SECURITY NOW!

Transcript of Episode #141

RSA Conference 2008

Description: Steve and Leo discuss recent security news; then Steve describes the week he spent at the 2008 annual RSA security conference, including his chance but welcome discovery of one very cool new multifactor authentication solution.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-141.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-141-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 141 for April 24, 2008: The RSA Conference. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!, wherein which we attack the attackers, we hack the hackers, we crack the crackers, we talk about what's going on in the world of security with Steve Gibson. He's the guy who created - coined the term, he didn't create it, he coined the term "spyware." Others created the spyware. He just found it. He also did create the first antispyware program, which he's long ago handed off to others. But he certainly was, as usual, kind of the Paul Revere of security. The hackers are coming, the hackers are coming. Hello, Mr. Gibson.

Steve Gibson: Oh, Leo, great to be with you for our 141st episode.

Leo: Oh, go ahead and rub it in.

Steve: Wow.

Leo: You love that because TWiT's only at 140. He loves that.

Steve: Yeah, I need a bigger - I need a bigger lead. So...

Leo: Oh, you'll get one, don't worry.

Steve: Boy, it took two, it took - oh, that's right, we started a lot later than TWiT did. I was going to say it took, you know, two and half...

Leo: Well, TWiT's three years old. Yeah probably did take, like, a couple years.

Steve: Yeah.

Leo: But, yeah, but that's a good point is that TWiT had a year on you.

Steve: Exactly. So we've been catching up quickly. So watch out.

Leo: Oh, man.

Steve: We can just shoot by, Leo.

Leo: Oh, man. So we're going to talk today about your visit to San Francisco and the RSA conference.

Steve: Oh, there was just so, well, I've got a ton of things to share with people. And it was a really, really interesting, worthwhile trip. And I got a lot of good feelings. I mean, largely, I've got to say that if people listen to this podcast, they pretty much have a grip on everything going on. I mean, the whole show was identity and authentication. I mean, basically you could just rename it the Identity and Authentication Show because, I mean, that's what everyone is all freaked out about.

Leo: Well, that's funny because that's what we've been talking about for the last few...

Steve: I know, I mean, it's like - I had sort of the same feeling that I had when we had Dave Jevans on from IronKey. It's where, you know, he was talking about all these things, and they're all things that we had discussed in prior weeks of Security Now!. So I was thinking, wow, isn't that cool that, I mean, we've covered all that. And similarly, I mean, there was nothing at the show that we haven't covered in one form or another. I mean, it was really nice. It's like, okay, if people are listening to this, they really are up to speed. Which is not to say that I wouldn't highly recommend this RSA security conference for any of our listeners who are, like, in the security business. I mean, it's not something I would expect random end-users to need to go to.

Leo: Well, I think a lot of end-users are very interested in this stuff. Oh, they wouldn't go, you're right, they wouldn't go to RSA.

Steve: Well, but on the other hand, I mean, if you had a high-end end-listener who was really into security, it wasn't - overall it has sort of a corporate aim. I mean, it's aimed more at corporate solutions, enterprise, securing your networks, authenticating your 100,000 employees, that sort of thing. But the individual breakout tracks where you go and listen to, like, small, either individuals or small groups of two or three talk about specific topics, and I'm going to talk about a couple of those during this show that I found were really interesting, I mean, they're interesting to anybody. So, I mean, certainly our listenership. And anyway, it was really fun.

Leo: Yeah. Yeah. I mean, I read one - an interview with one showgoer who said, "I didn't understand what one product on the show floor was meant to do." So it also is probably fairly technical.

Steve: Yeah. I will say, like I said, it was - what I found walking around was it was largely everybody doing the same thing. I mean, there were - everybody had tokens. Everybody had press-the-button-and-get-authenticated stuff. I mean, so there was, like, literally you just, as you walked by the booths, it was "the industry's strongest authentication solution." Okay, somehow everyone had that.

Leo: Yeah. So there's a little hype, as well. And, well, we certainly know that security, I mean, hype and security go together.

Steve: And you'd stand there looking at the booth, and which was a problem, you know, I had press credentials, so they were all like, oh, come closer, come - it's like no, no, no, don't scan me. Because, you know, the badges were all RFID-enabled. And so, you know, you could get scanned and suddenly you'd be getting phone calls. Actually I got one this morning that was sort of annoying. It's like, I don't need anybody to sell me on this stuff. I understand it. But standing at the booth, you could not determine from any of the background of the booth what their thing was. It was, again, it was world-class-strength identity verification for your enterprise. It's like, okay, well, but that's what the people on either side of you are saying, too. So it was - and it was huge. I mean...

Leo: Oh, really.

Steve: On the last day of - the last day of the show I just dedicated to dealing with all the exhibit space. The prior three days were all just going from one of these interview track breakout sessions to another, where I found really interesting things. And what was really bizarre is it was in the morning of that last day, in a really bizarre way, I found the one coolest new authentication gizmo of the show. It was - there was this woman just standing at the top of the escalator, looking kind of forlorn. And it turns out she's the inventor, the founder, and the CEO of this company in Sweden that has come up with something that is so cool that I can't wait to tell our listeners about it. And but she had a deal to be in one of the vendors' booths. So she comes over from Sweden with a whole bunch of these things, and this invention, and they reneged on their agreement. So, like, nothing had happened for her. And so here she was on the last day, just looking for some way to get her message out. And I walked by with my press badge, and she sort of thought, oh, maybe this would work. Well, let me tell you, I hope it's going to work because...

Leo: Oh, good. Oh, good.

Steve: ...this - she really deserves - and this - anyway, it is so cool and clever. I just love clever and new. And this is a multifactor authentication solution that we've never talked about, and nobody else has it.

Leo: Good. So let's talk about RSA. Unless you have some - do you have some errata or anything you'd like to talk...

Steve: Oh, I've got a ton of security stuff that happened in the last week. And of course a fun, interesting, sort of different SpinRite anecdote. I got a letter - we received, GRC received a letter from Dan Stoddard just last week. And he said: "GRC, I know you get a lot of these letters of appreciation, but I must tell you how pleased I am with SpinRite. Earlier this week a friend's laptop crashed. It would display the Windows boot-up logo briefly, then bluescreen. He called the laptop manufacturer and was told there was no way to recover his data. Frustrated, he asked me to take a look at it. I first tried running the Windows repair utility from the installation CD. No luck. Next I booted a laptop from a BartPE CD-ROM, but was not able to access the drive at all. Finally, I removed the hard drive from the laptop, connected it up to my PC with a hard drive-to-USB adapter. This, too, failed. Normally at this point I would have told my friend the hard drive was dead, with no chance of recovering his files. But I've been listening to the Security Now! netcast for the past several months and have heard Steve read letters from SpinRite users" - just like him - "SpinRite users who have successfully recovered data from crashed hard drives. So I purchased a copy of SpinRite from the GRC website and within a few minutes downloaded it and had created a bootable SpinRite CD-ROM. I have to admit I was somewhat skeptical at first. But as SpinRite went to work, I could see raw data from the hard drive flashing across the screen. I then realized the hard drive still contained my friend's data, and SpinRite was finding it. After a couple of hours the process was complete. I rebooted the laptop, and to my immense relief it booted up Windows normally with all his files intact. Needless to say, I am now a SpinRite believer. Thanks, Steve, for a great utility."

