Internet Privacy Update

Description: The day before recording this podcast in the studio with Leo, Steve attended an annual Internet privacy conference. After catching up with the week's security news, updates, and errata, Steve shares what he saw and learned during the conference, including three VERY promising new privacy and authentication tools.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-327.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-327-lq.mp3

Leo Laporte: It's time for Security Now!. Steve Gibson is here to talk about your privacy and your security online. Hi, Steve. I don't ever get to see you in person. This is twice in two months.

Steve Gibson: Okay, but it's not going to be a habit.

Leo: Oh, please.

Steve: No.

Leo: I would like it if you'd come in on a regular basis. It's nice to have you.

Steve: You have traffic up here, the same way we do in Southern California.

Leo: Did you run into some traffic?

Steve: No. This time I set my entire trip up so that there would be none.

Leo: To avoid it?

Steve: To avoid it.

Leo: Took back roads?

Steve: Specifically for that. Everything was designed.

Leo: Well, what brings you to our neck of the woods?

Steve: Well, I came up yesterday for an Internet privacy and identity conference, which was held down in Palo Alto, and spent the day listening to people who spend their days thinking about privacy.

Leo: Wow, that sounds interesting.

Steve: Yeah, it was. And so I want to talk about just a whole bunch of sort of tidbits that were thrown out. It was - it's sort of disorganized. It was disorganized there, and it's still disorganized in my head. And I don't know that there is any way to organize it. But it'll be fun to talk about that. And then there were a couple product presentations, which is going to be of huge interest to our listeners. And of course we've got news and updates.

Leo: And I know that you did a little work on the Apple sandboxing thing that we kind of surprised you with last week.

Steve: I now understand what it is.

Leo: Good. I'd love to get your take on that.

Steve: So we'll follow up, yup.

Leo: But I want to say this was a big sacrifice for you to be here today because you probably forgot that today is the day, actually it was yesterday...

Steve: I didn't forget. I'm going home to get mine.

Leo: ...that the Fires arrived.

Steve: It's waiting for me.

Leo: In fact, they shipped early in some cases. So you didn't get it on Monday, though; huh? We had - Liz got hers on Monday.

Steve: No.

Leo: Isn't that weird? So anyway, I thought I would be - I would let you - this just came. I haven't turned it on yet. But I just thought you could maybe hold it to see what it's like. It's got a kind of nice rubberized back.

Steve: Yeah, nice.

Leo: People have compared it to the BlackBerry PlayBook. It is roughly the same size, shape, thickness, and weight, although the iFixit guys have done a teardown, and inside it is nothing like the PlayBook. And in fact that might be one of the criticisms. It doesn't have as much horsepower, as much RAM, as perhaps it...

Steve: It has half, I think, of what the iPad has?

Leo: Yeah.

Steve: Or the PlayBook?

Leo: Yeah. And maybe that's - some of the complaints, and we're already seeing some complaints on this, are on the speed, and maybe that's why is because it's not as powerful. It's running Android, and there are some things, you can see it can already sign into - the first thing you do, it says "Welcome to the Kindle Fire." I'll sign in and...

Steve: It's got all your networks there [indiscernible].

Leo: Yeah, I'll sign into it. Don't show my password, please. Although you'd have to be sitting outside. It's pretty easy to type on this.

Steve: Wow. You're good with your thumbs.

Leo: Yeah. It's a good thumb typer. And that's one of the reason I like seven-inch, because seven-inch is narrow enough that you can kind of do that.

Steve: It does feel solid. It feels sort of heavy for its size.

Leo: Yeah. Which is not good for a reader because that's one of the things I like about the Kindle, it's basic.

Steve: Oh, and in fact I almost think that they've overshot the size goal with the new

Kindle. I've been using mine now, the $79 one. It's almost too small. I like the Kindle 3 that's got the keyboard on it because that paddle at the bottom sort of gives you something to hold.

Leo: Right.

Steve: I really...

Leo: So you don't like that new $70 or $80 Kindle.

Steve: No, I had to have one. But [indiscernible] kind of look at it.

Leo: I like how light it is, and I can put it in my pocket.

Steve: Well, for travel, if you want to walk around, it does fit in your pocket better. So I agree.

Leo: Right. So this is now - and we won't do any more because it's now going to download the Kindle software, an update to the software, and do a reboot. So one of the complaints people had about it was that...

