SECURITY NOW!

Transcript of Episode #307

The Future of Identity

Description: This week, after catching up on the week's security and privacy news, Steve and Leo take a look at the state of Identity Management in Cyberspace with the U.S. Government's publication of its NSTIC - National Strategy for Trusted Identities in Cyberspace.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-307.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-307-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 307, recorded June 29, 2011: The Future of Identity.

It's time for Security Now!, the show that protects your security and privacy online. And here he is, the man with the plan, the guy behind the scenes, the man who knows security and shares it all with you, the inventor of the acronym PEE, Mr. Steve Gibson. Pre-Egress Encryption.

Steve Gibson: And we've had it fixed now. It's been revised to PIE, as in Pie in the Sky: Pre-Internet Encryption.

Leo: Yes, Pre-Internet Encryption. Hey, Steve, how are you?

Steve: So that regular mortals can remember what the acronym stands for.

Leo: No PEE. Have PIE instead.

Steve: PEE was always - I was tripping over that a little bit, too.

Leo: There's actually a company that is a third party that is promising PIE, I think maybe did we talk about it last week, PIE for Dropbox now, which is great.

Steve: Yes, we did talk about it last week.

Leo: That's probably where I heard it.

Steve: And there are a number of other Dropbox competitors that purport to do a better job, and I've got that on my list of alternative solutions.

Leo: I switched to Wuala.

Steve: That's one of the ones off the top of the list, as a matter of fact.

Leo: You won't like one thing about Wuala. It's Java based.

Steve: Oh, well, no one's perfect. But, I mean, they had to run - you had to run something, probably, at your end, so...

Leo: And that's why it's cross-platform.

Steve: Better Java than JavaScript, I would argue.

Leo: Yeah. And I think Wuala does quite a good job of - the thing I - well, I'll let you review it. And I'd be very curious to hear if their model is good.

Steve: That's key.

Leo: But the thing I liked is, for free, if you donate - it's peer to peer. So if you donate some hard drive space, which I have done, then you'd get it back. So I have 463GB of cloud storage for free from Wuala, which I really like. But we'll talk about that.

Steve: Now, that's actually not so much cloud storage is somebody else's dirt storage; right? I mean, if you're donating your hard drive space...

Leo: It's shared dirt storage. This is what's interesting about it.

Steve: Right.

Leo: So that's why it's so important that they have free Internet encryption, because bits of your data are strewn across the Internet.

Steve: Oh, yes.

Leo: However, they have a very - and I'm curious about, I really can't wait to hear about this because they have what looks like a clever algorithm for redundancy. So if I take my hard drive offline, it doesn't kill my...

Steve: Clearly something will be necessary, yeah.

Leo: And by donating 400, I think it's 400 gigs, I'm just making it available to them, I've got it back. So it's cloud storage, but not on my dirt drive, somebody else's dirt drive. It's an interesting model. I cannot wait to hear you review it. LaCie owns that.

Steve: Yeah, the math doesn't quite work. If you get back the same amount that you give, then I'm wondering how they're incorporating redundancy into the model because...

Leo: Well, maybe it's not the same amount. I can't remember what the deal is. And they vet your up time. So you don't get the full amount right away. It slowly increments. I finally built up to it because they're checking, are you up all the time, so that, you know...

Steve: Right, are you a useful provider of dirt drive.

Leo: So I keep my dirt drive on my desktop on all the time anyway at home, and it's got terabytes of storage. So giving them 400 gigs [verbal shrug]. And I get the benefit because I have this, now, Wuala on all my systems, and I can store a ton of material. But anyway, but that's a conversation for another time. I'm looking at the lower third here, and I see somebody has written - me - "The Future of Identity." What are we talking about this week?

Steve: We're going to talk about the future of identity, not coincidentally. I mentioned the acronym that sort of got me thinking about this a week or two ago. It's an acronym that the National Institute of Standards came up with, and it's something that the executive branch of the U.S. government has been working on for some time. And I've been sort of keeping an eye on it to see what it was going to be because it's got a little bit of an Orwellian concern, except that from the documentation that they've put together it's very clear that this isn't going to go in that direction. But I want to talk about - we're going to talk about the future of identity, that is, the whole issue of identity in cyberspace. This acronym is NSTIC, the National Strategy for Trusted Identities in Cyberspace.

Leo: Now, as you say, this makes me nervous because what I don't want is a national identity card or something like that.

Steve: Precisely. And this in fact specifically uses those words, "This is not a national identity card." And in fact it's not even the U.S. government's. There has been work which we're going to - I'm going to run through the history dating back a decade where a consortium of about 30 organizations originally got together and began working on this.

And we've touched on aspects of this. OpenID is part of it. OAuth, we did a podcast on OAuth where we explained how it's possible for you to authorize one site that has information about you to go to another site or to make it available to another site with proper security and so forth. So we're beginning to see sort of the amalgamation and the condensation of a number of different sort of small, stratified, individual concepts into a coherent whole.

The government's role is really to try to establish some standards to assure interoperability among these. And probably, I mean, one of the things that they're able to do, for example, is to require that all their contractors abide by the following technology; that the contractors' vendors do so. I mean, the government obviously is a huge purchasing body. And so if it were able to get behind a coherent strategy, that would really help bootstrapping it and tend to prevent fragmentation. What we really want is interoperability. So anyway, we'll talk about all that. And we've got of course news and security updates and all the regular stuff, too. Oh, and some cool errata this time.

Leo: I can't wait. You know, I have to say it's gotten now to the point, and I bet I'm not alone on this, with Wuala or this national identity thing or whatever they call it, the Internet identity, that until I heard Steve Gibson's take on it I don't trust anything. But once I hear you vet it, and this is what I love about this show, then I feel some confidence. LastPass, very good example. I love LastPass and used it. But I really didn't have full confidence till I heard your dissection of it. So we really count on you for this kind of thing, Steve. Thank you.

Steve: It's about the technology, and that's really our - that's what we do here is technology.

Leo: And it's a huge service, I think, to the Internet community to have somebody who is super technically savvy kind of spell it out for those of us who are a little less so, shall we say.

Steve: Well, you just don't have time to go there. I'll do that for you.

Leo: Well, that's the whole - to me that's what open source is about, and why I trust open source encryption. It's not because I can read the code and make sense of it. It's because somebody, presumably, somebody can and will and determine if it's good or not. All right. I am ready to begin this episode. We start as usual with Steve Gibson with security updates.