Leo: Excellent.

Steve: So just love those stories. Any listeners who have SpinRite success stories, please don't let the fact that I get a lot of them deter you from sending me yours because every one I just - it's just so neat to have someone write...

Leo: That's - Steve's reward is not the financial reward, it's the emails he gets. He loves it, just loves it.

Steve: I just love it that it works.

Leo: Yeah, yeah.

Steve: Okay. So in the last couple weeks a bunch of stuff has happened. First of all, probably maybe most important, there's a huge problem has been found in the ClamAV system.

Leo: Oh, dear. That's not good.

Steve: It's open source, as you know, very popular open source antivirus. The problem is that because it's open source, the bad guys have the same access to it as the good guys have. So there are proof-of-concept exploits out such that, if you've got ClamAV filtering your email for malware, viruses, spam, whatever, you can send somebody using the current release of ClamAV a deliberate malformed piece of email. The email scanner has a buffer overflow in it.

Leo: Oh, interesting.

Steve: Which means that - and, for example, ClamAV is often run on email servers, where it'll be, like, scanning all the mail coming into a corporate facility, to the corporate server. So spam - and as far as we know it's not in the wild yet. Updates are available. So I wanted to make sure that anyone who thinks maybe even their corporation, if they think their corporation IT guys are using ClamAV, make sure they have updated to the latest because - and it's not the signatures they need to update. That's probably happening all the time. It's the code itself has a problem such that just it receiving spam can take over the server.

Leo: That's wild. That is wild.

Steve: Yeah. So anyway, so...

Leo: So people would - spammers would send out this message to everybody, hoping that they're going to snag somebody who's running the ClamAV...

Steve: Exactly. Anybody who has not updated, who's running the pre-most recent update, would be vulnerable. And their own AV, I mean, when you think about it, the last place you want a buffer overrun or a similar sort of exploit is in your AV, which you've added to make your system more secure. In the process you've made it much more vulnerable.

Leo: And by the way, it's not just ClamAV. I've heard these kinds of similar buffer overruns with...

Steve: Yes. I don't mean to be picking...

Leo: Almost all antiviruses seem to have this problem, or have had this problem at one point or another.

Steve: Well, remember my favorite quote from the RSA show is "Information wants to be free, and code wants to be wrong."

Leo: The other thing you should pay attention to is that ClamAV is used as the engine for many other third-party solutions, so you might want to check and see what the AV engine is in your solution and update as needed.

Steve: Also the very original instant messaging program, ICQ - remember that in the old days, Leo, when it had like a little flower petal logo? I think I was like - I was user, like, 4444 or something.

Leo: Really, wow.

Steve: I wanted to find out what it was and got onboard very early. And it's really not for me.

Leo: Onboard and offboard, I'm sure.

Steve: Yes. But there's an important vulnerability that was found in ICQ. It's got a weird exploit. It's in the status display portion that shows, like, somebody remote that is in your friends list is online or offline. Well, it turns out if their machine were to send you a malicious status report on them, that could take over your machine. So it's got the potential for creating a flash worm that would go through the ICQ system, basically getting into someone's machine and then sending out a malformed status to everybody they're connected to, which would then jump into all of those machines, and then all of them would do the same. So you could imagine like a flash worm that would just flash through the ICQ network and take over the whole thing. So you have - I don't know whether ICQ updates itself automatically. You definitely want to make sure, if you're an ICQ user, that you fix that because you don't want to be part of that flash when that happens. That would be bad.

The other big news is all the browsers have had updates since we last talked. Firefox is now at 2.0.0.14. I had been using 13 for a while, so it's now 14. And that fixed some important updates. Safari, both Windows and Mac versions, are now at 3.1.1, and there were some important things fixed in them. And Opera is now - just went from 9.26 to 9.27. And I'm going to say I'm liking Opera a lot, Leo. It's got a whole bunch of features that you only discover, like, after you've had it for a while. Like I right-clicked on a page, and on the menu was the option of blocking, selectively blocking content, where like you could then click on things on the page that you wanted it to block, like ads and things, and it would automatically add those domains to a block list. And it's like, wow. And it's got a built-in download manager and - anyway, I mean, it's just a whole ton of features that I just, as I use it more and more, I'm doing a bunch of work with a bunch of browsers on a topic that we'll be talking about here in maybe another month, it's taking longer than I expected, but then everything I do does, but it's going to end up being very comprehensive.

So I've been using Opera and Firefox and Safari. And Opera's got some neat features. Firefox v3 is in beta and is looking nice and stable. I loaded the Windows version of Safari just because there is one. I didn't install it on my machine, it's in a VM. And I have to say, I mean, it looks identical to the Mac Safari except you can grab any edge of the window and drag it, which is so nice, just like Windows. It's like, I don't know why the Mac just refuses to do that. It's just - it's a constant annoyance to me, as you know.

Also, Windows XP Service Pack 3 is almost ready. Microsoft has said they will make it available through Windows Update on April 29th. So, what, I guess that's going to be next Tuesday, which will be wonderful for those of us who set up Windows XP from time to time. I mean, I have it, for example, running in my VMs that I'm running these various browsers on. And it's like, oh my goodness, thank God that you can clone VMs so you don't have to re-upgrade every version of XP that you install. But going to Service Pack 3 will save us about a 100-plus patches. So that will be very nice.

Leo: Hallelujah. It's not a - unlike Service Pack 1 for Vista, it doesn't change the functionality in any way. It's just a rollup of patches.

Steve: Is that the case? I meant to look to see. I'm trying to remember whether I read that there was some change. I might be thinking instead of Service Pack 1...

Leo: Service Pack 1 for Vista does change a lot of stuff. I don't - you know what, I'll ask Paul Thurrott.

Steve: I kind of think maybe it does a little something. I can't really remember.

Leo: Okay, good. That's good. I'll find out. Listen to Windows Weekly tomorrow.

Steve: There you go.

Leo: Paul will know.

Steve: And the last little bit of news is not really, like, security trauma, except that, well, it is for the Hotmail people. It turns out that there's a botnet now that has a 10 to 15 percent success rate of cutting through Hotmail's CAPTCHA protection.

Leo: Wow.

Steve: And of course we've talked about CAPTCHA a lot because it's a cool technology. The idea is - "Are You Human," I think, was the name of our podcast that we talked all about CAPTCHA. And of course the problem is a botnet has hundreds, thousands, tens of thousands of machines in it. And botnets are now being used as a preferred spam generator because it makes it impossible to blacklist the sender's IP because you've got 10,000 of them, instead of it, like, coming from one server. So what the botnets do is they would love to be able to create a Hotmail account so that, rather than sending email just from their own IP, they create a Hotmail account and then use the browser interface to put their mail into Hotmail because there are obviously, who knows, hundreds of thousands of legitimate Hotmail accounts, and that means that you cannot blacklist by Hotmail.com, you've got to do more.

But the point is that even having as low as a 10 to 15 percent success rate, that would annoy a user, but the bot doesn't care. It just, you know, essentially that means that it's going to try eight times and it's going to get through between eight and nine, every eight and nine times it's going to be able to create a new account and use it until Hotmail decides that it's evil and shuts it down. And also researchers in the U.K. have published a paper describing their automated approach for breaking Hotmail's CAPTCHA that has a 60 percent success rate.

