesday afternoon, that would be worse. But anyway, this still is the big story because it directly impinges on topics we've covered in the last couple weeks. And we've already been discussing the companies that this happened to. And the repercussions throughout the industry were amazing.

We were discussing just last week the company Lavabit because I brought it up in the context of the rumors, and I never actually saw confirmation. Now I have actually heard the guy himself, Ladar Levison, say that he did have an email account with the name Edward Snowden on it. So the owner of the ex, as in no longer, Lavabit service did confirm that there was such an account. But I'm getting ahead of myself.

Last week Ladar Levison, who is the founder and has been running Lavabit for 10 years, shut it down without warning, just blanked it out. And when this happened I actually - I realized this was too big for a tweet, so I created a blog entry on steve.grc.com, it's the first blog I've done in a long time, because I thought this was really significant. So if anyone hasn't seen my blog, it was quite well retweeted and blogged, and I think there are 69 comments following it, and a lot of people thought this was significant. What's significant is his reason for doing so. Right now, if you go to Lavabit.com, and I would urge our listeners to, there's nothing but a page that says, I'm sorry, I've shut the service down because, due to - and he's extremely encumbered by, unfortunately, our government, the U.S. government.

Leo: Even on his Democracy Now! interview, he had his lawyer sitting there to make sure he didn't say anything.

Steve: Yes. And there was a lot of interchange where he'd come to something, and he'd say, he'd look at him and say, can I say.... And his attorney would say, uh, no, you can't, let's go in a different direction.

Leo: So depressing.

Steve: So Ladar shut his service down because he said to do otherwise would make him complicit in crimes against U.S. citizens. And he refused to do that. He said, unfortunately, I can't tell you anything more than that. I can't even - I am forbidden to tell you what it was that I said no to. He can't even say that. And, I mean, it is - so yesterday, when I saw the Democracy Now! interview, I tweeted, "Feel like being depressed? Watch this 15-minute interview, and that ought to do it to you." And I got a lot of feedback from people saying, oh, my Lord. Anyway, it's a great interview. I would really commend our listeners - I didn't want - it's 15 minutes. I don't want to fill the podcast with it. Everyone who's interested can find it. But it's worth watching if this topic interests you. It is really pathetic what has been done. And, well, so the next day, Silent Circle announced that they were also preemptively - actually they announced they had canceled their Silent Mail service. Now, Leo...

Leo: We talked about Silent Circle. This is Phil Zimmermann of PGP fame.

Steve: We did. But more than that, Leo, they have Navy SEALs.

Leo: Oh, yeah, that's the one. And they're still scared. Although they were quick to say we haven't received a government subpoena yet.

Steve: Well, and their concern was, see - okay. So first of all, understand that both of these companies ran not really secure mail.

Leo: Right.

Steve: And that's the crux of the problem. In fact, that's what my blog posting made clear. That's the point I had made the week before. When we heard that Ed Snowden was using them, I thought - and that they were, oh, oh, secure mail, I thought, okay, what are they doing? I went over, and as I reported on the podcast the week before, I was unimpressed. They were doing mail at rest, they were doing, I'm sorry, encryption at rest storage, so that the email that they received unencrypted was then encrypted with the account's public key, and they only had access to the private key when the accountholder logged in. But the fact was, when the accountholder logged in, then they would use the password to decrypt the private key, which would allow them to decrypt their mailbox, essentially, and then send it to them either secure or not. Probably secure. One would hope that the links to their server would be secure if they were promoting

security.

But the point was, this was not actually secure mail. This was encrypted storage. But the nature of current email technology - and again, the point I made in my podcast was email is resistant to encryption. We're going to be talking about overcoming that resistance in coming weeks here, as soon as, I mean, starting with next week when we talk about PGP and S/MIME and GnuPG and so forth, technologies for encrypting email. But it is not easy. Email resists it. Which really is why it hasn't happened. I mean, HTTP web browsing, that's all encrypted now, largely. That's - the problem's been solved. Not so for email, and we'll go into why. But neither of these services were truly secure. I mean, and so, unfortunately, I think Ladar painted a bull's-eye on himself for the NSA.

Leo: Although he'd already been subpoenaed or something. He couldn't say what, but he'd received, I would guess, a national...

Steve: About 10.

Leo: Oh, he said 10. And were they NSLs? Did he say what they were?

Steve: Through the years he has responded to regular standard court orders. And because, he says, I'm going to obey the law.

Leo: I have to, yeah.

Steve: And if I'm given a court order for this data, I'm going to turn it over.

Leo: Oh, so something different happened, then?

Steve: Yes, yes, yes. This was probably overly broad, or maybe they wanted to install, like, now, see, his technology didn't allow him to decrypt what was there. They may have come looking - oh, and by the way, this is about two weeks, wait, so two weeks or four weeks. This had been going on for some time. So this may very well have been related specifically to Snowden and that, where someone said we want this data. And so whatever it was, he was made to feel uncomfortable at a level where previous court orders have never been a problem for him, but this caused him to say, I give up. I cannot be complicit.

Leo: Do you want to speculate?

Steve: I really can't.

Leo: It would be rank speculation. But...

Steve: Yeah, I can't. I mean, we just...

Leo: Okay. So what we know is that the feds, it wasn't real security because the feds could just watch incoming and outgoing, and it would be unencrypted.

Steve: Correct. And even - yes. Well, and even there's one other little glitch here, and that is they could have said, when someone logs in, we want their decryption key. Because when they log in, you get their decryption key.

Leo: Oh. You do? Is that true?

Steve: Yes. And that's the problem.

Leo: Oh, they'd have to because otherwise he couldn't send the mail.

Steve: Right, right.

Leo: Okay.

Steve: And so this was the weakness. And this is why I said it wasn't - I think at the top of my blog posting I said something like - I put "nearly secure" or something in quotes.

Leo: Yeah, and you told me that. I told you last week, oh, I bought 10 years' worth of Lavabit. And you said, well...

Steve: Yeah.

Leo: Nice, but...

Steve: Okay.

Leo: I also use GNU Privacy Tool, as we're going to talk about at some point, to protect...

Steve: So here was the problem. Both of these organizations - email is store-and-forward, which means - and both of these, both Lavabit and Silent Circle had hundreds of thousands of customers. I mean, they were ongoing, successful operations. And but the fact that it's store-and-forward means that mail is coming in and being stored encrypted. Then, when you connect up using POP or IMAP, your client is able to get this, decrypt the mail, for it to be sent to you.

The fact that both companies preemptively shut down, what that did was that meant they were in receipt of email that had not been picked up, and all they could do was say we're sorry. And the Silent Circle people, they put their Navy SEALs on either side of the door, and they said, look, here's the problem. If we were to announce that we are going to be shutting down, that window of opportunity would allow the federal government to come in and get our stuff. They destroyed their servers at Silent Circle. And so their customers have been inconvenienced and are complaining. It's like, wait a minute, there was email that I had not picked up. And they said, we know.

Leo: That's the point.

Steve: Yes. Yes, because if we had given...

Leo: You and the NSA hadn't picked it up yet, yeah.

Steve: Exactly. Exactly.