Steve: Yeah, we don't have much in the way of updates. I mean, Mac is updating, and I think there's a big Java update.

Leo: Yeah. There's a bunch of Mac updates, yeah. I think ten, six, eight or something, yeah.

Steve: Yeah, just go do that. I did get some tweets from people wondering why

Microsoft was updating them off cycle. And we had mentioned before that Microsoft does non-security patches on alternative Tuesdays to the big mega monthly second Tuesday of the month patch. And three little just, I mean, these are classic bug fix-y things. There was a problem with some networks that were fragmenting large SSL packets, and Microsoft was not able to reassemble fragmented SSL packets. So one fix that they issued yesterday, Tuesday, fixes that so that they're now able to reassemble fragmented SSL packets. There was apparently some fuzzy fonts under IE9, so they fixed that. And then they also added something called OFV, Office File Validation, for the Office suites 2003, 2007, and 2010. So those three things were part of what happened last Tuesday. Not security things, just fixing sort of debris, bugs and things in Windows, which they have to do from time to time.

The only interesting piece of, well, we have got Attacks & Breaches section, which is separate. I was going to say the only interesting piece of security news that is not Attacks & Breaches was a little blurb that I picked up that I thought I would share with our listeners because it made me sort of breathe a sigh of relief. And that was Mozilla's announcement that Firefox will be getting native Adobe-free PDF rendering.

Leo: Yay.

Steve: Yes.

Leo: Actually, everybody's going to have that. Microsoft said Windows 8 will have it, too. I mean, this is - we're going to be able to get rid of Adobe pretty soon.

Steve: Yup. And sorry about that, Adobe, but you brought it on yourself.

Leo: Yeah, no kidding.

Steve: So they posted, "We intend to use PDF.js to render PDFs natively within Firefox itself."

Leo: JavaScript.

Steve: JavaScript.

Leo: Interesting.

Steve: Yeah. "Our most immediate goal is to implement the most commonly used PDF features so we can render a large majority of the PDFs found on the web. We believe we can reach that point in less than three months. The entire code so far is less than one month old, and it already renders a large set of PDF features. Initially we'll make a Firefox extension available to interested users that enables inline PDF rendering using PDF.js. But our ultimate goal is of course shipping PDF.js with Firefox. This will result in a substantial usability, but also security improvement for our users. PDF.js uses only safe web languages and doesn't contain any native code pieces attackers could exploit." So that'll be a nice step forward for Firefox.

Leo: Is JavaScript inherently open source? I guess there's ways you could obfuscate JavaScript. But for the most part, unless you actively try to do that, you can always see what the code is; right?

Steve: Oh, absolutely. The browser needs to be able to interpret it. There's no notion of compiling it. There are many obfuscators of JavaScript. And basically they sort of just do a compression, and then they tack onto the front of this blob the JavaScript decompressor. And so essentially the browser just runs the JavaScript, and it does sort of an in-place decompression. But similarly you could easily, in fact there are, there are pages on the 'Net where you can put in obfuscated JavaScript, and it just decompresses it for you.

Leo: By the nature of it, just like the CSS code, because your browser has to be able to read it in plaintext, so can you.

Steve: Exactly.

Leo: Yeah. So that's good. I mean, that's good news. It means if their PDF implementation is buggy or whatever, we can at least see it and maybe fix it, and we can know that it works all right. Which you can't do with Adobe stuff.

Steve: Well, I mean, Adobe is suffering from, on one hand, their own success because, as we know, the PDF evolved from Postscript, which was their original creation back in the early days. Apple licensed the Postscript interpreter, remember, for the first laser jet. Was it laser jet or laser printer?

Leo: No, it was a printer, it was a Writer.

Steve: Oh, Apple, Applewriter.

Leo: Applewriter, yeah.

Steve: Yeah.

Leo: Something like that. LaserWriter.

Steve: LaserWriter. The Applewriter was their inkjet printer.

Leo: No, it wasn't even inkjet.

Steve: No kidding?

Leo: That was the [sound effects].

Steve: Oh, goodness.

Leo: I had one. Tractor feed, baby.

Steve: Applewriter.

Leo: Applewriter.

Steve: But it did graphics, which blew everyone away at the time.

Leo: That's right.

Steve: Yeah. Anyway...

Leo: Well, that's a mistake Adobe didn't make with Flash, note. You can't implement Flash without Adobe code and Adobe license. But you can implement PDF without an Adobe - I don't know, is it a license or...

Steve: Well, at some point it behooved them to put it into the public domain, to make the format more widely available so that they were able to gain more traction. And unfortunately they've just been bitten by all the security problems of their old code.

Lulz Security, the company we've been referring to many times recently because they've just been so actively hacking, announced that they were disbanding. And there was some speculation on the 'Net about whether this was because the heat really had been turned up on them legally. Someone suspected of being a LulzSec member was arrested, I think in the U.K. And so they formally said goodbye on June 26. But in the process they released three quarter of a million newly hacked email addresses, passwords in cleartext, obtained from various sources.

Now, much as there was ShouldIChangeMyPassword.com we talked about last week, the fun site that has aggregated a lot of this, there is - there isn't as nice a URL, unfortunately. But at Dazzlepod.com/lulzsec/final is another aggregator that has a - I think the last time I saw it was at 400,000 and growing. They're going to be putting it all in. In this case, instead of putting your password in, you put in your email address, and they're obscuring the plaintext password. So they allow you to do a quick index on your email address to see whether your email address is among these hundreds of thousands of account databases that have been compromised and stolen. So I wanted to give our listeners a tip about that.

Leo: They just wanted you to say "Dazzlepod."

Steve: Dazzlepod. And also LulzSec made the news last week prior to disbanding by posting 446.6 meg of known-to-be-authentic Arizona State Department of Public Safety documents, which they stuck upon the Pirate Bay. A spokesman, Captain Steve Harrison of the Arizona Department of Public Safety, confirmed that the agency systems were hacked, and these documents were legitimate.

And the LulzSec guys said, "We are releasing hundreds of private intelligence bulletins, training manuals, personal email correspondence, names, phone numbers, addresses, and passwords belonging to Arizona law enforcement. We are targeting the AZDPS" - which is Arizona Department of Public Safety - "specifically because we are against SB1070 and the racial profiling anti-immigrant police state that is Arizona." And that SB1070 they refer to is the measure that passed recently making it a crime to be in Arizona without documentation proving United States residency.