Steve: Anyway, thank you for letting me touch it.

Leo: Well, you can touch it some more.

Steve: No, I'm done touching it. I'm going to touch my own.

Leo: Always touch your own. I did play with Liz's yesterday. And one of the complaints David Pogue and others have had is that it doesn't feel snappy. Our MacBreak Weekly team said sometimes you'd tap an icon, and you wouldn't know if anything was happening. And maybe that's what's happened a couple of times. And we tried some page turns, and you can actually see a visible, not big...

Steve: Stutter?

Leo: ...but minor stutter as it's redrawing the page. So 200 bucks...

Steve: Oh, my god, for the price. And I looked back at what I paid $400 for from Amazon, that funky wedge-y Kindle and went, oh, my goodness.

Leo: That's right, that's right.

Steve: I mean, it just looks like a dinosaur now compared to the Kindles we have just a few years later at 20 percent the cost of the first one.

Leo: I agree. I agree.

Steve: So if this thing has the horsepower - well, and, I mean, we're all spoiled about gigahertzes. I mean, of course it's got the horsepower. If they need to tune it and optimize it, they can do so.

Leo: Well, and in fact I wouldn't be surprised to see a firmware update addressing some of these complaints in the first...

Steve: Which is sort of a short way of saying what I just tried to.

Leo: Yes. Well, I think also what you're saying is there'll be new hardware, as well. I mean, they're going to iterate...

Steve: Probably.

Leo: They'll iterate on this.

Steve: Yeah, yeah, yeah.

Leo: Yeah, I agree. I do get a - now, I know you got a bunch of cases. You'll probably end up talking about the ones you got. I got the Marware executive case. So it's kind of fun. It's a leather - looks like a Moleskine. It's got that little rubber band on it.

Steve: Yes. And I'm not a fan of cases. Well, I mean, I'm a fan of cases, but not of attachment things. I like to have something where, like, I take it out, and I just - I use it.

Leo: You know how hard this is to attach? It's like you've got to snap it in and...

Steve: Yeah, good luck detaching it.

Leo: Yeah, exactly. So maybe this is the best choice.

Steve: So anyway, next week I'll have my opinion to add to all the other gurus.

Leo: This is what we call a "first look." I don't know. I think this, for a tablet that's made of glass, something like this is kind of important; you know?

Steve: Yeah.

Leo: And I think it looks good. It's got a stand on it, and it seals up. And I think this will be - and the little - one of those little hand - they do this all the time in these cases. Like you do this. I don't know. Does somebody hold their - everybody seems to hold their case like this. I don't know why they...

Steve: No.

Leo: I don't do that. But anyway. Oh, I can get started now. That was quick. So it's going to reboot. So it downloaded the update while we were talking.

Steve: Well, you have good bandwidth here.

Leo: We're going to take a timeout before we get into the security updates. Firefox 8...

Steve: And counting. Although Chrome is at 17 or something.

Leo: Yeah, I know.

Steve: It's like, my god.

Leo: You're not supposed to look. Just pay no attention to those numbers. Also some news about Adobe's Flash.

Steve: Well, you know, get it.

Leo: The usual...

Steve: Yeah, exactly. You see I have one line there, just "update."

Leo: All right. Let's get into the meat of the matter. We'll start with Firefox.

Steve: So, yes. Firefox 8. I grabbed it, I guess, a little before a week ago in beta, and loaded it, and looked at it, and then went back to 3.

Leo: 3. 3. We talked about this last week, but I just think it cracks me up. Not 7, not 6, not 5, not 4.

Steve: They all bleed memory.

Leo: 3 is the last one that didn't leak.

Steve: Yes. It is not leaking. And I've had so much Twitter feedback from people who even are now using 8, and they wake up in the morning, and it's gone to 2GB of memory consumption. Now, there is news just today that I haven't had a chance to follow up on in detail, that Mozilla is now saying it's the fault of the add-ons. Which...

Leo: Well, I always wondered because...

Steve: ...is entirely possible.

Leo: ...we put so many extensions on our Firefoxes.

Steve: Yes.

Leo: I noticed that that really does slow it down.

Steve: Yeah. So they're talking about having some sort of solution for add-on and extension memory consumption. So we'll see. So this fixes seven security flaws, that is, the update to Firefox 8, four of which they rated critical. And all four of those are exploitable through drive-by downloads. So people who are on 4, 5, or 6 or 7, ought to update to 8 for the security benefits. And, I don't know, turn your computers off at night.