Leo: Wow.

Steve: So, yeah. Now, I thought about this. I cogitated and ruminated for a while. And I tweeted something that has been more retweeted than anything I have tweeted for a long time. What I tweeted, and this might have been over the weekend, I said, "We can no longer safely delegate our security because our delegates may be compelled to secretly violate our trust." Which I think very succinctly states the problem. We can no longer safely delegate our security because our delegates may be compelled to secretly violate our trust. I mean, and this is the problem with this whole situation we find ourselves in.

And this is what every, I mean, commercial companies are very upset. I mean, Google is feeling this. Microsoft and Yahoo! and these companies named in the PRISM slides are feeling really put upon. And we discussed this last week because there was some commentary, I don't remember who it was, might have been Micro- was it Microsoft, where they were explaining how they're begging the federal government to let them say something, and the federal government says no.

Now, Bruce Schneier, our favorite cryptographer and smart guy, weighed in on this with - he covered, in his blog, the news of Lavabit's decision and had a nice little summary. He said: "This illustrates the difference between a business owned by a person, and a public corporation owned by shareholders. Ladar Levison can decide to shutter Lavabit - a move that will personally cost him money - because he believes it's the right thing to do. I applaud that decision," says Bruce, "but it's one he's only able to make because he doesn't have to answer to public shareholders. Could you imagine what would happen if Mark Zuckerberg or Larry Page decided to shut down Facebook or Google rather than answer National Security Letters? They couldn't."

Leo: They can't.

Steve: "They would be fired." He said: "When small companies can no longer operate, it's another step in the consolidation of the surveillance society." So, oh, and I want to make sure I don't fail to mention that Silent Circle itself is still an ongoing enterprise. They have Silent Talk and Silent Chat. It's only Silent Mail that they shuttered and that they shut down. Lavabit's gone completely because all they offered was not-really-secure email. Silent Circle also offered not-really-secure email, but their main two products, their main two offerings are end-to-end secure, TNO, PIE, all the good acronyms. That stuff they did absolutely right because it's not - because they were able to build a standalone, truly secure solution. This is the problem with email is it's got a huge compatibility problem because we're trying to add security to a fundamentally unsecure protocol. They were able to, and anyone can, I mean, it's not difficult to do security right.

So I wanted to make sure we don't - I didn't miscommunicate that Silent Circle themselves are gone. It's only their not-really-secure email solution. And they were never really happy with it either. They did it because people wanted it. And they said, well, we really can't. We can't. And people said, yeah, well, do what you can. And so do what you can is gone, and only the endpoint-to-endpoint correctly done solution is still up. And they're in no danger at all. Notice these guys shut this down preemptively. They haven't needed to shut down the others because they absolutely know that it doesn't matter if the NSA comes knocking. That's the way, if you design the system correctly, it doesn't matter. And they did.

Leo: I should, I mean, they had less to lose than Mr. Lavabit. I mean, their main business was not this. It was encrypted email, or IM and phone calls.

Steve: Yes. His was entirely that.

Leo: And they also said, unless they've said something since, that they had not received a government subpoena yet. They were doing this preemptively.

Steve: Correct. That's absolutely right.

Leo: And I might point out it's excellent marketing.

Steve: Yes.

Leo: Without much cost because this wasn't...

Steve: With or without...

Leo: ...much of a business to begin with.

Steve: Now, I will also point out, Leo, as far as we know, Ladar...

Leo: He's out of business.

Steve: He had no Navy SEALs, Leo.

Leo: No. And Ladar - and I respect Ladar because he - this wasn't a big business. He said he was making something like 50 to 100,000 a year. But it was his livelihood for 10 years. And he's basically quitting the job and saying I can't do this job properly, thanks to the U.S. government, so I'm not going to do it at all. And he's now going to have to find a job. So that's a significant thing to do, and props to him. And I at first was like, wait a minute, I just paid you for 10 years. And then I said, well, you know, that's cool. In fact, he has raised, what was it, $90,000 for his defense fund and needs more, I'm sure.

Steve: Yeah. And they also said, well, you could do this somewhere else, as in a different country. And he says, well, I live in Texas. I like Texas. I don't want to move.

Leo: Yeah. Real respect to him. I'm not sure about the Silent Circle thing. Their marketing has always been a little weird. It does seem a little self-serving to say, hey, nobody's asked us, but just in case, we're going to shut this down. And it's not a primary part of their business at all. Right?

Steve: No.

Leo: So, I mean, but the real message to everybody is that store-and-forward email is not - didn't Google just say don't expect privacy if you use Gmail? They just said that.

Steve: Yeah. And...

Leo: And they're being honest because there isn't - it isn't private.

Steve: The other point that I will be making when we discuss email encryption is that, even then, you are encrypting what's in the envelope. There is no way to encrypt the envelope itself.

Leo: Right. If you can't see the address, it's not going to get delivered.

Steve: Correct. Which says that there will always be...

Leo: Metadata there.

Steve: ...metadata leakage. That's why Bitmessage is very interesting. So don't any of our listeners think I'm not aware of Bitmessage.

Leo: Oh, okay.

Steve: Bitmessage does not leak metadata. It's a peer-to-peer network where you can send things to each other. It is absolutely secure. And there's no metadata leakage. Now, I almost considered aborting the encrypted email discussion for this reason, because Bitmessage is interesting. It looks very solid. But I don't think that's practical, either. I think we need to talk about the standards because there are, I mean, basically what PGP is and what S/MIME is, is a standard for encrypting email. And it's certainly useful to understand it and have that as a tool in your toolbox.

But never fail to remember that it's just your - the fact that you're sending encrypted email will always be known. There's no way to hide that. But with Bitmessage, everybody gets everything. It uses the Bitcoin blockchain technology. So basically you're receiving the entire community's sendings, and your local client, in the privacy of your own computer, extracts that which is meant for you. So nobody has any way of monitoring this. It's very clever. So we will of course be talking about that, as well.

Leo: You know, I don't have anything to hide. But I use PGP encryption. I understand - I'm not sure how far I want to go. I mean, so they get the metadata. In my case it doesn't be a big deal.

Steve: Yeah, exactly.

Leo: It's more a statement. It's more a statement.

Steve: Yeah. And I can certainly see, for example, between corporations and their law firms, corporations and their subcontractors, it's very - you could easily run across a situation where you need to send documents and files as email attachments encrypted to other people, not because you're planning anything nefarious, but because it's your company's private business.

Leo: Privileged communications. None of your business.

Steve: Yeah, and as I said, my favorite example that comes on this notion of people saying, well, why do you care about encryption if you have nothing to hide, is the webcam in the bathroom. Somebody sent something, a tweet I saw that I appreciated. He said, what I do in my email is boring and mundane. And I said, yes, that's much like most people in the bathroom. But still, who needs to see it?

Leo: Exactly. Exactly.

Steve: Not very interesting.

Leo: Yeah, yeah.

Steve: So I mentioned, too, I mentioned last week that there had been a mention on ABC's "This Week With George Stephanopoulos" Sunday show that I had not had a chance by then to track down. And that was the news that, in 2011, that the FISA Court itself had ruled that what it was being asked to do was unlawful and unconstitutional, and that that report had been suppressed. Turns out...