So those guys are being a little bit politically activist and slapping Arizona as a consequence. So but apparently, if we're to believe what's been said, and apparently it's been confirmed, LulzSec has disbanded, and they're going to go in...

Leo: How weird.

Steve: It is.

Leo: It's just so strange. The whole thing is strange. I expect a movie at the very least.

Steve: And finally, we talked last week about the Citigroup attack where Citi had 360,000 credit card numbers and other information had been lost, compromised in an online breach. The news came out since then that this attack was going to cost Citigroup $2.7 million, they confirmed to U.S. government officials earlier this week. "According to Citigroup, personal information and card numbers from approximately 3,400 cardholders" - so 3,400 out of that 360,000. So "...personal information and card numbers from approximately 3,400 cardholders was subsequently used to make about $2.7 million in unauthorized purchases." And "Citigroup stated that affected customers would be reimbursed for the fraudulent charges."

So the point is that the information was stolen. It was immediately used in 3,400 different account cases to purchase stuff. And as we know, credit card companies hold their cardholders harmless for this kind of information theft even if it's not their fault, if it just somehow gets loose from some other website. I've had to change my card number a number of times as a consequence. And so in this case it's costing them $2.7 million.

Leo: That's actually probably not that much compared to some of the other losses that they've suffered in other times. That's chickenfeed from their point of view.

Steve: From the Twitterverse, @AlienCG was the person who tweeted me, I don't know his real name, but he reminded me that you can add a label to the end of your username in Gmail. So you could say, for example, username, then the plus sign, and whatever you want to after that, before @gmail.com. And he said, "Could this help add some security to a logon?" And I thanked him for that, and I told him that I would mention it to our listeners because I had mentioned last week that it's difficult for users to easily create ad hoc email addresses. And this does allow that. At the same time, it exposes your primary email account name, so it's not quite the same. But it would allow you, for example, to go username+aol, username+yahoo and so forth. And if you started getting spam or unwanted stuff, you could simply cancel that or route it into the trash reliably as some way of sort of segregating incoming email. So I thought that was a good tip.

And then John Nasers, @jnaz on Twitter, he was the first person to notify me of a free new Peter F. Hamilton Kindle book.

Leo: Damn. I'm just finishing "The Void." Which, by the way, is a long book.

Steve: Believe me, you could do this for dessert. This is very - it is a short story.

Leo: It's short? Good. Oh, good, okay.

Steve: And the title is "If At First...." And of course that's as in "If at first you don't succeed," which sort of is the nature of the story. Reading from the description it says, "Peter F. Hamilton has proven himself a modern master of epic space opera, carrying the tradition of far-future empire building begun by Heinlein and Asimov into the new millennium. But Hamilton is also a master of the short story" - but we haven't seen many of those.

It says, "And when he tackles one of science fiction's most enduring themes - time travel - the result is as provocative as it is entertaining. It starts in 2007 with a break-in. The victim: Marcus Orthew, the financial and technological genius behind Orthanics, the computer company whose radical products have delivered a one-two punch to the industry, all but knocking PCs and Macs out of the ring. The perpetrator: a man obsessed with Orthew. Just another simple case of celebrity stalking or so everyone assumes at first, including Metropolitan Police Chief Detective David Lanson. But when Lanson interviews the suspect, he makes a startling claim: Orthew is from the future. Or, rather, a future - a parallel timeline. Thus begins the ride of a lifetime for Lanson as his pursuit of the facts tumbles him headlong down a rabbit hole - and the hunter finds himself hunted."

Leo: I can't wait.

Steve: Well, so I grabbed it, and I read it in, like, an hour.

Leo: It took longer to read the synopsis.

Steve: It did. Fun story.

Leo: I can't wait.

Steve: But then I realized why Peter had done this.

Leo: Uh-oh. Is he setting up another trilogy?

Steve: Well, what's going to happen is, that was to get you into discovering that his very first books are about to be made available. His very first books, that's where I started reading him in '93. He did something called "Mindstar Rising," which a character called Greg Mandel, who had some sort of an organ that secreted stuff in his brain. And he could, like squeeze it, and it would, like, juice him. And anyway...

Leo: Hamilton's a very interesting mix of hard sci-fi, really good hard sci-fi, with basically just great emotional writing. I mean, it's an unusual combination in sci-fi, I have to say.

Steve: Well, and of course the Night's Dawn Trilogy is where most people discovered Peter because that became so famous.

Leo: Yeah, but I think the Void trilogy is his best work.

Steve: No kidding. I've got it, and I haven't started it yet.

Leo: Oh, you haven't read it?

Steve: No.

Leo: You know, it may turn you off because there is a large fantasy component. But it fits in very well, but it has some kind of sword-and-sorcerers type stuff in it that some people, some sci-fi people just say, I'm not going to do that.

Steve: That would be hard for me, although I understand it has our characters from...

Leo: It does. Ozzie and company are back.

Steve: And that sucks me in, I think.

Leo: And I think that the overall sci-fi premise - I don't think you'll have a problem with it, the fantasy part. In fact, you'll love it. And I have to think that - I believe that "Dreaming Void," "Evolutionary Void," I can't remember what the three titles are, but the Void trilogy is absolutely...

Steve: "The Void Is Finally Over" is probably the third one.

Leo: Finally over. No, I'm in the third book. I'm almost, I have about - only have about 16 hours left. It's a 75-hour book, audio book. But I have to think it is his best writing. It's his best development. He's done a wonderful, wonderful job.

Steve: Well, I was really sorry that those first three books - there's "Mindstar Rising," "A Quantum Murder," and "The Nano Flower," which he wrote in '93 and '94 and '95 respectively. They've been out of print ever since. Anyway, "The Mandel Files" is repackaging them, and it'll be released on August 23. It's available for preorder from Amazon. So I just want to let our users - our users - our listeners know. If there's anyone who is as much of a Peter F. Hamilton fanatic as you and I are, Leo - oh, and these are short. These are standard regular paperback size. They're not major projects. But he develops a really interesting character with lots of fun, and I can't wait to read them again. So we'll be able to before long.

Leo: So you have read them before.

Steve: Yes, I read them back then in '93, '94. That was my introduction to Peter F. Hamilton. So when Nights Dawn Trilogy came along, it's like, oh. Then I was a little freaked out by kind of what direction that trilogy took.

Leo: That was a little weird. And Pandora, I liked "Pandora's Star." "Fallen Dragon" is a great one, if nobody's read any of his stuff, to read, the first Hamilton.

Steve: Yes. That's what I recommend.