Leo: Wow.

Steve: So more than half the time they're able to crack Hotmail's CAPTCHA. So I think the Hotmail guys are - Microsoft, of course, owns Hotmail now. They're going to have to go back to the drawing board and come up with a better CAPTCHA solution because it's just - it's not doing the job anymore.

Leo: I mean, come on. A lot of spam comes from Hotmail and Gmail and all of these created mails, whether they're using automated break-in tools or not. I presume that's what you mean when you're saying 60 percent success rate. They're talking about some sort of computer program that can figure out what the CAPTCHA is.

Steve: Yup. Which of course is what CAPTCHAs are supposed to prevent.

Leo: Right, right.

Steve: They're not doing that very well.

Leo: Those bots, they're everywhere. Spam is such a problem. It's just not getting any better. It's just getting worse and worse and worse.

Steve: Well, and when it's not, I mean, it used to be original spam was just annoying commercial stuff, home mortgages and various organ enlargements and...

Leo: Right. Now it's, yeah.

Steve: And now it's malicious. It's take over your computer when you click the link by mistake, or in some cases not even having to take any action at all. So, I mean, it's real malware that is being sprayed, you know, instead of just annoying advertisements.

Leo: Yeah, yeah. So there we go. That's the news.

Steve: That's the news.

Leo: That's the news across the nation.

Steve: Okay. So RSA, of course, we've talked about RSA a lot. RSA Corporation had the early, well, was the patent holder, thanks to its founders. RS&A stand for Rivest, Shamir, and Adleman, who did the original public key work and have a whole bunch of patents which have since expired because that was more than 17 years ago, the life of patents. So that stuff is all out in the public domain now. But they're a big, strong security company that offers all kinds of great features. And they produce an annual show in San Francisco, the RSA security conference. Although the formal name is RSA Conference 2008. It was a fantastic show. I mean, it was really well put together. I'm just very impressed with the job they do. Now, I'm tempted to end the podcast now.

Leo: What?

Steve: After telling our listeners they have got to go see the keynotes.

Leo: Are they online? They're all online?

Steve: Yes. Now, I created a short URL just for everybody listening because the big one is long and nasty. We will have links on your show notes and on GRC's to the page of the keynotes, which I cannot recommend highly enough. Now, not all of them were fantastic, so I'm going to recommend some, and I'll put those on my page also, and Dane can get them from my page, Leo, so that you have them. So it's snipurl.com/rsa2008.

Leo: Oh, that was easy.

Steve: Yup, snipurl.com - why don't you type it in right now just to verify that...

Leo: I got it.

Steve: Okay. Snipurl.com/rsa2008. That will take you to their page where we can find all the keynotes. You can - they're available in Windows Media format or in Flash.

Leo: It also says "View Interactive Webcast." What does that mean? You can view the video, or you can view an interactive webcast.

Steve: Okay, well, that's, okay, that's what I was about to say was it's that thing that comes up in Flash. Click on one of those, and it'll come up.

Leo: Yeah, I'm watching it right now, the opening ceremony. So it's got a whole interface. You've got the video, you've got the slides - I guess these are the slides from the...

Steve: That were shown during the presentation.

Leo: Oh, that's cool. So you can actually watch their - oh, this is a nice way to do it.

Steve: Oh, it's beautiful, Leo. And over down in the lower left you can see the four days. And when you click on one of those, it shows you the keynotes. Okay. So the title of this year's show was - it was all about Alan Turing, whom we've talked about of course, the famous cryptographer mathematician who did the Turing test, the Turing machine, who cracked the Enigma cipher using his math and technology. And so "Turing Lives" was sort of their whole theme, which was sort of laced through the whole show. So the opening ceremony is worth watching, the first half, where they talk about Turing. So it was just sort of interesting. And of course we've talked about him extensively. The second half is the dance number.

Leo: What? There's a security dance number?

Steve: Oh, goodness. They took the whole - the old, remember the "Brick House"...

Leo: Yeah, "She's a brick...," the Commodores, yeah.

Steve: Yeah, the Commodores, right. And they relyriced it into "It's a Botnet."

Leo: Oh, geez.

Steve: Oh, it's so bad. Oh, goodness.

Leo: Why, why, why? Why would they do that?

Steve: So I want to make sure everyone knows I am not suggesting that they listen to the second half of the opening ceremonies.

Leo: But now you know they will.

Steve: Well, yeah. You can get a taste for it, but believe me, it doesn't get any better once it starts. It was just...

Leo: Let me just play it.

[Music]

Leo: I'm going to make them listen to it.

[Music]

Leo: Oh, that's just ridiculous, and they've got a whole group of people up there. Were you there for that?

Steve: Oh, yeah. Oh, yeah. She's a botnet.

Leo: Were you groaning?

Steve: And they had the - and because it was sort of hard to hear, they had subtitles for the whole thing going on. I was like, oh, goodness. So, yeah, that kicked off the show. And I thought, well, okay. We'll see how this goes.

Leo: What did the security pros in the audience - how were they reacting to that? Were they enjoying it? Were they digging it? Were they getting down?

Steve: It was, you know, I mean, it was light-hearted and spirited and fun. And it was like, okay, is this what I paid for? The good news is that's not what you paid for. There was tons, tons of really high-quality content. Okay. So John Thompson of Symantec, I absolutely recommend his keynote. He brings out their guy who's in charge of malicious software. And unfortunately they try to do a little bit of canned humor that just doesn't work in this setting. But I know that our listeners will be fascinated by their statistics. And it was his comment, I couldn't remember who said it, but I watched it again, actually I ran through several of these again because, you know, in order to prepare my recommendations. And it was Symantec that has the numbers that showed there is more malicious software now that users are encountering than good. And so it was in that presentation where their numbers that they have, this worldwide, this global network which is monitoring malware and viruses and spyware and everything. And so end-users are now coming in contact with more bad software than good software. And it was this year, apparently, that that tipped, that scale tipped over to that side. So John Thompson's Symantec presentation I really recommend.

Now, my - okay, I've got two favorites. The panel discussion at the end of the first day, April 8, which was Tuesday, was the cryptographers panel. And we've talked about Whit Diffie and Dick Hellman of the Diffie-Hellman key exchange, and of course Ron Rivest was one of the founders of RSA. I actually knew Diffie and Hellman back in the early '70s, when I was at Stanford University's AI lab during the summers, I got a job there in the summers. They were, I mean, these guys were there doing their early Stanford crypto stuff. So it was fun to see them again, and I chatted with them. Their panel is great. And Whit Diffie is this wonderful, white-bearded, long hair, I mean, he's exactly what you want in your cryptographer. He was just tremendous and very funny, had lots of little quips and things. Again, I think our listeners will really find it interesting. Just, I mean, here are the guys that founded the crypto industry, you know, talking to you for 45 minutes about things that they think are important and what's going on.

And one of the things, I don't remember, I think it might have been Rivest, one of his points was, I thought it was interesting, he said humans do a bad job of judging low probability events. That is to say - it might have been Hellman now I think of it. Anyway, our listeners can listen to the keynote. But the point was things that tend to happen very seldom, we make the mistake of confusing that with never.

Leo: Right.

Steve: And, I mean, to our detriment. I mean, so you might argue that something like the chance of terrorists commandeering commercial airliners and doing evil with them, you know, what's the chance of that? Well, it's not zero, and we found out on September 11th. And so...