Leo: Yeah, this pissed me off.

Steve: That was on - yes, I remember it did. This was October 3rd of 2011. And David Corn, reporting for Mother Jones on June 11th, so just a couple months ago, in the wake of the Snowden revelations, he tracked this down. His reporting said: "In the midst of revelations that the government has conducted extensive top-secret surveillance operations to collect domestic phone records and Internet communications, the Justice Department was due to file a court motion Friday," so just recently, "in its effort to keep secret an 86-page court opinion" - this is the FISA Court opinion - "that determined that the government had violated the spirit of federal surveillance laws and engaged in unconstitutional spying." So this is the Justice Department filing a court motion to keep this 86-page court opinion secret.

So David continues: "This important case, all the more relevant in the wake of this week's disclosures" - oh, so this was just when this was happening - "was triggered after Sen. Ron Wyden, Oregon..."

Leo: God bless him.

Steve: "...a member of the Senate Intelligence Committee, started crying foul in 2011 about U.S. government snooping. As a member of the intelligence committee, he had learned about domestic surveillance activity affecting American citizens that he believed was improper. He and Sen. Mark Udall of Colorado, another intelligence committee member, raised only vague warnings about this data collection because they could not reveal the details of the classified program that concerned them. But in July 2012 Wyden was able to get the Office of the Director of National Intelligence to declassify two statements that he wanted to issue publicly.

They were, one, "On at least one occasion the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to the Section 702 minimization procedures used by the government was unreasonable under the Fourth Amendment." And, second, "I believe that the government's implementation of Section 702 of FISA [the Foreign Intelligence Surveillance Act] has sometimes circumvented the spirit of the law, and on at least one occasion the FISA Court has reached this same conclusion." So at least that he was able to declassify last summer. And that's different from and prior to this 86-page court opinion which apparently Justice is now trying to keep from having being made public. So anyway, that's the details on what we heard two Sundays ago. I just wanted to...

Leo: I really don't understand why the government feels like this needs to be kept secret. This doesn't need to be kept secret. And frankly, in this case, secrecy is being used to hide incompetence, malfeasance. There's no reason to keep this secret. You're not - this doesn't protect us against terrorists, to keep this secret.

Steve: Yes. Yes. It's like them classifying the number, the integer number of plots that have been foiled. They said, oh, that's classified. What, because it's two? Or because it's 200?

Leo: It's embarrassing, probably.

Steve: It's ridic- probably is, yes, unfortunately. But, yeah, you're right.

Leo: I understand that there's some things you have to keep secret because you have to protect the means and methods so that the terrorists can't use counter methods. That's understandable and fine. That's not what this is.

Steve: Well, there's an old joke, Leo, in business. Never ask your attorney if you can do something.

Leo: Right, because they'll say no, yeah.

Steve: They say no. I mean, that's the safe answer. No.

Leo: Yeah, no, it's a bunch of - use a bunch of attorneys, yeah.

Steve: Never ask your attorney. Well, no, but my point is, why not just stamp everything with "Top Secret"? Why, I mean, the point is, if you have the ability to declare things top secret, and you've got a big stamp...

Leo: Might as well.

Steve: Why not?

Leo: Why not?

Steve: Yeah, what's the danger?

Leo: I'll tell you why not. Because we live in a republic where it is important that the

people who are governed have the right to weigh in on what we're doing because it's in our name. It's in our name.

Steve: We're paying for it, yes.

Leo: We're more than paying for it. They're representing us. And I have to point out, at least we can still talk about this freely and openly without consequence.

Steve: Yeah.

Leo: Nobody's hauling you or me off to jail. We are not in a gulag situation. But nevertheless, the amount of secrecy that is being employed by our elected representatives and, worse, unelected bureaucrats, is not acceptable. And I applaud Ron Wyden for doing what he can. But we've got to go a lot farther here. This is not okay.

Steve: Well, and the good news is it's been opened. And a lot of people are now looking at this very closely. And many people were surprised. This was a rude awakening, not just to the public, but to our lawmakers.

Leo: Yeah. President Obama said, well, I wasn't going to do this so fast. I was going to do it. Sounds like a six year old. No, really, I was going to do this.

Steve: That was an unimpressive - that was an unimpressive press conference.

Leo: Well, there were things to be gained from it. For instance, he acknowledged we have an unprecedented ability to collect this information. That's a real acknowledgment. That's saying...

Steve: Because the growth of technology has now created this facility.

Leo: That's really, in a way, going farther than we've gone before, to admit we can do it. And he said they're going to try - unfortunately, it's General Clapper that's choosing the members of the commission.

Steve: Oh.

Leo: The last guy you'd want to do this since he lied to Congress last spring.

Steve: James Clapper, yup.

Leo: But at least they're going to appoint a commission, and one hopes there'll be some work done in this direction. It's very disappointing.

Steve: Well, bottom line is we know. And we may have known or worried, I mean, it's funny, one of the questions, I think it was that same question, where someone said, Steve, how did you know? It's like, I didn't really know. I just knew that the idea - I was worried about bad guys, not our government. And that's where TNO and PIE came from. I wasn't worried about our government. Now it's really worrisome.

So a little mistake surfaced in Android's random number generator.

Leo: Oh, yeah. Oh, yeah. This is not the first time random number generators have been blamed.

Steve: Oh, and our listeners who have been following the podcast, any of you who've managed to survive eight years, how many times have we talked about this? I mean, remember, this is why I spent all that time on the so-called "ultra high entropy pseudorandom number generator." Remember that Netscape's first SSL implementation, SSL 1.0, it was immediately in trouble because it was generating bad random numbers.

Crypto absolutely needs randomness. It absolutely does. Anytime you have a communication, you are generating, you are encrypting that communication using symmetric encryption and a random key. Then you're often using - you're either keeping that key secret, or you are encrypting the key, the hopefully random key, with asymmetric encryption because you can't afford asymmetric encryption, too slow to encrypt the whole thing. So you absolutely have to have good random numbers. And you absolutely never want to use the same one again because, if nothing else, bad guys could be capturing all the ones you've generated and just trying them. That's better than trying them all. Capture the ones that you've already used. Maybe you'll use it again.

Well, guess what? Android does. It actually generates identical, not just weak, not just poor, not just not all 256 bits are random, but all of them are the same. None of the bits are random. So it turns out that a weakness was discovered quite a while ago, back in Christmas of 2012. On December 25th, Nils Schneider discovered a problem which affected some implementations of Bitcoin. And it's not exactly clear how this took eight months to sort of sift out and finally get attention. But on the Bitcoin.org site, they blogged on the 11th, so three days ago: "We recently learned that a component of Android responsible for generating secure random numbers contains critical weaknesses."

Okay, now, that's like saying, well, I don't know, I don't have a good analogy prepared. But that's ridiculous. It's actually generating duplicate random numbers. Okay, "...contains critical weaknesses" - certainly that's true, at least - "that render all Android wallets generated to date vulnerable to theft." And I'm going to explain exactly how vulnerable in a second. But they say: "Because the problem lies with Android itself, this problem will affect you if you have a wallet generated by any Android app."