Leo: I thought they were going to fix this.

Steve: Well, in fact, I think 7 was supposed to fix the memory problem. Now, there is that cool add-on called Memory Fox which does seem to be working for me. It doesn't reduce its virtual memory footprint, so it's still consuming system memory. But it does push it out of RAM, which is valuable just for itself. Also, v8 gives us an optional Twitter search feature, built in. So 8 can search Twitter for you. It's like, okay. I'm not sure...

Leo: You've always been able to add a custom search to Twitter so that you could just do "t" and then the search. But I think this does it...

Steve: Right. And there was some problem that we talked about actually in the past where third-party add-ons could be installed without your explicit permission. And so they've blocked that. And now you'll get control over that happening, before that happens. So anyway, Mozilla Firefox is at v8.

Leo: Can I ask you a question? Did anybody offer you a cup of coffee when you arrived? Do you have a quinti venti...

Steve: I got 12 shots in me already.

Leo: Okay, never mind.

Steve: I'm fine.

Leo: In person you're just so calm and serene, I didn't realize. Good, all right.

Steve: Yeah, when is that? So Adobe has updated, yet again, Flash to 10 point whatever they are, 1 or 2. So get it. You'll get the notices and ...

Leo: Did they say anything about the security?

Steve: Yeah, they fixed a whole bunch, I think 12 or 13 problems, so...

Leo: It's not even worth mentioning anymore, is it.

Steve: No, it's not. Just get it.

Leo: Are you happy that Adobe is finally killing Flash on the mobile platform? Because I think the other shoe on that is they're going to have to kill Flash on the desktop because, if websites stop using Flash, what's the point; right?

Steve: What we're seeing is, and I heard this yesterday at the conference, that HTML5, scripted, which is to say JavaScript and the capabilities, the hooks that are inherent in HTML5 really do obsolete Flash. You just don't need it. So it's going to end up that, when the history books are written, it will have been an interim technology.

Leo: Right, just like RealAudio.

Steve: Yeah. I mean...

Leo: Just a temporary thing.

Steve: Not everything lasts forever.

Leo: Nothing does.

Steve: And this one really, yeah, oh, good point, yeah.

Leo: Not even us.

Steve: So, yeah. So it served its purpose.

Leo: Yeah.

Steve: So many sites that are only using it to display video, they don't need to, I mean, many sites just used it for that. And so we don't need that anymore. And if you need more fancy stuff, you'll be able to do it with the hooks that HTML5 provides and JavaScript. And you get more performance. You don't have to have an add-on. You don't have all the memory consumption problems. I mean, it's very much like what Windows CE tried to be. Microsoft didn't have a battery-operated operating system when Palm and all of the OSes that were made for portability came out. So they tried to take Windows and squeeze it in.

Leo: Bang it with a hammer.

Steve: Exactly. And that never worked.

Leo: Now, are you worried that HTML5, because of its heavy reliance on JavaScript, is going to have issues, security, I mean, obviously it will. And you can't use NoScript if the whole world is on HTML5.

Steve: Yeah. And NoScript, I think, serves the purpose of giving you a gatekeeper, where you're able to go to a site and decide explicitly, it's like, okay, this looks like a place I'm willing to trust, or I need to, I have no choice. So I think, again, we're seeing more focus on putting fences around things. We are talking about sandboxing. We have a lot of attention that Google has given to security in Chrome. When I've got a bunch of Chrome tabs open, I see individual processes in my task list in Windows. So each of those pages is a freestanding process that Google has gone to some measures and lengths to isolate from everything else. And also, if the script hangs, you're able to just kill that one, and it doesn't kill the whole browser. So we're seeing an evolution in all of that.

Leo: Once the world is all HTML5, we'll have to obviously handle it.

Steve: And I like having - it's like Adobe had too much power and really didn't have - wasn't being responsible with it. Too many, there were too many...

Leo: Right. In terms of security.

Steve: Oh, my god, I mean, there have been so many people who have been infected through Flash. So it's like, eh, they had a shot.

Leo: Duqu.

Steve: Duqu. I've seen some rumor on the 'Net that we're going to be waiting a month before Microsoft fixes this TrueType embedding problem, which...

Leo: So just to catch people up, if they didn't see last week's episode, Duqu is another worm kind of similar...