Leo: Well, I'll give you another example. People forget that New York City is actually very earthquake prone. It's just there hasn't been an earthquake there in a couple of hundred years. So people figure, aw, never gonna happen. But, and if it does, it's not going to be a pretty sight.

Steve: And that's a great example, Leo, is that, yes, I mean, it's interesting because, I mean, how people are just bad with statistics. There's something, whatever it is, the way our brain is wired, and actually the way our brain is wired was my other very favorite keynote because a friend of ours...

Leo: Oh, Jeff Hawkins, yeah.

Steve: Yup, on Wednesday. But anyway, so it turns out that the way we're wired, we just don't do well with statistics. Something about us, about humans, we just don't...

Leo: It's not intuitive.

Steve: We don't get statistics. And one critically bad way not to get it is to confuse low probability with zero probability. Anyway, so again, that cryptographers panel discussion on April 8, Tuesday, is absolutely worth watching. And then my other favorite was Jeff Hawkins, whom we've talked about, in fact; "On Intelligence" is the book he wrote recently, and that was one of our Audible recommendations at some point. And this of course is the book that talks about the work he's done. Jeff, to remind our listeners, is the founder of Palm and Handspring and Numenta, which is his company which is working on software to model, essentially to solve problems in the way that the human brain does by modeling the exact neurological functioning of the brain. He's got this technology called HTM, Hierarchical Temporal Memory, where he - basically they are building in software exactly what, I mean, they're exactly modeling in software the way the brain is neurologically wired. And so they're doing it much more closely than the old neural networks did, where you just sort of basically had a bunch of goo, you know, neurons wired up in software, and you threw things at it, and they sort of learned. Here, because they're modeling the brain closely, they're getting, well, much higher quality results.

The cool thing about his keynote is first you get to see him, and he's kind of a neat guy, and he's odd and neat. But he also has really good results that he shows. You've got diagrams of his stuff, he shows pictures, he shows, for example, he gives examples of the kind of photos - they're doing photograph recognition is the way they're developing their technology now. And all the technology is downloadable from Numenta. So you can get this and play with it yourself. And he shows some phenomenal results where they were training one of their models on image recognition, showing them pictures of boats and cats and dogs and animals and all kinds of random stuff, and then showing the kinds of things that this technology of theirs can then correctly recognize where, I mean, even I'm looking at it going, well, okay, that's a boat, but how the hell could it possibly know that? I mean, it's really impressive. So here, I mean, for free, our listeners can watch this keynote and see this for 45 minutes. And I absolutely highly recommend it.

Craig Mundie from Microsoft, also back on Tuesday, had a really interesting discussion with their - Christopher Leach is their chief information security officer. And so they're talking about perfect identity versus perfect privacy, security versus privacy. Their theme is "End to End Trust." And so basically here's Microsoft talking, I mean, the guys at the top talking about where Microsoft is and what they're working on and what they're thinking. And I highly recommend that, as well.

Leo: Very interesting stuff, yeah.

Steve: And if anyone's curious to see Michael Chertoff, he was added late to the program, that is, a few days I think it was, maybe about a week before. He's, of course, Secretary Michael Chertoff, the head of our Department of Homeland Security for the U.S. And so he spends about 45 minutes talking about their stuff and what's important and what's going on. So, I mean, just really, really great, great information. Which is why I said I'm tempted to just end the podcast now.

Leo: But before you do, you might - I would like to, I mean, yes, we can all go and look at those videos. And we can, you know, it's not - I'm thrilled that they did that. I think that if more conferences did that, yeah, maybe there'd be lower attendance. I'm sure that's what they're worried about. But boy, they'd sure get the word out. And I bet you people would look at that and say, boy, I want to be there next time. I don't want to miss that.

Steve: Yes. And again, I want to say that I will work to give our listeners some notice before next year's conference in case there are people who look at this stuff and think, wow, I really want to be part of that, or I want to attend. I mean, there was pretty much on the exhibit space was 100 percent enterprise-targeted content. But the individual breakout sessions, I think there were 14 different tracks. And so at every hour there were 14 things going on. And, I mean, I needed five of me in order to see them all.

Leo: Well, good, so you can watch them online. I think that's really great.

Steve: Well, no, those you cannot.

Leo: Oh, you can't, ah.

Steve: No. Only the keynotes.

Leo: I wish they'd put those online, too.

Steve: Well, they were all being recorded. But the access is restricted. So only people who had access to them at the show are able to download them. But you are able to - so, for example, I could get them and listen to the ones that I missed.

Leo: Yes, I get it.

Steve: But I guess my point is that, I mean, there was so much good stuff happening all in parallel that I was having a hard time, hour by hour, scheduling myself, choosing this over that, which one do I really want to see more. So one that I stumbled on on Wednesday, it was - it had, like, a strange name. It was Securing the Internet with Strong Authentication or something like that. And I thought, okay, well, that's good, I definitely want to know what that's about. Turns out it was all about something we had talked about before, which is EVCerts, Extended Validation Certificates. And I was really pleased to see that the panel is as upset as I am about the proliferation of certificate authorities.

Our old-time listeners will remember how I was ranting - perhaps a little more than necessary, but still - over discovering recently when I went and looked at IE's list of qualified certificate authorities, that this list had just exploded since I had looked at it many years ago. I think once upon a time there was maybe 11 certificate authorities, meaning that there were 11 organizations that were able to sign SSL certificates. Well, the list has just gone insane. And my argument was, the problem is, from a security standpoint, even though everyone ought to have the right to create a - to become a certificate authority, from a security standpoint just, I mean, common sense tells you that the more of those there are, the greater the chance of a mistake. And mistakes have been made. The famous one, of course, was a bad - somebody malicious got a Microsoft certificate. And so it was like, oops, that was revoked, and everyone's recovered from that. But, I mean, there have been...

Leo: That's important to remember, though, the certificate doesn't guarantee safety. It just means it's revocable if it turns out somebody's misbehaving.

Steve: Well, okay.

Leo: It guarantees identity.

Steve: Well, what has happened is the standards have been lowered over time. So that, for example, and I was curious about that, I went over to Go Daddy just thinking, okay, well, you know, these guys are sort of, you know, the budget domain name guys, and they offer certificates. Well, they literally say here's a - I don't remember what the numbers were. But it's like, $49 or $39 or something for an SSL certificate that just verifies your domain. So what they're doing is they're doing domain validation only, nothing else. So now all an SSL certificate really means is that you're connected to the domain that you think you're connected to, but it says nothing about who owns that domain.

Leo: Hmm, interesting.

Steve: And so, I mean, I'm paying - what am I paying? I'm paying $500 a year, although I think I buy three years at a time to get, I mean, because it bugs me, but I buy VeriSign certificates. GRC is 100 percent VeriSign. And so for three years it's $1,295. But I have to go through some hoops. I mean, they check out my D&B. We do some faxing. Sue, my office manager, gets a phone call. I mean, so...

Leo: Good, good.

Steve: ...there is some - well, but the problem is, there's nothing to say that I have a VeriSign certificate or a Go Daddy. I mean, both gives you the same SSL connection. And Go Daddy's $39 certificate, or it's $29.95 or something, I mean, that gives you the lock on your browser window even though it doesn't mean nearly as much as...