Leo: That's the sad thing. Any.

Steve: Yes.

Leo: None of them do it right.

Steve: Well, because they're all using...

Leo: They're all dependent on the...

Steve: ...the Android, give me a random number please, function.

Leo: Although that was a mistake, clearly.

Steve: It just gave them the same one. "An incomplete list would be Bitcoin Wallet, blockchain.info wallet, BitcoinSpinner and Mycelium Wallet. Apps where you don't control the private keys at all are not affected." That is, where you've provided a private key from somewhere else, rather than it being something that the wallet generated. "For example, exchange frontends like the Coinbase or Mt. Gox apps are not impacted by this issue because the private keys are not generated on your Android phone."

Leo: Now, I'm using, I mean, we use Bitcoin wallets on Windows and Mac, which use their - I don't know what [indiscernible] they use. Are those okay?

Steve: Yeah. And the good news is those are so well vetted that, well, early, early Windows had some random number generator problems. But Microsoft understood that and fixed it. So, and Mac I don't think ever had any problems because they came from UNIX, and the UNIX guys figured this out a long time ago. So Nils explains. What's the problem? Bitcoin uses Elliptic Curve DSA, Digital Signature Algorithm. Elliptic Curve DSA, ECDSA, requires a random number for each signature. If this random number is ever used twice with the same private key, that private key can be recovered. So all it takes is the mistake of ever using the same random number twice.

He says in his blog, where he explains this: "This transaction was generated by a hardware Bitcoin wallet using a pseudorandom number generator that was returning the same," and he has in quotes, "'random' number every time." It's just - it was - it couldn't have been written into the code, here, this is a lot of random bits, just only ask for it once. No. Can't be the case.

So what Nils did was he examined the Bitcoin blockchain, and he discovered a few vulnerable Bitcoin addresses. After some research, because we know that the blockchain has an anonymity problem, it's possible to de-anonymize in some instances, after some research he says he was able to contact the owner of those vulnerable addresses. And he said, "He allowed me to spend the funds." So back last Christmas Nils knew of this problem, analyzed the blockchain, found a weak wallet, tracked down the user, and with that owner's permission, took the money from his wallet.

Leo: Wow.

Steve: So...

Leo: Wow.

Steve: That cool?

Leo: You know, I installed a Bitcoin wallet on Android when I first set up Bitcoin, and we have about seven - thank you to everybody anonymously who's donated bitcoin to TWiT. We have a bitcoin donation QR code and number on the front page, and we've got about seven bitcoins, which is, what, 750 bucks, something like that.

Steve: Wow, cool.

Leo: Yeah. And I did set up a Bitcoin wallet on Android. But fortunately it crashed. It force closed so often, I just said, well, this isn't working, and I erased it.

Steve: Our first clue.

Leo: Thank God I never got it tied into my account. Yeah, that was a clue. That was a good, you know, okay.

Steve: So it is possible now, you want to update Android to make sure that this problem is fixed. So verify that you've got a version where it is.

Leo: Oh, interesting. So they have fixed it in later versions.

Steve: And you can rotate the keys, then. And in fact this blog posting goes on to talk about specific implementations. And you can just - you can regenerate keys, and then you'll be okay again. So, although, really, I wouldn't put a lot of money in a mobile platform wallet. Maybe have an account there where it's your play money. But if you've got serious bitcoinage, you just don't want it on a mobile platform. It's true, all of these platforms are at risk. This podcast covers that constantly. But mobile is really just more at risk.

Leo: Yeah.

Steve: So I would be - I'd just put - don't have the keys to all of your coinage on a mobile platform. I mean, really, just move over play money over there.

Okay, now, this was really interesting. There are security experts who now believe, based on the statistics they are seeing - 236 days remaining until XP is no longer updated. Hackers are believed to now be saving XP exploits for after that curtain drops because Microsoft will then no longer patch XP. So what's happened is the cat-and-mouse game

we were talking about, the find a problem - the value of an exploit is a function of how long it's able to be used before it's discovered and then patched and closed. So there's this game of new vulnerability found. You really want to keep a low profile.

It's like the FBI, who apparently have ways of getting spyware into people's machines. But it's very rare that they will do something as high profile with that as they did with Tor recently, where they basically let something go that was quickly found, but there was a window of about three days during which anybody who got infected probably got a knock on the door from the FBI. Normally you want to keep these things on the QT so that they're not widely exploited. So they're using phishing attacks, limited attacks, rather than huge sprays. So you can see the advantage if there are vulnerabilities in XP. The fact is XP's deployment, I think we're still at 43% was the number I just saw.

Leo: Isn't that amazing?

Steve: Corporations do not want to move because it's expensive. Microsoft just doesn't give away Windows 7.

Leo: And XP works.

Steve: And it works. That's exactly the point.

Leo: Why replace something that works?

Steve: Works just fine. So the problem is that, come 236 days from now, I've got my little counter over on my Win7 machine telling me how many days left of XP, Microsoft won't fix these anymore. And so the bad guys are now building up a stockpile because, at that point, I mean, and Microsoft really doesn't go back and fix anymore.

Leo: So they're not - but, now, they'll have to be new flaws, not, I mean, they've fixed everything to date.

Steve: Yes, they are, well, they fix everything they...

Leo: So it'll be newly discovered flaws.

Steve: Yes. They fix what they know. And, again, you can see Microsoft saying, well, that'll get them off of XP. It gets...

Leo: Yeah, that's too bad.

Steve: It keeps reminding people. It is too bad. But unfortunately it's not safe. I wanted to quickly mention GRC's cookie forensics page. Many people responded, too many for

me to talk about in the Q&A, who never knew about my little cookie forensics. And many of them thought, well, they were surprised by what their browsers were doing.

One person posted in the newsgroups, so I saw that. He wrote, he said, "I deleted cookies using IE10," so he's on IE10, "the gear icon, safety, delete browsing history, and then checked delete cookies, and restarted IE10. With first-party cookies accepted and third-party cookies blocked, the checkcookie page flags problems only for third-party session and third-party persistent cookies of type icon, embed, and object. Checkcookie color codes these all blue as browser leakage bug." And I responded to that posting, I said, "Wow, that's still there? Amazing." And I said, "I recall that it was due to IE that I added those tests." It's impossible, it turns out, to keep Internet Explorer from transacting third-party cookies if they're added to those non-page items, which is easily done." And I finished just by saying, "Incredible."

So this is IE, where you have explicitly turned off third-party cookies, and you haven't. Because it turns out, remember that many things are fetched by the browser, not just JPGs and images and JavaScript and so forth, but the favicon is the little thing, the icon in your URL that many sites customize. Google's got the little colorful thing. GRC has got the little ruby G icon. You probably have one, Leo, for TWiT.

Leo: I do. It's my head. Well, TWiT is the TWiT logo and then on Leoville it's my head.

Steve: And it turns out that, since the browser is querying that, you can respond to that query for a favicon with a cookie, and IE will start sending that cookie back.

Leo: Oh, that's good to know [laughing].