Leo: It's a single volume, and it's easier to get into than the trilogies. But, boy, is he a great writer. And I've become a big fan. I think he's an underappreciated writer, to be - what is that you've got there?

Steve: Well, this is - I was going to mention, this is in my Miscellany.

Leo: I just got that book. It just came out.

Steve: One of several. Well, okay. This is - I wanted to let our listeners know, anyone who is messing with JavaScript, as I now am, Volume 5 is what I learned on a couple months ago, which is, for people who have video, you can see it on, what, that would be your left; right? And...

Leo: The skinny one.

Steve: The skinny one.

Leo: Relatively.

Steve: Now, I was annoyed...

Leo: We would never have thought it was skinny a couple of years ago.

Steve: No. I was annoyed that its copyright was '06 because that makes it five years old, well, or, yeah, five years old. And that's an eternity in web time. And I felt the age of it. It was talking about older IE versions, like IE6, and didn't know about Netscape or Firefox 4 and so forth.

Well, anyway, just last week the author David Flanagan, who is pretty much O'Reilly's JavaScript guy, finished a yearlong project which was a massive rewrite of his original "JavaScript: The Definitive Guide," which is the book. And now we have a book with a 2011 copyright, and I'm happy again. Actually, I'm going to reread this entire new one because I was about to re-read the older one, just because I've been now programming in JavaScript for a couple months, and I thought, okay, now is the time to reread it with an appreciation for, you know, I'll get so much more out of the second reading.

Leo: I have the fourth edition, but I just got - I got David's new one because I was at O'Reilly for Foo Camp, and they gave us the new one. And the funny thing is there's another book, I think it's a companion volume, called "JavaScript: The Good Parts."

Steve: Oh, I have that, too, yeah.

Leo: So "JavaScript: The Definitive Guide" is this thick. "JavaScript: The Good Parts" is about that thick.

Steve: Yeah, that sort of tells you about how much is not good.

Leo: You need both, let me tell you. No, I think JavaScript's a very interesting language. And because it is rapidly becoming the de facto standard for not just web apps, but for mobile apps, with things like Web OS and the new Windows Phone 7, and even Apple.

Steve: Well, and we know that Windows 8 is going to be supporting JavaScript as its application development platform natively, as well. So, yeah, I mean, it was just - it was overdue for me to learn it. I've been wanting - I have been recently doing, as we know, client-side things, like the Password Haystacks is all JavaScript. And it has turned out that I think I have - I still have to be careful with overstating what I think I have. But in a couple weeks I'll be introducing our listeners to something extremely cool, that it looks like it's going to survive its testing.

I discovered an app which I had to tell our listeners about because we all have friends who are proud of their five or more megapixel cameras, and who send us unresized photos. It drives me nuts. I'll, like, check mail, and some 10-meg thing is, like...

Leo: Remember when mailboxes used to be 10 megs?

Steve: Yes.

Leo: You couldn't have more than 10 megs.

Steve: It's like, what in the world is coming in? And then, when I open my email, all I see is some person's armpit because the picture is so huge. And I think, what is this armpit?

Leo: I don't know what kind of pictures you're getting.

Steve: No, not naked armpit.

Leo: I know what you mean. And you have to scroll, and you have to scroll, and you have to scroll, and you have to scroll. I agree with you. Resize, folks.

Steve: Okay. There is something that solves this, and it is very cool. It's called RoboSizer.com. Go to that URL, Leo. RoboSizer.com.

Leo: Okay. Typing it in.

Steve: And this is, well, first of all, it makes resizing instant for we who know how to do it. I mean, for example, right now I'll fire up Photo-Paint or PaintShop Pro or something and resize manually. This makes it much faster. But what's cool about it is that - and this is why we want to recommend it to our friends. I mean, I'm going to say, Mom...

Leo: Those friends.

Steve: You put this in, and it hooks the OS across all these applications.

Leo: So you don't have to run an app.

Steve: It's transparent.

Leo: Oh, that's nice.

Steve: You simply, when you attach - when you upload things to the web, you upload photos to the web, you attach photos to email to send them. It supports social networking, all the web browsers, all of the instant messaging clients. So basically it just takes responsibility for, in the background, transparently resizing photos. And it's shareware, I think, for a month, and then $24.95. So it's not free, but I just wanted to let everyone know about it because I'm sending it to my friends. I've got one buddy in particular who just - he loves his camera, but he's like, oh, look at this. And I see weeds. It's like, wait a minute. And then it's like, oh, my god, because I'm using Eudora still, and it won't resize instantly for me, so it's annoying.

Leo: Great. RoboSizer.com. That's great.

Steve: I'm through with armpits for a while.

Leo: Windows only, of course.

Steve: Yes, it is Windows only. And then this, I've had this note for, well, you'll see from the nature of the note for how long. And I just thought I would share it today. This is from someone named Ryan, Ryan McCain, actually, who wrote to me years ago. He said, "I live in Louisiana, and during Katrina all of my computer equipment got wiped out. I've been able to get my laptop, and as you can imagine, it wouldn't boot up. I downloaded SpinRite illegally, not thinking it would do anything, but wow. It did its thing for a few hours, fixed or marked a ton of errors, and my laptop can now boot. I had so many personal photos, documents, et cetera on that laptop, so SpinRite has been a blessing. Here's the catch: I lost nearly everything in Katrina, including my house, one of my kids, pets, job, et cetera."

Leo: Oh, no. Oh, dear.

Steve: "I mean EVERYTHING," he put in all caps. He said, "I'm an honest person, so I want to pay for your software. However, I can't afford to pay it all at once at the moment." And I'm thinking, no kidding.

Leo: No kidding, yeah.

Steve: But he says, "One day you're skating through life with a great family, a nine-to-five job in IT. The next day you're trying to muster up enough strength just to get through the day. As you can imagine, money is very tight as we continue to recover from this nightmare. I'm not wanting your sympathy, I'm simply explaining my situation. I can give you $10 per month until the price of the product is paid off. I know that sounds absurd, and I'm embarrassed to even ask that of you. However, I'm trying to keep my wife and kid fed, and things are really tight around here. Hell, I never thought I would be one of those people who went to the library to get on the Internet. That will give you an idea of how things are down here, not just for me but for thousands of people in the Gulf Coast. I appreciate any leeway you can give me here." Well, of course I wrote immediately, and I said...

Leo: Yeah. I have a feeling I know what you said.