Leo: So that is interesting. Somebody must have said to Go - somebody, some master certificate authority must have said to Go Daddy it's okay to do this; right?

Steve: No, Go Daddy is a CA.

Leo: They are.

Steve: Yes.

Leo: Well, who gave them the right to be a CA?

Steve: Well, look through the CA list, Leo. I won't...

Leo: I know, the Hong Kong Post Office, I know. So who is it that awards this ability?

Steve: Well, it's - okay. Each browser manufacturer has - it's the browser that contains the master list of CAs. So Fox - FoxPro. Firefox. Firefox brings one. Opera has theirs. Safari has theirs. IE has theirs. However, they pretty much all have to have the same ones that everybody has because anybody who's issuing SSL certificates to websites, their browser has to be able to get a secure connection to that website, or it puts their browser at a competitive disadvantage to...

Leo: And of course Go Daddy's huge, so they've probably got to do it. But shouldn't there be some standard for what a certificate authority requires?

Steve: Well, and thus - thank you, Leo. We've walked right into what EV certificates are. First of all, they are a lot more expensive. They are double the price, in the case of VeriSign. Now, once again, Go Daddy does offer much less expensive, actually half price. For example, a one-year VeriSign EV certificate is $995, a thousand dollars. Two years is $1,790. So you get a discount, as typical with domain names or anything like this. Go Daddy's one-year EVCert is half that price, it's $500. Actually, it's $499.99. And their two-year cert is $800.

Leo: Okay. So they're half price.

Steve: So they're half price.

Leo: Do they do the same thing? Is the EV certification required?

Steve: Yes, yes. There is a formal document that specifies what every certificate authority has to do in order to be able to issue EVCerts. And any certificate authority that short-circuits that process, that doesn't go through the level of validation required, is at risk of having their CA, their ability to set the EV bit, essentially, I mean, this is just one bit in a standard x.509 SSL certificate. All it is is a bit. But they will have that revoked if they start issuing these things cavalierly.

Leo: Okay. All right.

Steve: So, now, get this. Apparently whatever it is you're put through to get one - and frankly I'm so sold on this, much as I hate the idea of having to pay the price, I'm going to. So I'll know what it takes at some point. But apparently it can take up to three months to qualify. You have to, I mean, I don't know if it's a DNA test and you send them blood or - but, I mean, my eyes glazed over. And I'm thinking, god, I hope I will be able to get one of these.

Leo: Yeah, no kidding.

Steve: Because, I mean, they verify that the people, the identities of the people who control the domain, who control the server, I mean, there's all this stuff we go through. So it's not just a domain name. It is, I mean, they're really validating the company, the corporate entity, the ownership, the management, the structure, the executives, I mean, it is seriously rigorous. Now, to give you some sense of the relative number of these, first of all, for a long time IE - IE7 was the first Microsoft browser that supported extended validation. And so there wasn't a big pull for it. So at this point today the number I heard quoted was that 5,000 EVCerts have been issued.

Leo: Now, in IE7, if I go to an EV certified site, does it look different? Is there some way...

Steve: Oh, that's what's so wonderful about it. It's why I have to have it. Yes, Leo. Go to - you can go to PayPal, or you can go to VeriSign. So, for example, https://www.verisign.com. That'll give you a secure connection. And under IE7 and Firefox 3 and Opera 9.5 - which is not out yet, but that's in beta. So EVCert at the browser level is spreading beyond IE. And you'll see that the bar turns green. And on the right-hand side it identifies the company, the corporate entity behind it because that's what the EV certificate is, it's what you paid for. I mean, and the reason they're getting twice the money is, first of all, they can. But, I mean, they are really doing some serious work in order to, I mean, I guess at each end. I'm doing work and they're doing work in order for me to prove to VeriSign that I am who I am. So but the point is, how many times have we said, okay, right-click on the page, go to page properties, click on certificates, get the certificate, look at the chain...

Leo: You don't have to do that anymore.

Steve: Exactly.

Leo: Now, I have seen studies that say that consumers have no idea between, I mean, they'll look at the green bar, go oh, that's pretty.

Steve: That's today, Leo. I mean, this is...

Leo: You've got to raise awareness here.

Steve: Well, what's happened is the SSL certificates are now so easy and cheap to afford if all you're doing is protecting your domain name, that phishing sites are buying them from Go Daddy.

Leo: Why not, yeah.

Steve: Exactly. Because, oh, look, there's a lock on my browser. This must be secure.

Leo: It must be my bank.

Steve: Right.

Leo: Despite the fact it says Hacker.com.

Steve: Exactly. So, I mean, we know that consumers are freaked out about online commerce, about online banking, about online purchasing, about online everything having to do with their credentials and their money. And so this is new, but this is going to happen. I mean, I've known about EVCerts. We've talked about it before. I wasn't sold until I really thought about it. And frankly, it was this presentation. The guy in charge of security from Mozilla was one of the guys on the panel. One of the other guys was the guy I mentioned who was at CERN who misspelled "referer" in the original HTTP specification that only has one "R" in the middle instead of two, the way he spelled it. And so, I mean, these are serious good guys who are talking about, you know, this is why we've had to do this is that SSL certificates got to the point where they meant nothing because there weren't these standards in place. I mean, it was like, you're supposed to do this stuff. Well, that just got weakened over time. So we absolutely want to hope, need to hope that the same will not happen with this. But, I mean, everyone understands the mistake that was made. And so EVCerts, I'm convinced - I'm thinking in fact of switching GRC over 100 percent to SSL, that is, just make all of our connections SSL, since it's just a warm fuzzy thing. And I like the idea of, I mean, especially GRC being all about security, of us just having unsniffable connections 100 percent of the time.

Leo: You know who's not? Amazon.com.

Steve: Yeah, I know. And I thought eBay would be, too. But they're not. And PayPal, but PayPal is. So, but Leo, only a thousand EVCerts have been sold yet. So it's, well, I forgot to say, as opposed to 850,000 generic SSL certificates.

Leo: Now I'm using all my different browsers to see who's supporting it, which sites are doing it, which sites are not doing it. And then we've got to get the word out to consumers that this exists.

Steve: Well, what'll happen is, they'll begin to sense it. You'll begin to see...

Leo: The green does jump out at you. It really does.

Steve: Yes. The green bar, and I love the fact that they - oh, in IE7, if you left-click on the name of the company, it pops up in a window that says VeriSign has verified that this is this company. So, I mean, they're pushing it to the next level, saying okay, we're going to give you a certificate that we're really going to stand behind, "we" VeriSign, for example. So we're going to do the work to make you prove that you're who you - that you are who you are, that this is a corporate entity in good standing that owns this certificate, such that when you click on this, we're going to be making that warranty to the end-user.

Leo: Right, right.

Steve: Anyway, it's going to end up being very important.

Leo: Yeah, no kidding. So it's too bad, of all the major browsers, Apple Safari is the only that isn't currently supporting it. Firefox 3, as you said, Opera 9, and IE7 all do.