Steve: Well, yes. And the embed, the embed tag and the object tag, all three of those you cannot shut down, no matter what you do. And we discovered this years ago when I did the cookie forensics. And I think I saw it somewhere, so I thought of everything possible that I could test cookies on, and then that's why there's, like, eight different little bubbles in the cookie forensics page. Anyway, once again, if I've convinced people they ought to go check, I created a shortcut because I still don't have this linked on GRC's main menu: bit.ly/checkcookie, all lowercase, c-h-e-c-k-c-o-o-k-i-e. And our browsers are broken. I mean, even today. And my plan was to use these to force the vendors of browsers to clean up their acts, and I just never got around to it, so.

Okay, now, Leo, you've got a 15-second YouTube video. This just surfaced while I was pulling things together. I have not had a chance to test it scientifically. People are skeptical. It's just wacky. But it's just too fun not to share. And that's what this podcast is for.

Leo: Here we go. Is it supposed to look like that?

Steve: Yeah, in the beginning.

Leo: Oh, okay.

[CLIP] MALE VOICE: The best way to test it is with a meter.

Leo: Oh, let me rewind so we can get the audio here.

[CLIP] MALE VOICE: Everybody has batteries in many different kinds of devices. And sometimes it's useful to know if a battery is good or bad. Of course the best way to test it is with a meter. But not everybody has a meter, and you don't always have one handy. We're going to how you a simple test, in seconds, to determine if a battery is good or bad.

Leo: Great Baltimore accent here, by the way.

[CLIP] MALE VOICE: Here are two batteries. The Energizer is good. Alkaline batteries are rated for 1.5V, and this one is brand new. It's showing 1.65. That's excellent. The Duracell is showing 1.2, and as soon as it gets any load on it, it goes less than that. Believe me, it's beat. Without a meter, how can we tell the difference? With a simple bounce test. A good battery will not bounce, and it will land with a thud and frequently stand up. A bad battery will take several bounces and usually fall over.

Leo: Huh.

[CLIP] MALE VOICE: It works for all kinds of alkaline batteries...

Leo: That's really interesting.

[CLIP] MALE VOICE: ...AAA, AA, C, or D. And we don't know exactly why it works, but it probably has to do with the chance of density of the material. In any case, it always works, and it works like a charm.

Leo: That is a great hack.

[CLIP] MALE VOICE: Good luck testing your batteries.

Leo: Oh, wow.

Steve: Isn't that fantastic?

Leo: That's bajarider1000, if you want to watch the video yourself, bajarider1000 on YouTube. With a great Baltimore - Balmore accent there. Nice mid-Atlantic accent. That's really interesting.

Steve: Okay. So, now, several people sent back to me, because I tweeted this, so if anyone wants to find it, you can also check @SGgrc's, my Twitter stream, and you'll see the link, and I go, WHAT?!?!?! and so forth. They said, wait a minute. He's got two different brands of battery. Now, that's true. So if you were to do this scientifically, you'd get a couple fresh of each, drain one of each, and then do bounce tests. Although someone named Jesse Madonna sent back, he said, Steve, have you tried it? I have access to a multimeter, and this bouncing test works.

Leo: Wow.

Steve: So anyway, if it's true, fabulous hack. And remember, the way you remember it is you want to - the battery that bounces, you bounce out of your remote control.

Leo: Bounce the battery that bounces.

Steve: Bounce the battery that bounces. So, wow.

Leo: Wow. That is really interesting.

Steve: I love it. So, "Elysium."

Leo: You saw it.

Steve: Disappointed.

Leo: Aw. Yeah, I think a lot of people were.

Steve: Yeah. It's - and when I tweeted that, which I did yesterday, or, no, Monday, many people said, did you like "District 9"? Because we all know that "Elysium" was made by the same guy.

Leo: Neil Blomkamp, yeah.

Steve: Loved "District 9."

Leo: As did I.

Steve: Oh, my god. "District 9" was so fun and new and fresh and original, and also in some ways ridiculously over the top, like with the power of the alien guns. It was fantastic. "Elysium" had none of that. It had a ridiculous cartoon character bad guy, Kruger, that just...

Leo: I liked him. He was really bad.

Steve: Oh, Leo.

Leo: It's more of an action film than "District 9" was.

Steve: Okay, well, so you're welcome to like it. I was very disappointed.

Leo: I will tell you...

Steve: But I didn't have high hopes.

Leo: ...my ratings I gave on NSFW last night, I thought an A for "District 9" and a B/B+ for "Elysium." Not as good as, but not horrible. Now, I saw it in the third row of an IMAX theater, so it was a big film.

Steve: Yeah. I did want to mention that one of my favorite movies of the summer just came out on disk, and that's "Olympus Has Fallen."

Leo: Really. You liked that.

Steve: Yeah. It may have been the first one that Jenny and I saw at the beginning of the summer movie season.

Leo: That was the one about the White House being invaded or something, yeah.

Steve: Yes. Yes, standard, straight-up action flick. I thought it was fun. And when I staggered from the theater, I immediately tweeted that I was still breathless after 10 minutes. I mean, that was - I thought it was great. And I do want to mention, finally, that I have discovered "Breaking Bad."

Leo: Well, it's about time.

Steve: I know. I know.

Leo: Last season, dude.

Steve: There was so much noise about the start of Season 6. And the gal that used to cut my hair was talking about it five years ago. She said, oh, Steve, are you watching "Breaking Bad"? So she induced me to, like, get the first season. And I think I watched the first two episodes, and he was wandering around in his underwear in the desert, in his RV, and I thought, no, okay, I don't think this is for me. But, oh, my goodness. And so it's my - sort of my background when there's nothing else to watch. And actually we're sort of in a dry spell at the moment before - the good stuff is over, and...

Leo: "Homeland" is coming back, you know.

Steve: Oh, good, good, good. So there are a few things. I do like "The Network." I know that you're not a fan of that. But I do like that. And as I said, I'm struggling to make myself keep watching "Dexter."

Leo: You mean "Newsroom"?

Steve: I'm sorry, yes, "Newsroom."

Leo: Okay. It does harken back a little bit to "Network," the movie, where "I'm mad as hell, and I'm not going to take it anymore."

Steve: So anyway, "Breaking Bad," I just wanted to mention that, yeah, okay, I'm finally up to speed on it.

Leo: How far - you watched all five previous seasons?

Steve: No, no, no, no, no. I think I'm somewhere in the middle of, like, Season 3. He's now struggling with his wife, who has found out.

Leo: The dude gets wilder and wilder.

Steve: It's just - it's just - I finally understand that nothing, apparently nothing really big is going to happen. It's just the story of these two...

Leo: A few big things might happen.

Steve: Okay.

Leo: Stay tuned.

Steve: Anyway, I'm really having fun.

Leo: Stay tuned.

Steve: I'm really - I'm going - oh, and one thing that happened was, that had me thinking of this whole NSA nonsense, is I wanted - I was very curious to know about fulminate of mercury because I'd sort of heard...

Leo: Right, contact explosive.

Steve: I was afraid to Google it.

Leo: Yeah, you're right.

Steve: Because, you know?