Steve: "You owe me nothing for your use of SpinRite." I said, "I'm very glad that it was able to help you post-Katrina. And the LAST thing," in caps, "I want from you is $89 that you don't have."

Leo: No kidding, yeah.

Steve: "The most expensive aspect of your having used a pirated copy is the time I'm taking here to reply to you, which I'm glad to do. So please, you have the best wishes of all of us here at GRC, and you owe us nothing whatsoever. Peace, and hang in there."

Leo: Wow.

Steve: So he wrote back. He said, "Steve, that's very generous of you. Thank you very much." Well. He says, "My only priority at the time was saving as much information off of that laptop as possible, no matter how many laws I had to break. 90 percent of the videos, pictures, et cetera, I had of my kid who passed away during Katrina were on that laptop."

Leo: That's just, oh, my god, I'm just devastated.

Steve: "So it was much more than just a few songs and funny videos that I was trying to restore. Thanks to SpinRite, I was able to recover every one of his pictures and videos. Feel free to read this email on the Security Now! podcast as a testament to just how great SpinRite is. Thank you for your kind wishes, not only for my family, but for everyone who's still getting their lives back together in the Gulf. Ryan." So.

Leo: I don't know what to say. That's, wow, yeah.

Steve: It was very neat.

Leo: Ryan, our thoughts and prayers are with you. Wow.

Steve: And presumably, since that was a while ago, he's pulled his life back together. Of course, nothing can replace - I can't SpinRite his lost son, so, yeah.

Leo: You never recover from that. That's terrible. Oh, my god. All right, Steve. Let's see what the feds are up to now with this identity thing.

Steve: Okay. So this is, in my opinion, probably the most important thing going on that is Internet-wide for virtually all of us. And that is the problem that we tackle daily with authentication and identity on the 'Net. It's a constant recurring theme. We talk about passwords a lot. I've got, as I said, I hope to have one more shoe to drop, or the other shoe, or something, on the issue soon, some work that I've been doing.

But we have this problem that we've discussed, we've come at from various ways. We've talked about OpenID in the past, the idea that you have what's called a "single sign on," where you would authenticate yourself to a single location. And either then you would maintain that persistently, and other sites you visited could figure out who you were from that and trust that, or when you go to sign onto a site, it bounces you to somewhere else to authenticate, and then you come back having done so.

Then we've talked about the OAuth, the OpenAuth project, where, for example, if you were at Flickr, and Flickr said we'd like to grab your Facebook friends with your permission, what happens is you say, yes, let's go do that. And so you're bounced over to Facebook, where you log in with Facebook, if you're not already logged in persistently. You give Facebook essentially permission to provide that information to Flickr, and then you're bounced back. We did a podcast about that. That's how the OpenAuth technology works. And there's the crypto going on in the background is Flickr representing what it wants to Facebook, Facebook showing you what it is that it's going to give, and making all that kind of transaction secure.

Then there's, like, a number of other technologies. There's something called SAML, which is a Security Assertion Markup Language, which is unfortunately the result of massive committees working over a decade, everybody wanting something slightly different. And this thing has just grown to the point - it's something that I talk about with my YubiKey friends because they're very interested in, like, beyond just YubiKey. Stina, her original concept was solving this problem. And so she came up with the YubiKey sort of as a, oh, well, here's something, recognizing it's not the whole answer. It's a multifactor authentication component of a much bigger problem. And there's something called UMA, User-Managed Access, which manages sort of like what information will be revealed, what purpose it will be used for, who will have access to it.

I mean, these are really big problems. And so I'm very bullish on one hand that - or I guess hopeful. I'm hopeful that we're going to come up with ways to make this secure. At the same time, any user who follows along with, like, the condition of a current desktop, has got to wonder how you can do anything securely on an insecure platform, which is - I lay awake last night thinking about this, as I was thinking that this was what we were going to be talking about on the podcast, because you can argue that it's extremely difficult to extend trust very far into an insecure place.

The TPM, the Trusted Platform Module, which many laptops have, and we're beginning to see it on desktop motherboards, the idea there is that you have sort of a secure boot process where you start from a known core of security, and you only run authenticated software in sort of a stepwise fashion where you incrementally boot yourself into running in a way that, for example, would prevent a rootkit from being installed in the boot sector of the first track of your hard drive and then allow it to take over and compromise the security from there on out.

So lots of focus has been given to this. There's something called the Liberty Alliance which was formed 10 years ago in 2001. Initially it had 30 organizations that got together to attempt to establish open standards, guidelines, and best practices for this problem. I mean, everyone recognizes there's a problem. And the goal is aggressive. I mean, the goal would be to, for example, have something robust enough that we could do voting online, and it was not compromisable; that we would have access to medical records; that we would be able to order prescriptions. And part of the problem is that you have to be very careful, obviously, about privacy and information leakage and all of that.

So the players in this are heavyweights who understand the problem. And it's taken them a decade, and they still don't have it, how to assemble this. Today this Liberty Alliance, which there was a site, ProjectLiberty.org, which was an active wiki for a while, which is now locked because the group of now 150 organizations have moved over to something called Kantara, the Kantara Initiative. So it's KantaraInitiative.org. The word "Kantara" is Swahili for "bridge." And so that's now where this work is. And, finally, the current U.S. executive, the office of the President, has stated that the U.S. government is going to start looking at how to move this forward, how to create an initiative.

So the National Institute of Standards and Technology, the NIST, has released just a couple months ago - I've been watching this for a long time, but in April the document was finalized called the NSTIC, which is the National Strategy for Trusted Identities in Cyberspace. And I'll just read from their little opener. It says:

"This strategy has a goal to foster a public/private partnership where industry and communities come together to solve the issues identified in the NSTIC to create an identity ecosystem which enables web service interactions to be...." Then we have a number of bullets. "Faster: Once you use your credential to start an online session, you would not need to use separate usernames and passwords for each website. For example, your computer or cell phone could offer your 'trusted ID'" - and that's in quotes because we're not sure what that is yet, so this is goals and outlines - "to each new site where you want to use the credential. The system would work much like your ATM card works now. By having the card and a PIN you can use your ATM card all over the world. By having a credential and a password, you would be able to use your trusted ID at many different sites. This saves you time while enhancing security. No more searching in your drawer for your list of passwords."

Then they go on to say it would be more convenient. "Businesses and government will be able to put services online that have to be conducted in person today, like transferring auto titles or signing mortgage documents." So they're being aggressive about the level of security. And believe me, I'm being skeptical here. I'm not suggesting we know how to do this today. And I wonder whether we even can today with the platforms that we have. But I want to give everyone a sense for, like, the big vision.