Steve: And I don't know why Safari hasn't. Well, again, there is a bit of a chicken and egg. I'm sure you remember back in the beginning of the web, people were sure it wasn't going to take off. Because they said, well, but why are people going to have websites when there's no users, and why are there going to be users if there are no websites? Well, that problem solved itself, obviously. So the same thing is going to happen here. This is an important good thing that is going to, I think, go a long way to strengthen regular end-user consumer. And so what'll happen is, people won't use Safari when they want the EV certification if they have a browser that lets them know. And so Safari will have to do it. And other high-end websites that are suddenly not green when an increasing number of sites are green, well, the ones that aren't are going to have to belly up to the bar also.

Leo: Right.

Steve: So there will be pressure on...

Leo: Oh, you bet, you bet.

Steve: There'll be pressure on Safari to join the other browsers. There'll be pressure on non-EV sites to join the EV parade. And before long it'll just be - there will still be $29.95...

Leo: Yeah, and I'm going to, you know, somebody like me is going to do that. I'm not - there's no - well, if I ever - I don't - I'm not in SSL at all. But I'm not doing eCommerce, so there's no, I mean, I'm not going to spend $2,000 for a cert.

Steve: It does hurt.

Leo: Yeah.

Steve: It does hurt. Just for some bits. Thank you for this little pile of bits.

Leo: Well, I understand why they charge that much. If they're doing that much validation, if they're actually calling you and doing all that stuff, that's expensive. I can understand that. I don't know if it's that...

Steve: Yeah, and similarly you can understand why Go Daddy says, hey, $29.95 you can have a cert. We're not saying anything other than, gee, it's www.mysiteoftheday.com. That's all we're going to do. But if you want a padlock, you can have one. And what that does...

Leo: Well, it gives you SSL, though, too.

Steve: Exactly. It gives you SSL, which is a good thing. And it no longer costs a lot.

Leo: Right. And that's, I mean, for that alone I think it's worthwhile, you know, just to encrypt your transaction with websites. If everybody did this, we wouldn't have to worry about VPNs and all this stuff because you'd always be encrypted as you surfed.

Steve: Right. And email clients are now supporting SSL connections, so that would allow, I mean, it makes it very simple to keep things encrypted.

Leo: Yeah.

Steve: And it's no longer a big, huge expense to do so.

Leo: Now, let me just - we've talked about some of the things you saw at RSA. And I think that - it sounds like it was a great conference. But just overall, what's your sense of it? Are we winning the battle against bad guys?

Steve: No. The overall sense I got from listening to the keynotes, from attending all of the, well, many of the individual tracks as I was able to, and as I said, I wish there were five of me, there was this sense of sort of doom and gloom. It was like, you know, it's like we're losing. The problem is, as we've talked about before, the 'Net was designed for sharing. It was not designed for securing. It was designed to be open and sharing. You put up web pages, and everyone can look at it. I mean, and so here we are trying to come along later and fix the fundamental lack of security.

And similarly, I mean, one of my other favorite quotes, and I don't remember, I think this might have been from the Symantec keynote, was something that really stuck with me. They were saying, "Do not protect the network, protect the information." And I thought that was an interesting distinction because the sense I got was that our much-reviled DRM, which has up to now been used by commercial publishers to lock and control what's done with their content, I could almost foresee a day when DRM is sort of ubiquitous and is as useful and used by end-users as it is by commercial publishers. The idea being that I've talked, for example, about the files on my little key ring and how I'm using TrueCrypt in order to protect them. But the problem is you need to have admin rights, and that's why the IronKey solution has some compelling advantages because you don't need to be an admin in order to be able to unlock your IronKey.

But imagine if all files had DRM? I mean, everything the computer produced. If that was a fundamental part of even a text file, it was everything was in some kind of securable wrapper so that that just becomes ubiquitous, I mean, we are so far away from there today that I can't even think about how we get there. And we don't want to think about how we get there. But, I mean, it's just like, doesn't that make sense? And then you don't have network perimeters, you don't have this problem of, oh, crap, somebody got in and now what can they do because you just open your door and say come on in. All of our files are individually protected using some amazing new alien technology that we don't have yet.

Leo: Well, encryption.

Steve: Some, yeah, I mean, but it's - yeah, something.

Leo: You know, sometimes I think that these proclamations might be self-serving. But it seems like it would be easier to protect the data than to protect the network. Much easier.

Steve: Whoo, I think it's much harder, actually.

Leo: Oh, really.

Steve: Oh, yeah. I mean...

Leo: Well, then, why not just protect the network?

Steve: Because that doesn't do the job. We're trying to protect the network, and we're failing. And so the idea being - well, and...

Leo: I guess that's what I mean by it's easier to protect the data than - if you can't do it, then it's not that easy.

Steve: And, for example, here I am in my fortress of solitude, as you frequently - or fortress of security or something. And, I mean, I'm behind a ton of protection. So that's neat. But when I walk out of the house I've got my files on my thumb drive on my key ring. Now I'm outside of my network. And so now that's not protected. And so I just, I mean, the kernel of the content - I'm not saying, I mean, Symantec's not selling it. They don't have it, either. But I just - I sort of got this interesting, it's like protect the information, meaning that this notion of ownership and authentication and rights, the idea of digital rights being useful to end-users and part of our experience, part of our use of information so that, I mean, again, we are so far away from having that, it just makes your eyes cross. Because we're talking about a whole 'nother infrastructure, and everyone having public and private keys and/or whatever, I mean, I don't even know how we would do this. But it's like, wow, that's the answer. I mean, it's impossible, but that's the answer, is that fundamentally when we create files, the files protect themselves. And somehow they know who's supposed to be able to open them to get the information out of them. It's just an interesting idea.

Leo: Seems like we could do both, attempt to protect the network and protect the data.

Steve: It's just, well, no one's - yes. And I was just being facetious when I said that everyone's going to take their firewalls off and just say, oh, come on in because...

Leo: Let's do both.

Steve: ...why not.

Leo: What the heck.

Steve: But I have to say - and again, speaking of being self-serving, we're at the RSA Conference 2008. So it's all about solutions for security.

Leo: Right, right.

Steve: So, yes, okay, we're trying to promote security. But there was this sense of a cloud.

Leo: I agree. I feel it, too. I mean...

Steve: Well, and end-users feel it. Like this is all becoming too hard to use, and security, and multifactors, and I need all these things, and I'm afraid to do stuff online...

Leo: And ultimately it fails. You can't really be safe.

Steve: I don't think I mentioned that I've had to cancel my most used online credit card.

Leo: Oh, boy.

Steve: Three weeks ago it got out of some site that I use, as careful as I am, as I try to use PayPal and Google - what's Google thing?

Leo: Google Pay.

Steve: Google Checkout.

Leo: Google Checkout.

Steve: Google Checkout, yeah. I mean, I try to use those to minimize how many different websites I give my credit card information to. But there's lots of sites that don't take PayPal and don't take Google. I mean, my own, for example. And so somehow I got a call from a robot on the phone saying, "Please hold for security."

Leo: Yeah, no, we did talk about this last week, yeah.

Steve: Oh, okay. And so it's like, okay, well, so, there again. I mean, again, my card was protected by the company that blocked those. It was sharp enough to block them. But that's an example of what happens to some consumers. I mean, so this kind of secured information gets loose.

Leo: And we look at spam, and that's completely out of control. And as you said, now it's a security hazard as much as anything else. I mean, it just doesn't feel like we're gaining on these guys. It feels like they're gaining on us. And it's really frustrating because they're jerks.

Steve: And I think at this point it would be fair to say that the bad guys are winning.