Leo: But you can. And there's good recipes online. We used to use it in college because it's a kind of nondestructive - by the way, there is an article I just read on the science of "Breaking Bad." And the amount of fulminate of mercury that he got out of, what was it, I can't remember what he made it out of, was unrealistic. The amount he had in his hand, unrealistic. And it would have gone off in his pants long before he got to use it. So it is, it's a contact explosive which, when wet, does not explode, but as soon as it's dry will explode on contact. So we used to make it in college and paint it on the floor, and then ring a loud bell. And when my roommate got up and put his feet on the floor, it'd go pow pow pow pow pow. And he'd dance all the way out of the room. Great fun.

Steve: You remember that, yeah.

Leo: Easy to make.

Steve: I think ammonia's involved.

Leo: Standard household chemicals.

Steve: And the ammonia dissolves, and it dries, and...

Leo: Yeah. I don't recommend, by the way, in any form or fashion. I did not make it. It was one of my roommates. I just watched the results.

Steve: Those chemistry majors were fun to have around.

Leo: They're fun to have around. And I don't know what "MythBusters" did or did not do. Apparently they tried it, it didn't work. But you know what, it's real.

Steve: Oh, it definitely works.

Leo: You don't want to carry it in your pants.

Steve: We were playing with it at Berkeley, Leo. It, yeah...

Leo: All right. So, Burke, did you try this experiment? And he bounced the batteries, and...

BURKE: [Indiscernible].

Leo: And you can tell whether they're good or bad based on the bouncing? Now, you have to do it on a hard surface; right? I'll do it on the clipboard.

Steve: Oh, cool. So we have some initial anecdotal evidence.

Leo: Well, I'm not very good at this. Lower? Okay, that's got to be bad because I could not get that to stand up. It's like that high; right? The bounce that counts. That one's good. Right? Didn't stay standing up, but I don't know.

Steve: No, it's not - it doesn't have to stand up. It's just the bounce.

Leo: This bounced a lot; right? So it's how much it bounces; right? That's kind of more heavy. I bet you could weigh these. You think? I don't - give up. It's silly. Okay. On with the show. We don't have time for this.

Steve: [Laughing] Okay. So if you've got that PNG file, Leo...

Leo: I do, indeed. In a font I haven't seen in many moons.

Steve: The people who are looking at video are seeing a screen that many testers of the

SpinRite research are seeing. This is where we are at the moment. We just discovered yesterday that I think four people or four machines out of maybe more than a hundred, in one particular point in the code, have interrupts disabled where they never should. So I finally figured that out. We solved a problem that had been dogging us.

That screen that you're looking at is where I am in sort of starting from first principles of a machine and figuring out what's on the PCI bus, what's the BIOS showing, what controllers do we have that we're able to talk to directly because SpinRite will be directly interacting with the hardware at a level much lower, at the lowest possible level, for the first time. We've had some very hopeful results, by the way, with MacBook Air and Mac Minis because the older ones at least are running in the non-AHCI mode that SpinRite, the initial version of SpinRite, 6.1, is being developed to operate with. So it's going to be screamingly fast.

People have been successfully booting SpinRite on their Mac, I'm sorry, booting the test code, because SpinRite still doesn't run, of course, because of the keyboard problem. The older Macs that have optical disks, we're able to boot, not with USB because Apple didn't put USB BIOS support in those. But they've got optical disks, so you can burn a disk and then boot SpinRite that way. The ones without optical disks do have USB BIOS support, and we are booting all, you know, FreeDOS, the GRC version of FreeDOS 1.1, on USB sticks, like everybody's doing it now who is working in our test group. So that problem's been solved at that level. I'll be turning my attention to that as the next thing we do.

But the next piece of work, which I'll start after the podcast, since everything to date, we've just finished with the 10th release of SpinTest, and we now know what everybody's got. We're detecting everybody's hard drives, no machines are hanging, and we're moving forward. So anyway, it's coming along beautifully.

Leo: I love that. I love it when a plan comes together. All right. We do have questions. We're also running out of time. I should mention Bruce Schneier is joining us on TWiG, and he only has an hour, so we're going to get through as many questions as we can in the time left. Steve, I have questions.

Steve: Yes. Let's skip the first one because I've already referred to that throughout the show, essentially, and we've got 10 minutes before Bruce is going to be on the line. And that still gives us an hour and a half podcast, so we'll do what we can.

Leo: We'll get going here. We'll get going. No. 2 from Darren Mills, Albuquerque, New Mexico, home of "Breaking Bad." He says he finally gets why Steve was spooked by the spooks: Insert regular, but deeply sincere, podcast and SpinRite praise here. That's what he says, with little brackets. When the news broke of Lavabit's decision to throw in the towel and completely shut down after 10 years, my first thought was of your upsetting decision several years ago to suspend work on CryptoLink because you said you saw the handwriting on the wall. I was and have continued to be upset that we weren't going to get a Gibsonian VPN solution because I knew it would be the best thing ever created and blow everything else away. But now I get why you were spooked by the spooks.

You recently said you might create CryptoLink anyway, not as a commercial product, but as freeware, if you had the chance. I guess you still want it, and I know I still want it. I always will. So please get what you need to get done on SpinRite. Then I

sincerely hope you will again think seriously about giving the world CryptoLink. We need it more than ever. I'd pay a lot to have it, even though I know maybe that's not why you would be doing it.

Steve: So I only - I saw this, and that triggered many similar comments that I've seen in Twitter and in the mailbag saying, okay, Steve, now I get it. And CryptoLink would have been TNO. It will be, if I ever get around to creating it. So there isn't the concern that I could be forced to be complicit in spying. My worry still is that the other shoe hasn't dropped, and that we might be seeing a regime where anyone selling an encryption product is forced to add a backdoor. That I will never do. But if it's not being sold, if it's freeware, then I don't think there's any such way of being compelled. So...

Leo: Would you do it in open source, as well?

Steve: Yeah.

Leo: Yeah. I think you have to.

Steve: Yeah. I agree.

Leo: That's the only way you can be sure there's no backdoor.

Steve: Yeah. And I would just do it, always knowing that it's going to be free, that it's not going to be another commer- I was thinking of it as this will be the next thing I do after SpinRite. It's like, eh, I'm getting old. I'll just do CryptoLink. I'll make it free.

Leo: I'm getting old. You know, you give away so much stuff. I would never demand more free stuff from you. But if you want to do it, I think it would be very valuable.

Steve: Yeah. It was going to be so much - I did so much planning and early work on it, and I got very excited because it was just going to be so simple to use. So...

Leo: Oh, well.

Steve: We'll see how it goes.

Leo: We'll see. Dave Redekop, London, Ontario, Canada wonders about GRC and TLS in SMTP. And if you've been listening to this show for any length of time, you know exactly what he's talking about. I love this show. Steve, your show has become so important in IT, I'm setting aside time weekly to listen LIVE. I know this is what Leo wants, and it's working. Quick question: Why do you not support SMTP

TLS (encrypted SMTP email) on your own server? EOL.

Steve: You know that David was part of the core team, and probably still is, with our very early Security Now! sponsor, the group...

Leo: I knew I knew that name. Astaro.