"Safer: Your trust credential will foil most commonly used attacks from hackers and criminals, protecting you against theft and fraud, safeguarding your personal information from cyber criminals. Private: This new 'identity ecosystem' protects your privacy. Credentials share only the amount of personal information necessary for the transaction. You control what personal information is released and can ensure that your data is not centralized among service providers." And I've noticed throughout this there has been a lot of attention paid to thwarting information aggregation. And then there's a constant notion of only providing what's necessary. I mean, there really isn't in this a "this is going to be a way for us to spy on you" background. There really is an anti-Big Brother sort of clear design to the system.

And "Voluntary: The identity ecosystem is voluntary. You will still be able to surf the web, write a blog, participate in online discussions, and post comments to a wiki anonymously" or pseudonymously. "You could choose when to use your trusted ID" or not. "When you want stronger identity protection, you use your credential, enabling higher levels of trust and security."

So that's sort of their overall sort of broad stroke, the idea being that people would be able to use the system. This NSTIC is meant, is sort of a document that's been put together. The existing alliance are sort of working with the government, making sure that their targets are aligned. And, for example, this says, "The strategy does not advocate for the establishment of a national identification card or system. Not does the strategy seek to circumscribe the ability of individuals to communicate anonymously or pseudonymously, which is vital to protect free speech and freedom of association. Instead, the strategy seeks to provide to individuals and organizations the option of interoperable and higher assurance credentials to supplement existing options, like anonymity or pseudonymity."

So, and it gives a couple of examples, for example, of how this might work. They paint the picture of Antonio, age 13, who "wants to enter an online chatroom that is specifically for adolescents between the ages of 12 and 17. His parents give him permission to get a digital credential from his school. His school also acts as an attribute provider," that is, "it validates that he is between the age of 12 and 17 without actually revealing his name, birth date, or other information about him. The credential employs privacy-enhancing technology" - and we have the ability to do this - "to validate Antonio's age without informing the school that he is using the credential." So "Antonio can then speak anonymously but with confidence that he and the other participants are between the ages of 12 and 17."

So that's sort of an example of the powerful benefit that a system like this could potentially offer if we had a way of putting it together. This document explains that the offline world, which of course we're all familiar with, "has structural barriers that preserve individual privacy by limiting information collection, use, and disclosure to specific contexts." We are able to control what we tell who to. "For example, consider a driver's license. An individual can use a driver's license to open a bank account, board an airplane, or view an age-restricted movie at the cinema; but the Department of Motor Vehicles," who issued the driver's license, has no knowledge of "every place that accepts driver's licenses as identification. It is also difficult for the bank, the airport, and the movie theater to collaborate and link the transactions together. At the same time, there are aspects of these offline transactions that are not privacy protective. The movie theater attendant who checks an individual's driver's license needs to know only that the individual is over age 17. But looking at the driver's license reveals extraneous information, such as the individual's address and full date of birth."

So they have another acronym. The Fair Information Practice Principles, FIPPs, is an existing, widely accepted framework for evaluating and mitigating privacy impacts. And there are eight principles in this Fair Information Practice Principles: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing. So that sort of gives you a sense for how this would be used.

They have another example. Someone they call Parvati "uses a credential issued by a third party and bound to her existing cell phone to access online government tax services. She can log in with a click of a button. She no longer has to remember the complicated password she previously had to use. She views her tax history, changes her demographic information, files her taxes electronically, and monitors her refund status."

So the idea is that what the government is doing with this whole NSTIC is basically they're sort of putting their imprimatur on the work that has been done for the past decade, pulling these technologies together. They're going to propose this system. One can imagine that they will use it themselves. And by virtue of their purchasing power and contracting power, we've seen many instances where they've done similar things, where they've, for example, required certain security safeguards be put in place for the contractors that they're using, and the contractors' subcontractors.

So you can imagine that, as this comes together, the government will say we're going to require that what you do be NSTIC compliant. I mean, and the government does not want to get into the business of providing this. There will be private sector companies, very much like VeriSign with their VIP approach, which we talked about extensively as a nice third-party provider of multifactor authentication, or like Yubico that provides the YubiKey and then has an open specification that allows anyone who wants to to provide authentication using that hardware token. And of course we've got unfortunately the example in recent memory of RSA with the fiasco of what happens when you have a widespread, highly used token, and this data gets away from you.

So with anything like this, obviously there are liabilities that come with this centralization of information and power. Yet we do have the technology, when we work out all the details, for making many new sorts of services possible. Which I think is clearly where we're headed in the future.

Leo: Cool. Sorry.

Steve: No, that's fine.

Leo: I got nothing to say.

Steve: Yeah. This work is...

Leo: This is great.

Steve: This work is going on. It is happening. I think the U.S. government will end up requiring this kind of authentication and use by its contractors. They will have to go buy it from somewhere. That will create a market. I mean, there's so much attention that has been put in this about user-side privacy, I mean, recognizing that this is not from the government. This is not mandatory or mandated. It would be available from the commercial sector. The government's involvement I think would help to keep it from being fragmented. We've talked about how we don't want to have a necklace of individual authentication things, so we'd like to be able to have our credentials be portable, be widely accepted. There's nothing to prevent a user from getting multiple credentials, although the technology does allow a user to specify what information is given to whom with this notion of attribute providers.

And that's one thing we've never talked about before. That's like another entity standing back which is able to essentially provide attributes, like we were talking about this 13 year old whose school was able to assert his age. And so they were part of this ecosystem. Their assertion was digitally signed. And so the assertion existed separate from the school so that the assertion could be validated and verified, and the verifier could be checked, and so its level of authentication could be assured. And then that way somebody was able to take this attribute and know that there's an entity standing behind it with some standing.

So, I mean, we've talked extensively about digital certificates and how, for example, owners of websites get a digital certificate. They assert their identity to a certificate authority who then signs that assertion. And it's that assertion, essentially, that our browser receives. And then our browser checks to see whether it believes the signer of the assertion. So this is sort of an extension of this existing public key infrastructure. That is, it takes this concept that we are able now to produce tamper-proof documents, tamper-proof things. We can granularize them to being attributes which people have.