Leo: Ugh, you know, I mean, excuse me, I mean, obviously this is - everybody knows this. But just, you know, you're taking something really incredible, really powerful, really useful, and just trashing it for no real good reason, just so you can make a little extra money. I mean, it just frustrates the heck out of me.

Steve: Yeah. I have to say, Leo, my sense is we're going to win. I think, I mean, we've got a long way to go because we, the good guys, we started out nowhere, with technology that was operating systems where security wasn't - network security wasn't an issue because there was no network. They were standalone computers that got stuck onto the 'Net. And of course we all know the story of Windows and how long it took to get a firewall in Windows that was on by default. I mean, it took until Service Pack 2 of XP, the current service pack of XP. Not even an old service pack of XP. So it's taken a long, long time.

But there will be - certainly there will always be problems. But I think we're going to get authentication, we're going to get - well, for example, when everybody has SSL certificates because they're no longer expensive, and exactly as you said, then sniffing all goes away because no longer will your email username and password be going through an access point in the clear because the first thing you'll do is set up an SSL connection and encrypt the tunnel. And, I mean, so there will still be problems. But incrementally we're going to win this, I think, long term. I don't know if you and I will still be around...

Leo: Oh, that long term.

Steve: Oh, yeah, yeah.

Leo: Oh, we're a ways off.

Steve: Oh, yeah, yeah. It's not happening soon. It's difficult to see how we get there. And due to the need for standards, and this has to be done in a standards way, it's going to be baby steps. It's like the EVCerts. EVCerts is a perfect example of a good step forward which ultimately - again, it's chicken and egg. Ultimately commercial websites will have to prove that they are who they say they are, and they'll be able to advertise that in the bars of web browsers. I mean, it's - the other thing that was so clear to me, and I'm sure this is not news to our listeners, but the web browser is our window to the world. I mean, it is the application now, especially with Web 2.0 and 3.0. It's the way you do things.

Leo: We're going to talk a little bit about your Swedish lady and her amazing authentication system.

Steve: Oh, the one cool, I mean, the coolest thing I saw at RSA Conference 2000.

Leo: And she was just skulking in a corner because she'd been denied her booth.

Steve: Oh.

Leo: That's frustrating.

Steve: And she was cute, too. But, you know.

Leo: Oh, now the truth comes out.

Steve: Swedish.

Leo: Swedish. Smart.

Steve: Stina Ehrensvrd, I think is how I would pronounce - no, Ehrensvrd, E-h-r-e-n-s-v-a-r-d.

Leo: I just hope you got her phone number, that's all I can say. He's not saying anything. So let's talk about your Swede.

Steve: Yes, okay. Go open your browser, Leo, www.Yubico.com.

Leo: Yubico.com.

Steve: Yubico.com.

Leo: Follow along in the home version. Oh, there she is. She's the CEO, and she's very attractive.

Steve: Yes, and, okay.

Leo: Not that we're focusing on that.

Steve: No, no, no.

Leo: This is an authentication system.

Steve: Look at the little picture of that thing.

Leo: It's a key, it looks like, a USB...

Steve: Oh, yes, it is, Leo, get a load of this. It is a USB tiny thing which is a USB keyboard.

Leo: What?

Steve: With a one-time password system. So you know how you can have USB keyboards instead of, like, USB thumb drives or...

Leo: Oh, it shows up as a keyboard, I get it, I get what you're saying. The driver is using the HID driver.

Steve: Exactly. So it is a USB keyboard. And...

Leo: Wait, I don't see any keys on it.

Steve: No, and that's just it. Okay. See the little circle?

Leo: Yeah.

Steve: That glows green. And it is a touch button.

Leo: Okay.

Steve: So when you - okay. So for people who aren't seeing it, let me describe it to people. It is a tiny little wafer. As our listeners know, I'm very sensitive to the size of the junk on my key ring. I just can't have, much as I love the IronKey, I have a tiny little Kingston 4GB thumb drive because I actually can have it on my key ring, and it doesn't bother me. So Stina was standing there at the top of the escalator, heading down toward the...

Leo: Did she invent this?

Steve: Yes.

Leo: How cool. Stina Ehrensvrd. We should give her credit. Wow.

Steve: She's the CEO, the founder, and the inventor.

Leo: She is so cool.

Steve: Isn't it? It's just a perfect solution, Leo. I mean...

Leo: Well, tell us how it works. Tell us how it works.

Steve: Okay. So she sort of stops me, kind of, as I was getting ready to go down to the convention floor, and said are you with the press. And I had my press credentials, which the RSA folks were kind enough to provide me. And I said yeah. And she said, well, I have something that I want to - can I talk to you for a minute? And I said of course. And so she holds this little thing, which is just, I mean, it's wafer thin. I know that you and I have seen, like, USB thumb drives which are just like a little plastic wafer, that is all they are is like the four little contact fingers with a little - and that's what this is. So it is, I mean, it weighs nothing. It's got no extraneous fluff on it. And she says this is a one-time password authentication. And I'm like, yeah, I know, the floor is full of those. And then she says it's a keyboard. And I said, what? She says, it looks like a keyboard. And it's like, oh my god. And I then...

Leo: You got it right away? Wow.

Steve: Well, yeah.

Leo: Okay, you better help us because we're a little slower than you.

Steve: I live in this space. So, and I said, that is so cool. And then she sort of apologized because here she was pulling random people off to the side to show them this. And she explained to me that she had a deal and they reneged because she was supposed to be in one of the major corporation booths, but they decided no. And I think it's because they didn't have anything nearly as cool as this thing. So, okay. So the idea is, first of all, no battery. Unlimited shelf life. It lives forever. Unlike many of the other, I mean, all of the other things have a battery. Now, it does mean that you need to plug it in to use it.

Leo: It gets power from the USB port.

Steve: Yes, it's powered from the USB port, which has 5-volt power...

Leo: Wait a minute, I'm starting to see this now. So it actually types in your passwords.

Steve: That's exactly what it does. Which means it can be wacky and long. So the idea is...

Leo: Oh, now I get it.

Steve: Leo, it's so cool. Yes.

Leo: Okay. So tell me what's going on inside. What is it doing?

Steve: Okay. What's going on in side is there's a nonvolatile counter that increments once for each power-up event. So every time you plug it in there's a nonvolatile counter that increments by one.

Leo: So just like the VeriSign key, except you don't have to press the button. As soon as you plug it in, you're generating a new password.

Steve: Well, okay. So then there's a second counter that starts at zero when it's powered up and counts once for each code. And they use 128-bit AES to encrypt this. So basically this is a one-time password system. So, and you can - I've got to get some more of these so you can see it because I plugged mine in. And they've got a bunch of demo stuff where you can, like, see it happen. And the little ring sort of glows green. And I was, like, pushing on it. And I said, well, it doesn't go in. She says, oh, no, it's just a touch surface.

Leo: Ah, okay.

Steve: So you just put your finger on it and wait. It takes about a second. And she built a delay in so that it wouldn't misfire. And then it spits out this long string of gibberish. And we are very familiar, our listeners are familiar with long strings of gibberish because that's what this show is all about. And I don't mean verbal. So, and of course every time you do it, it generates a different long string of gibberish, which it's turned into ASCII, and it's typed by this thing pretending to be a keyboard.