Steve: Nerds on - Nerds on...

Leo: Or Nerds On Site.

Steve: Nerds On Site up in Canada, yeah.

Leo: I knew I knew that name. David, nice to see you again. That's great.

Steve: So GRC, absolutely - so what David is saying is that we're not supporting TLS in SMTP. Meaning that our email server does not support encrypted connections to other email servers. And he's right. And I wish it did. But it doesn't. I'm using the product called hMailServer, which is extremely good. When I went to choose a mail server, I did a lot of looking around because that was just this holiday season that I built the brand new Server 2008 machines and moved everything and fixed all the problems and so forth. And I scrapped the old Ipswitch IMail Server and got this one. But it does not support TLS in SMTP. I hope someday they do. When they do, I will definitely upgrade.

We do, however, support SSL connections for us. So, for example, all GRC employees connect over SSL to that server. So if I'm sending something to Sue, it is never in the clear. Or if Greg and I are exchanging things, or Greg and Sue, or vice versa. So for our own email, where it never leaves that server, we're a hundred percent encrypted. And many, it turns out many SMTP servers offer SSL connections on alternative ports. The whole idea with this negotiated encryption is you establish a non-encrypted connection over port 25; then, if the servers both agree, they bring up an encryption tunnel over the existing connection. But, for example, SMTP defines port 465 for SSL and 995 for POP over SSL. So there are alternative ports where you can connect to your mail servers using SSL for encryption there. But the problem is, even if we did support STARTTLS, the other end would have to support it. We know that that's rare. Again, I would like to support it if we could. And we will as soon as we can.

Leo: I'm going to skip ahead a little bit to Will Farrell in Canada. Not the Will Ferrell. But also Tyler in Humble, Texas. Both of them raise an issue that people keep raising with me. And I want you to address this. We've talked about Mailvelope, which is a Gmail extension for using PGP key signing and encryption. And both of them point to Hak5 episodes. They've done two of them in which they say that it's insecure, how Mailvelope stores your private key in plaintext in its plugin directory. Since that episode it's been patched four times - this is Tyler in Humble, Texas writing - so one hopes it's safer now. The first link gives a brief intro, blah blah blah. He's pointing at

the Hak5 shows on Revision 3. Longtime listener, first-time writer. So what do you think? You've, I presumed, looked at those shows now.

Steve: Yes. I chose this because it allows me to make the point that you still absolutely have to secure the endpoint. So, yes, endpoint-to-endpoint security means that, from the moment it leaves, it is secure. It is secure in transit. It's secure if it's being stored any number of times. It's secure if the NSA gets a copy of it. And then it finally gets sent on to its destination. Only when it gets there is it decrypted. But it is decrypted at that end. And it is not encrypted before it's encrypted at the sending end.

The point is the endpoints must remain secure. That's why earlier I was saying I would not have bitcoin, all my bitcoinage on a mobile platform bitcoin wallet because the mobile platforms are still immature from a security standpoint, and they just have a great, a very high level of exposure to potential threats, just based on the history of the problems that we've seen them having. So we'll end the podcast by just...

Leo: We don't have to end it. We don't have to end it. We've got a few more minutes. I want to go a little longer. I do want to say, though, this is the issue of somebody has physical access to your computer, you've got a problem. I store in fact my private keys on my computer, where if you had access to it, you could export it and take it home with you. But the private key is further secured by a passphrase.

Steve: Yes. It is absolutely dumb that something that's all about security, like Mailvelope, would ever have not been storing those private keys encrypted in its own directory that it has control of.

Leo: It doesn't matter. It doesn't matter. If you got to my computer, you could open my keychain and export an ASCII version of my private key. You could also get it from my Dropbox. Please, feel free to hack my Dropbox. It's secured by my hand with a long, very random passphrase. Of course you want to keep the private key secure. But if somebody has access to your computer, it matters not...

Steve: Well, and that's my point.

Leo: ...whether Mailvelope is storing it encrypted or not encrypted. If you're using a keychain, it can be exported.

Steve: A good solution, which we discussed somewhere in here, is using the LastPass secure storage as opposed to Dropbox because you do have to provide encryption for your stuff if it's going to be in Dropbox because we know that Dropbox's encryption is not TNO.

Leo: I just exported my secret key as ASCII in literally three seconds. So if somebody had access to my computer, they could just open the keychain, export it

out.

Steve: Yup.

Leo: And put it on a USB key. I don't worry about it because you have a good passphrase. So I think this - I don't - I think this is BS. This is another one of those, huh-huh-huh. If somebody has physical access to your computer, you're screwed.

Steve: No. Because there's no reason not to encrypt its private directory if you have to log into the plugin in order to use it. You have to authenticate to the plugin. So assuming that you could log out of the...

Leo: Okay, but I'm just saying, GPG keychain access is an app you can run and export my key. Is that broken? Because that's what it does. So does PGP, by the way. You can export keys. The point is...

Steve: Oh, I see the problem. We're talking about different things, Leo. Mailvelope maintains its own store, which is not part of the Mac keychain.

Leo: No, I understand. Yeah, but I'm...

Steve: And the Mac is protecting...

Leo: No. No Mac keychain is protecting PGP. This is an app that runs normally. It does not require a login. You have to get into my computer, of course.

Steve: You're saying Mailvelope does not require a login?

Leo: No, this is GPG, GNU Privacy Guard.

Steve: Okay, that's...

Leo: Same thing with PGP. You can always export an ASCII private key, which can then be put - mailed to somebody or saved. You can always do that. If you use PGP, this is something you can always do. You've always been able to do this. Just like Mailvelope does it, so does PGP, so does GNU Privacy Guard. So if you have physical access to my computer - but that key is worthless without my passphrase. You understand that; right? It cannot unencrypt mail without my passphrase. Do you see what I'm saying?

Steve: [Indiscernible].

Leo: In other words, Mailvelope's doing it like every other PGP tool does it. If you install PGP, you get a keychain program which has all your keys, private and public. I can go to my secret key, export it as an ASCII file. It's the same thing you're getting from Mailvelope. But it's still no good because you need my passphrase to continue to unlock. Is that not true?

Steve: Mailvelope has a private directory of keys. And there's no reason for it not to encrypt that when...

Leo: Okay. It's the same - it's this Chrome story again.

Steve: Precisely.

Leo: No other PGP program does that. And it's the same with Mailvelope. You can have my private key. Without my passphrase, it's no good to you. Every time I use Mailvelope I have to enter my passphrase. Right?

Steve: Right, right.

Leo: So admittedly, you should secure your private key, and you have on your personal computer. This is why you have to have a login, and that it's just not sitting in the open for people to use.

Steve: Right.

Leo: But GPG and PGP both do the same thing. And I don't think they're insecure.

Steve: As part of the protocol.

Leo: Well...

Steve: No, no, no, I'm agreeing with you, Leo. As part of the protocol...

Leo: You need a passphrase.

Steve: ...in order to use the private key...

Leo: That's right.

Steve: ...at the time you need to use the passphrase.

Leo: Yes.

Steve: So you don't want to spread your private keys around, but neither is it the end of the world if it gets loose.