And so there could be, like, an attribute repository and a company whose job is to provide subsets of those attributes so that you provide your pharmacy with the ability to know exactly the following things about you. The pharmacy then makes a request to this attribute provider. You have told the attribute provider what to provide, or you have signed your permission to the pharmacy. The pharmacy then forwards that permission to the attribute provider, that then is able to take from its large collection, select those attributes that you have given the pharmacy permission to have, and then it signs those, sends them back to the pharmacy. The pharmacy gets them from a signed provider, and it's only able to get what you allowed the pharmacy to get because it was your permission that allowed the release of that information.

And potentially, complex as that sounds, all of it happens in the background. That is, users are, I mean, this is sort of like next-generation cyberspace technology that begins to get control of our information and allow us to manage our information in a responsible way and, ultimately, transparently. So there's all this nonsense of having to create separate identities for every website that we go to ultimately goes away. And so we end up being able to authenticate much less frequently. That authentication is spread across virtually all of the Internet. And we're able then to control from providers who know different things about us. That's able to be aggregated under our control, and we're able to then control the dissemination of that in a way that other third parties are able to trust. It's a big deal. And we're really heading towards it.

Leo: It sounds like this replaces, or maybe not replaces, but does it replace digital signatures technology using certificates or PGP, that kind of thing?

Steve: Well, it absolutely uses it.

Leo: It's complementary.

Steve: Ultimately, it will replace them. That is, we have all these fragmented things. We have, as you say, like personal digital certificates, signed, to like encrypt and/or sign your email. We've got OpenID. We've got OpenAuth. So we have authentication. We have information provision. We've got all this stuff has sort of been created ad hoc and not pulled together. What we would ultimately have, in the same way that there's just a single SSL certificate infrastructure - there aren't five of those, there's just one. And in the same way there would be the answer for personal identities. We would have control of it. You could have multiple identities if you wanted to. You could be anonymous or use a pseudonym, that's fine, create one. Although...

Leo: That's kind of problematic, though, because then you don't have to have an identity. Or is your pseudonym tied to your identity?

Steve: Well, but the DMV is not going to sign your pseudonym. They're only going to sign you.

Leo: Got it.

Steve: And so part of all this information is a chain of trust. And at each step of that chain - and this is why this SAML, the security markup language, is such a big deal. Stina was telling me that no organization could even write this. I mean, like, write the code. They're working now on reference implementations. But all anyone will ever be able to do is just take it and use it because it is so big, it is so complex. And to do this, to have the flexibility that we need, yet the power that we need, there's just no way to do this simple because you do something simple, then someone says, well, what about that? It's like, oh, yeah, well, we don't do that. Well, okay, if you don't do that, we can't use it.

And so unfortunately this is like the kitchen sink to the power of a hundred. And it's a committee-produced monstrosity. But it's standing up over time. It's now been about - in '07 it got sort of stabilized and finalized. And people are poking at it, and it's looking like it's holding together. So the good news is it'll all be done for us. It'll be behind the scenes. Nobody'll be involved with it. But it absolutely takes advantage, it leverages this concept that we've discussed of this notion of it is possible to create tamper-proof tokens, tamper-proof documents. We're able to sign things and encrypt them and assert that this hasn't been changed. All of that technology we've been talking about for the last five and a half years, that all is in place.

So now what they're doing is they're saying, okay, let's extend this. I mean, let's talk about how we pull it all together and then begin using it. And what's interesting to me is that we're beginning to emerge from pure theory mode into, okay, here's the kind of ways this would get used. This is what it would mean for us. And the challenge, of course, is that it not get hacked. I mean, and I immediately think of, like, okay, if I have a token that I plug into my computer - the NSTIC document talks about smartcards. It's like, well, okay, my current machine doesn't have a smartcard reader, but it's got USB ports coming out its ears. So maybe it's like a YubiKey kind of thing that I put into a USB port in order to provide authentication.

The problem is that that's not secure because the moment the data is sort of like un-enveloped, the moment the data is available, malware in our computer would have access to it. So that's where, for example, in the Yubico case, remember we talked about their cool device which is a complete authentication computer out in the token, out in the USB. Well, for this sort of thing to work in an identity ecosystem fashion, it itself, that is, this token would have to be smart enough to establish a secure encrypted connection with the other endpoint. That is, you can't have the token provide information to the computer because it could be compromised. I mean, unfortunately our current PC platforms, and by that I mean personal computers, Macs and Linux machines and everything, I mean, they're just so insecure that the only thing they can really be trusted to do is be a conduit in some fashion.

So, I mean, I really see, don't for a second think I don't see major challenges to implementing this in a secure fashion. Yet I think you have to have the dream before you can begin saying, okay, now we know what we want. How do we go about getting there? And I really do like how comprehensive this dream is and how much potential there is for the future. I can imagine 20 years from now this will just be, oh, yeah, I mean, it's just the way we do things. People will have digital identities of various sorts. They will have been issued by various issuing authorities.

Leo: Doesn't have to be a governmental authority.

Steve: Absolutely not. Well, in fact, it probably won't be. The government will be there; but you could also, in the same way that...

Leo: Guess it depends who you trust.

Steve: In the same way that I as GRC got an SSL certificate from VeriSign by jumping through some hoops and proving to them that I am who I say I am, in the same way there will be certainly - or you're able to purchase anonymous tokens from VeriSign, the football or the credit card and so forth, or just download them onto your smartphone to provide you with an anonymous, yet repeatable factor for login. We'll have all of that, too.

But where they're really heading is to this thing being vastly more comprehensive. I don't think more onerous. I really think just more comprehensive. We have the technology to do this today. It's just a matter of getting everybody together, agreeing on standards, and then beginning to deploy it. And there is a chicken-and-egg problem, and that's where I think the government can probably come in by saying, "We like this. We're going to require everyone we deal with to use it." And that'll tend to get it going. But otherwise I don't see the government at all being too heavy-handed in this.

Leo: I know some people, the idea of government doing this makes them nervous. To me it actually seems sensible because you need a centralized third party to certify it.

Steve: Yes.

Leo: And I know people, a lot of people who listen to this show, don't trust our government. And we probably shouldn't trust government. But who better? I mean, you want Microsoft to do this? They have been, by the way, with little success. So I think it needs to be that. And then I think this is a nice - you liken it to certificates, and I think that's a good - the web certificate system, I think that's a good analogy. I think it makes sense to have third parties that are certified and that kind of thing. I'm excited. We needed this. I've been signing my email for years, to no avail. It's all been the Web of Trust technique.