Leo: So if I, instead of using my PayPal dongle, I would use this. When I get to the PayPal login, I type my password, then it says, okay, give me the dongle number. I would plug in my Yubico key. It would automatically type it in for me after I press that button, I guess.

Steve: Yes. Now, what's very cool, there are a couple things that I really like about this that, much as I have liked, when we talk about VeriSign, and we know that I think their credit cards are cool, you know, their one-time password system and the footballs and the dongles and all that, it does bug me that their business model requires major corporations to buy tons of these and then use VeriSign as the back end. That is, so VeriSign servers are performing the authentication. I've looked at, as we've said, I've vetted the API, I've looked at the protocol, it's 100 percent private. They're doing nothing, they're asking for no information they don't need. Basically they're saying what's your dongle number, what does the dongle tell you, yes, that's good. I mean, that's all they're doing.

But it means that, for example, as we know, my next product is going to be a really cool, next-generation VPN solution. Well, I can't use VeriSign because I'm not a big guy. I'm not Bank of America or PayPal or eBay or one of these huge companies. But I could use this because they offer a low-level SDK in C and Java, meaning open source, with all the code. So I could build the authentication into the VPN client itself so that when you're out on the road roaming around, you could use a YubiKey. Oh, and by the way, these are $4, depending upon quantity.

Leo: Wow.

Steve: So they have backend servers if you want to use them.

Leo: They have a web API. They have a web service.

Steve: Yes. And they are fully OpenID compliant. So you can use this as your OpenID authentication.

Leo: Oh, I'm liking it more and more.

Steve: And they have a PAM module, so you can use it for logging into Linux and Macs and anything that has PAM. They support - they have web clients in Java, C-Sharp, .NET, Python, PHP, and Ruby. So pretty much any website would be able to use this. It's just - it is a cool solution. Now, one way it differs from, for example, the VeriSign credit card and football is you could use those, for example, at a web kiosk to authenticate. That is, you could use those where you had no access to USB, that is, where you can't get to a machine's USB. But, for example, in a corporate environment where you want to have a corporate VPN, and you've got roaming laptop users, well, this is a really nice third-factor, multifactor authentication solution. And I just, the cleverness of it being a keyboard, a USB keyboard that all operating systems support - Macs know about USB keyboards, Windows, Linux, I mean, it's a universal standard.

Leo: That saves me from typing in some crazy, goofy password, too.

Steve: Oh, and these things, I mean, I've looked at it, at what it's typing in. And it's just, you know, it looks like...

Leo: Are they long, long, long?

Steve: Yeah, it looks like one of GRC's nutso Perfect Passwords, just gobbledygook, although it's all ASCII so that it doesn't have a problem getting through the web, and it doesn't need to be URL-escaped and all that. So, yeah, it is a - it's not something you would ever want to type in. Every time you touch the button it generates the next one. So it is a super-secure, one-time password system in the form of a super-tiny little USB thing that really could go on your keychain and be authentication. And since they're providing OpenID and back-end, anybody who wants to use this could, like, get these and use them for authentication.

Leo: You know what I like, let's say we wanted to do subscription-only access to, say, the video that we stream of this. We could - you send us the subscription fee, we send you one of these. And without that you can't get on. We don't have to worry, we wouldn't have to worry about piracy or even, well, I guess DRM we would have to worry about because it's content. But, I mean, that's pretty cool. At four bucks a pop that's very affordable.

Steve: Now, again, I wanted to say, in a show that was all pretty much stuff that we've talked about, and everyone saying this is the world's most amazing security identity authentication stuff, I mean, here was one thing new. And I just - I loved - I felt, of course, sorry for her story, that she would have been in a booth but she got removed. It's like, okay, well, sorry about that. Anyway, this thing is just - it is way, way cool. And I wanted to bring it to our listeners' attention. I mean, if we've got people who are, like, potential users, who are running websites, who have a need for some sort of authentication where, like - and what, again, I like about it is that you're not setting up a huge account with someone else. You can do all the authentication yourself in your own server or in your own utility or whatever. Just it's way cool.

Leo: Now, by the way, Yubico.com. And if you go there, she has on the front page somebody named Steve Osborrn saying "The coolest authentication hardware device ever." I think she means you, Steve. You might want to call her and say, uh, it's Gibson. Of course we've probably butchered Stina's name, too, Ehrensvrd.

Steve: Well, and I'm sure that's not me because...

Leo: I think it is you. There's no security researcher I know of named Steve Osborrn. I just Googled it. There's nobody there. I think it's you.

Steve: Let's click on references.

Leo: It's not mentioned. It's not mentioned. I think she threw that in, and she figured everybody's going to know who Steve Osborrn is. I think it's you.

Steve: Maybe it was a language gap, yeah. I mean, because she had, I mean, she was speaking English much better than I speak Swedish.

Leo: Oh, yeah, all the Swedes speak English very well.

Steve: Well, if this is me, you have my permission to change Osborrn into Gibson because...

Leo: It does sound like what you would say. In fact, I think you say that.

Steve: You know, it's funny because I read that this morning when I was getting the URL. And I thought, oh, isn't that nice, I wonder who he is. Maybe that's me.

Leo: It's you. I'm pretty sure. I don't see a Steve Osborrn in these other references. I'm pretty sure it's you. But I could be wrong. If there's a Steve Osborrn listening, I apologize. But he can't be that well known because he doesn't show up in Google. And you do, by the way, if you type in Steve Gibson. If you do, you'll get sent to GRC.com. That's Steve's website. That's where he sells SpinRite, of course, the world's finest, best, the only, really, hard drive maintenance and recovery utility that's worth talking about. He also gives away a lot of great free stuff. Oh, highly recommend visiting just the freebies on GRC.com, like ShieldsUP!, which you can use to test your firewall, Shoot The Messenger, DCOMbobulator, LeakTest, UnPlug n' Pray. I love Wizmo. You might want to take a look at the newest Wizmo plug-in, which turns off zero config. I had a woman call the radio show Sunday, and she said my wireless keeps dropping its connections, it keeps dropping its connections. And I went, oh, I know what that is.

Steve: And speaking of which, Leo, my tech guy, Greg, has had a constant problem with that. And in his case, the wireless zero config, turning it off did not solve the problem.

Leo: Ah, okay.

Steve: He did a lot of Googling. It's been bugging him for months. It was his laptop's modem.

Leo: Oh, wow.

Steve: It was the modem drivers. He disabled them, and the problem disappeared.

Leo: That's why computer issues are so tough. Because it's a million things. It's such a complex system. Well, Wizmo's fun even if lanlock, or wanlock I should say, doesn't do it for you. It's certainly worth having. And that's also where you'll go to get 16KB versions of the show, for those of you who are bandwidth-challenged. We also have complete show transcriptions there, thanks to Elaine. And we'll have show notes, and there's a lot of links.

Steve: Yes, we're going to be link-happy for this week's episode. I'll get that page to you and Dane right away, Leo.

Leo: Excellent. Steve, I thank you so much. Great talking to you. And I, you know, I think this sounds like the RSA conference was worth your trip up to San Francisco. Sounds like it was fascinating.

Steve: It was fantastic, and I'm really glad that this show is able to bring it to our listeners.

Leo: Yeah. We will see you all next week on Security Now!. Thanks for joining us. Take care, Steve.