Leo: Exactly. And it is kind of general practice with GPG tools that you can export your private key in an armored ASCII file or text file. And that's because the - and you don't want to give it to people, obviously. But if somebody has access to your machine, and you're using any PGP solution, they can do it easily.

Steve: Then, right. But it does...

Leo: And that's what Mailvelope does; right?

Steve: It doesn't give them anything because they still have to have access to your usage key.

Leo: Exactly. So that's it.

Steve: Yup. We were talking about the same thing.

Leo: Same thing. It's much like the Chrome story. And I agree that Chrome probably should password-protect the password storage just to make it - and if Mailvelope wanted to go the extra mile and password or encrypt their store, that would be a good thing. But it all is presupposing that someone has physical access to your computer. And as Google pointed out...

Steve: Which is where we began, is...

Leo: You're screwed, if that's the case.

Steve: If you don't have that. Now, I did want to mention, finally, that the most recent decision we have seen from the appellate courts, and I think this was the Eleventh Circuit Court, I'm not sure, one of the appellate courts, and we talked about it at the time, and this is somewhere where the law is still really gray, and that is, can an individual be legally compelled to produce their password. And the good news is, the most recent decision is no, that the courts have decided, they've ruled that that is tantamount to something you know. It is in your brain. And you cannot be compelled to testify against yourself. That's Fifth Amendment protection.

So knowing the password, my point is that ultimately, if you want to protect your

machine, you use TrueCrypt, and you may have a password that is where part of it is written down, but then you also know part of it. The point is, it's got to be something that requires testimony from you, and the law cannot compel you, currently, to produce that.

Leo: Right. And you know, though, I'm sorry, I'm not heated with you, by the way. I'm a little mad at Hak5 because I get this a lot, Mailvelope's not secure.

Steve: Right, no...

Leo: And at first I said don't use it. And then I looked into it, and it's BS, and Daren knows better than this. This is link bait.

Steve: Right. So your point is, and we were saying the same thing, but just using different terms, is that, because you have to have a password in order to use a private key, the private keys themselves don't reveal anything.

Leo: They're an extra piece. It's like two-factor authentication. And so you should absolutely do everything you can to secure your private key. And you should have a long - and this is important to people who want to use PGP. You should have a very long, good passphrase.

Steve: Passphrase, in addition to your private key.

Leo: So do the best you can to secure your private key, understanding that if somebody has physical access to your machine, they can, with every PGP tool I've ever used, easily export the secret key and save it. Or mail it to themselves. But that's not enough. That's not sufficient. So I don't think Mailvelope deserves any criticism. They're doing what every other PGP tool is doing. They're not storing it on their servers, are they?

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

Leo: Yeah. I just - I think that it's misrepresenting the issue. Maybe Daren doesn't understand it, but to make a big deal out of this is - and unfortunately, this has caused a lot of people not to use Mailvelope.

Steve: Yeah, which is unfortunate, as you say, because it provides very nice integration.

Leo: Works.

Steve: Yes.

Leo: And I've looked into it. And as far as I can tell, it's not doing anything unusual.

Steve: Well, we will be going into - we will be looking at it closely in the future. Yes.

Leo: Let's do that, yeah.

Steve: There's nothing I want more than to be able to give this the Security Now! blessing, the way we did for LastPass.

Leo: And so let's just be clear, leave it at this. Mailvelope does what every other privacy guard, GNU Privacy Guard or PGP tool that I've ever seen does. It is normal. It is not insecure. But it is a real security flaw to let somebody have unfettered access to your private computer.

Steve: Because, yes, because the nature of the PGP protocol which Phil worked out all those years ago always, always protected your private keys with a passphrase.

Leo: Right. So you need - and it's good. And I don't certainly give people my private key.

Steve: No.

Leo: But I do store it in Dropbox. And there's a reason. That way, by the way, I can use PGP tools on the iPad, for instance, because I need to import my secret key into new installations of PGP. So the way that you do that is you store your public and private key on a centralized server that you can access, a.k.a. Dropbox...

Steve: Well, or LastPass. LastPass is also running on...

Leo: LastPass would work, yeah.

Steve: Yeah. And for people who aren't using Dropbox, LastPass gives you...

Leo: LastPass is more complicated because the tool I've been using, which is, I think, called AP - I can't remember the...

Steve: Oh, pulls it directly from Dropbox? Is it Dropbox support?

Leo: It can get it from Dropbox; but, see, this is the problem with the iPad. There's

no file system that you have access to.

Steve: Right.

Leo: So having it, yes, it's great to have it in LastPass. And certainly in other installations when I'm on a desktop, that's fine. But unfortunately, if you want to put PGP on an iPad, you need to use Dropbox. Or...

Steve: We're going to have fun in the next few weeks, Leo.

Leo: I have a lot of - I was looking back, and my oldest PGP key is from 1997. I've been doing this for a while.

Steve: You know, I misspoke when I said that S/MIME predated PGP? Turns out it's the other way around. Phil was so early on this. He reacted very badly to some congressional law that was being made, as I understand it.

Leo: Yeah, he's come very close to prison many times.

Steve: Yeah [laughing].

Leo: Anyway, I'm not - I didn't mean to be heated. I was - and I'm not heated. I just want to fervently have people understand...

Steve: You want to be clear.

Leo: This is not a problem. This is normal behavior.

Steve: Yup.

Leo: It's not a weakness. Steve, we are out of time. Schneier, Bruce Schneier is coming up in just a moment, I'm very excited about that, to join us on This Week in Google. We do Security Now!. We have questions left over, if you want to do more next week or the week after.

Steve: Yep, we'll pick them up in two weeks because we're going to get on with the PGP protocol next week.

Leo: Yeah. Excited about that. And again, I'll tell people, Leoville.com, I have my - I

store my public key, not my private key. You can download it and send me - and a lot of people, every day I get a few emails from people saying, "Did this work?" And that's nice. It's good. We're slowly encrypting email, bit by bit.

Steve is at GRC.com. That's his home, the Gibson Research Corporation. That's where SpinRite is, world's best hard drive maintenance and recovery utility. Don't fear that he's working on a new version. He's already told us it'll be a free upgrade for all owners. So buy it now, and you'll get the new version automatically.

Steve: Mo' betta.

Leo: Mo' betta. He also offers a lot of freebies, I mean, this is a place to go to just browse. The cookie thing that you do, passphrases, GRC.com. If you have questions, GRC.com/feedback, SSL encrypted. And you can also find 16Kb versions of the show, SSL encrypted, and transcriptions by Elaine, SSL encrypted. GRC.com. We have the unencrypted, because I don't think we use SSL on TWiT, we have the unencrypted audio and video available at TWiT.tv/sn, or you can subscribe wherever you get your Internet shows because we're there. We're everywhere. Get it every week. Help start Year Eight with a bang. Next year is Year Eight, or we are we completing Year Eight?

Steve: We are finishing Year Eight. Next is Year Nine.

Leo: Wow. There's only one show longer lived, and that's TWiT itself. Amazing. Thank you, Steve. Thanks, everybody. We'll see you next time on Security Now!.

Steve: Thanks, Leo.