Steve: Yes. And this document establishes the right principles. I mean, and I've read the whole thing. Everything about it, as I'm reading - and I'm skeptical of Big Brother, too. I don't know how we're going to do it. I mean, as a coder and technologist I think about all of the hurdles and the pitfalls and the challenges we face. But it's clear that we need that. We need this in order to move forward and to really leverage cyberspace to the full extent possible, I mean, we have the technology.

Leo: Yes, yes. Identity is critical. We've learned that lesson. And anonymity, while you - I think this is nicely done because you can have anonymity.

Steve: Yes.

Leo: But there's also a way to certify you are who you say you are. And I think you need both. So I think this is good. This sounds - I'm excited.

Steve: Yeah, me, too.

Leo: And I appreciate your giving it the onceover.

Steve: Well, so I wanted to sort of bring our listeners up to where we are in this because - and I'm sure we'll be pinging back on this from time to time as things happen. There's 150 international organizations involved, a bunch in the U.S., but a bunch outside the U.S. So the goal would be that this would be one single global technology. And again, I liken it very much to SSL certificates. We know how that whole infrastructure works. This is that to the power of a hundred because it's far more than just saying, oh, this site is who it says it is. It's granular information and assertions of fact about individuals. And I forgot to say, also devices. This is also made very clear, for example, that network adapters might have assertable identities and be uniquely identifiable. So you could establish a connection between two endpoints where those are network adapters on the Internet, and they're able to establish an absolutely provable and authenticatable connection from endpoint to endpoint. So as you think about this more, this enables things we cannot do today. And I think that's very exciting, too, because it creates huge new opportunities.

Leo: Very exciting. So what's the next step? What happens next for this to fly? I mean, do people have to - third parties have to create systems and so forth, or...

Steve: We're beginning to see companies who are stepping up. The website that I referred to, not the Liberty.org, the Kantara Initiative, if anyone's interested, the KantaraInitiative.org, that's the state of the art in this. I mean, essentially - and you'll see the NTSI - I keep getting the acronym wrong - NSTIC stuff is participating in the Kantara Initiative, which is much bigger than the federal government. I mean, the government is just sort of saying, we like this. This is what we hope it's going to be, and this is what we want it to be so that we're able to give it our stamp of approval. But there are beginning to be companies that are offering these kinds of services. And so this Kantara Initiative is what to keep an eye on moving forward. And I'm going to do so.

Leo: Yeah. I mean, I would very much like to, for instance, replace my - I'm trying to remember who I got them from, Thawte or somebody - my email certificates with a new form of digital identity that's universal. So KantaraInitiative.org. Now, but are they offering...

Steve: No. It's just the organization...

Leo: Just the group.

Steve: ...sort of the organizing point. Yeah, we're still premature. I mean, it's going to take probably the major providers like Apple and Microsoft.

Leo: It's got to be in the email. It's got to be in Google and all of this stuff.

Steve: Exactly. And so, for example, I didn't realize that Google is an OpenID provider.

Leo: Yes, yes.

Steve: But of course they would be. And so you can, right now, you can use your Google credential, which does allow multifactor authentication. So you can turn that on, get multifactor authentication with Google, and then use Google as your OpenID provider to log into any sites that support OpenID. So OpenID will end up getting replaced with something much stronger and more robust. But and then Google will be a provider for that, as will other sites. And this'll just sort of, I mean, I remember, and I'm sure you do, too, Leo, because we were both there, before the Internet, when there were people talking about, well, you know, we're going to hook up all of the computers in the world together. But first I said, well, you're first of all nuts.

Leo: Yeah. Oh, this Internet thing will never fly.

Steve: How are you going to do that? And then, when it began kind of limping along, but there wasn't anything there, there was the chicken-and-egg problem. It's like, I mean, we used to hear, oh, this is never going to happen because no one's going to put their stuff on the Internet until there's people on the Internet to look at the stuff. And there's not going to be people on the Internet until there's something to look at. Well, it happened.

Leo: It happened, it did.

Steve: And it just sort of organically occurred. And the good news is, I mean, something this important and big has to be done right. That's why I'm glad it's not a mandate from the government. The government couldn't possibly design this. I mean, this has taken a decade and 150 organizations spread around the world. And they kind of think they've got it now. So, and code is being written. This is just a big 'berg that moves forward very slowly. The good news is I think it's a good 'berg.

Leo: And we're not the Titanic. Let's hope, anyway. No, it's very exciting, and I think we did need this. And I've been waiting for this. And, I mean, I've been a believer all along because I use OpenPGP or GNU Privacy Guard to sign my mail. And that confused people because it would put a little bunch of - it would put a hash at the bottom of the mail, and people'd say, what's that? Now I use certificates to sign it because most email programs support that. But that confuses people. They say, "What's this P7 S/MIME attachment?"

Steve: Well, and another example is the way we got the extended validation certificates. No users had to do anything.

Leo: Right.

Steve: But now their bar lights up green if there's, like, higher level of assertion. That'll just - it'll end up getting built into our world. And everyone's going to take it for granted. But it's going to be good.

Leo: Steve Gibson is the man in charge at the GRC Corporation, GRC.com. In fact, if you go there you can get a copy of SpinRite, the world's finest hard drive maintenance and recovery utility, saving hard drives even in the midst of disaster. GRC.com. If you have a question for next week about this or any other topic, GRC.com/feedback. And you can also find a lot of freebies there, information about his Password Haystacks, for instance, which is really a good thing for people to know. I've been using it religiously ever since, and I'm so grateful to you for that. New stuff coming, too. GRC.com.

You can follow the Steve on the Twitter. Someone sent me an email saying, "Why do you keep calling it the Twitter? You're so old. You should stop doing the show." It's a joke. You'll follow the Steve on the Twitter, @SGgrc is his Twitter handle. And that's a good place to ask questions, too. As you can see, he includes that in his stuff. And you'll find all the shows, 700, what is - 700. 300. Not quite. 307 episodes.

Steve: Slow down, Leo. We'll get there. We'll get there.

Leo: We will. We'll get there sooner than later. 307 episodes available in transcription, 16KB, and 64KB, so you get your choice there, all at GRC.com. Steve, thank you so much for being here.

Steve: My pleasure, Leo, always. And we'll do a Q&A next week.

Leo: Next week.

Steve: And then hopefully I'll have something really cool. Maybe in two weeks. I'm going to try to get it done in two weeks.

Leo: That'd be neat. We do this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1800 UTC at live.twit.tv. And we invite you to watch live or download it after the fact. You can also get it at TWiT.tv/SN. Thanks, Steve. We'll see you next week.