Steve: To Stuxnet.

Leo: ...to Stuxnet that does take advantage of a TrueType font rendering engine in Windows.

Steve: Yes. In the reverse engineering of Duqu, because all the security guys got samples of it, they started checking out, okay, how is this thing propagating? And they discovered, by looking at how it was spreading itself, a previously unknown kernel flaw in the TrueType font rendering in all versions of Windows.

Leo: And as we mentioned last week, odd that they put that in kernel, but there you go.

Steve: Well, they did it for performance back in the day. And so this is biting them. And it's not the first time that them moving GUI stuff, their GDI...

Leo: Right. Remember the WMF issue?

Steve: ...their Graphics Device Interface, GDI got moved into the kernel, and all kinds of problems. Yeah, and of course the WMF flaw, too. So by figuring out what Duqu was doing, they discovered a previously unknown flaw in Windows. Microsoft is saying, whoops, we'll fix that as quickly as possible. It did not make it in last Tuesday's, the second Tuesday of the month update. And now the concern is that other malware will

start using it, too. So all you have to do is cause something to render a font in a specially crafted font that is able then to execute any code that it wants to in the kernel. And that never has a good outcome. So anyway, so I just wanted to say to users, to our listeners, that little quick fix that Microsoft has, I talked about it last week, it's still near the top of my Twitter feed. So you can go to Twitter.com/SGgrc.

Leo: I have it right here.

Steve: And there's a link there that'll take you there. And click that button, and you're secure. And then Microsoft will be fixing it for real. I'm sure for December they'll have this thing ready because this just can't be that hard to get...

Leo: Does the fix disable TrueType fonts or...

Steve: No. It just disables something you don't need anyway.

Leo: Okay. So it's no big deal.

Steve: So thank you anyway, Microsoft.

Leo: Thanks for turning that on in the first place.

Steve: So just in the news, everybody's in a big froth about this. My own Twitter feed has been full of this, is this supposed rootkit that all of the phones have installed by default.

Leo: What?

Steve: HTC, T-Mobile, a bunch of phones. It's called CIQ, Carrier IQ. And...

Leo: This is intentional, though. This isn't something they accidentally...

Steve: Yes. It's like all the carriers are spying on you. Boy Genius Report reveals that the HTC Sensation and EVO 3D - and that's like some time ago, and this is all just sort of...

Leo: Look what it says here: 141,046,720 handsets deployed, right on their front page. They're, I mean, they're saying everybody uses this.

Steve: Yes. So what this actually is, this is like, everybody calm down. This is a third party that offers technology to handset carriers to enhance the customer experience. So

this thing, I mean, you can call it a rootkit, but it's part of the kernel. I mean, it's part of...

Leo: It is kind of not appropriate to call it a rootkit.

Steve: It really isn't. It's inflammatory, and it worries people. So the question is, are our handsets spying on us? Well, yes.

Leo: We knew that.

Steve: They know where you are. They know what you do. And so...

Leo: They didn't need a rootkit to do that.

Steve: Precisely. And so it's - Carrier IQ is the company. And, for example, Carrier IQ themselves say, "Carrier IQ is the market leader in Mobile Service Intelligence solutions that have revolutionized the way mobile operators and device vendors gather and manage information from end users," which is to say the people walking around with these phones in their pockets. "Recognizing the phone as an integral part of a mobile service delivery, and using the device to measure key parameters of service quality and usage, the Carrier IQ solution gives you the unique ability to analyze in...." Now, "you" meaning the carrier.

Leo: The carrier, right.

Steve: "...analyze in detail usage scenarios and fault conditions by type, location, application and network performance while providing you with a detailed insight into the mobile experience as delivered at the handset rather than simply the state of the network components carrying it."

Leo: So the way they're selling it to carriers is this is to help you in your network management.

Steve: Precisely.

Leo: Network load management, usage, so forth.

Steve: And so one way to think of it is that the carrier always was providing your connectivity, but they were a ways back from you. So this pushes some intelligence out through the cell tower, out to the endpoint, which is your handset. And so, if a lot of users, when they all open a certain application, their phones crash, well, that's something that you'd like the carrier to know immediately. And so this provides you with that kind of closing the loop feedback.

Leo: The concern is that in the process it monitors, not only location, but could monitor what apps you've installed, when you use them, how you use them, how frequently you use them.

Steve: Anyone who thinks they have privacy from their carriers about what their phone is doing is fooling themselves.

Leo: And Sprint says, "We just want to know what problems people are having with their network or devices so we can improve service quality. It collects enough information to understand the customer experience and how to devise solutions to use and connection problems. We cannot and do not look at the contents of messages, photos, videos, et cetera, using this tool." HTC says you have to opt into this error reporting function.

Steve: It pops up a screen. And then you're able to optionally send feedback about the event to explain...

Leo: We're seeing those screens more and more. Google, Microsoft, everybody does this now. Which, when you install OS X, Apple says...

Steve: User experience feedback.

Leo: Yeah. iTunes, would you like to send information back to Apple? And you know, the truth is, I've always just said yes. I think most people are, yeah, I'll help you out. I want to make it a better product. So go ahead and collect that information.

Steve: Sure.

Leo: Maybe now, if this is something that worries you, you should think about it. But you've got the right point, which is they can do this anyway.

Steve: Yeah.

Leo: They've got all this. It's like your ISP. Your ISP knows everything you do online. They have to.

Steve: Right. Right. So I think the proper area of concern is what the third parties know and can do who have installed apps on your phone.

Leo: Good point.

Steve: And we'll be talking about that a little bit later in this podcast, as we have talked about it for the last seven years.

There was a nice vote in the Senate, 52 to 46, to oppose regulation which was opposing the FCC ruling. The FCC is currently fighting the large carriers on the issue of Net Neutrality. And so the good news is that the Senate did what I think was the right thing because there was some legislation that was opposing what the FCC was trying to do. SANS editor Murray said the FCC rule surrendered to AT&T and Verizon on the air side, where it matters, in return for sites on the wired side, where it doesn't.

Leo: That's kind of what Google's manifesto with Verizon suggested, as well.

Steve: Yes.

Leo: Don't regulate the wireless carriers. You can do the landlines fine. Don't regulate the wireless carriers.

Steve: Right. And Alan Paller, who's the director of SANS, said the answer to William Murray's question "may be that AT&T and Verizon lobbyists, along with those of a few other lobbyists representing IT companies, are now approaching Enron's lobbyists in power..."

Leo: Oh, boy.

Steve: "...to shape federal actions and in disregard for the public good. Lawsuits by the big carriers who don't want to be bandwidth-neutral carriers are still pending." So despite this, there is a fight which is underway. And this is one of the things to watch is to what degree carriers will have control over the way they deliver bandwidth. Are they common carriers that are just open conduits? Or do they have the right to give preferential treatment to some services on the network over others?

Leo: Now, that's the good news. Here's the bad news. You know this is American Censorship Day. Today the Congress is having hearings on SOPA, IP Protect, which are two bills in front of Congress that would essentially turn on, as we've talked about before, an Internet censorship system, H.R. 3261. And everybody and their brother, including Matt Cutts, I was really interested to see this on his blog - Matt Cutts is of course the antispam fighter for Google we talk to all the time. He says, "I need your help. Please call your congressperson." Let them know, especially if you call them on the phone, he says. If you live in Texas, Michigan, Vermont, and Iowa this is especially important. Tell your friends. Let people know about this SOPA and these SOPA hearings that are going on right now because it would really in effect shut down the Internet as we know it and give, basically give our government the right to censor, based not on due process, but just on...

Steve: Well, and this segues perfectly into another article that I wanted to mention. Ars Technica carried a great piece about Warner Bros. admitting that they issue takedowns for files they haven't even looked at. SANS gave this some really good coverage. They

sort of created a synopsis of this, saying that Warner Bros. has admitted that it used an automated takedown tool to request the removal of files from the Internet that were obviously not infringing on the company's copyrights. The case involved Hotfile, a locker site that maintains it is in compliance with the Digital Millennium Copyright Act, the DMCA, because it follows the rules about notice and takedown procedures. In fact, Hotfile provided Warner Bros. with a takedown tool to facilitate the process in working with them. Hotfile is now arguing that Warner Bros. violated, that Warner Bros. themselves violated the DMCA when it ordered the takedown of files that were clearly not infringing copyright. The data used in those takedowns appears to come from an automated data scraper, rather than a human being's examination.

Leo: We can't be bothered. We can't be - it's too much trouble.

Steve: Warner Bros. says it cannot possibly, okay, quote, "It cannot possibly examine all suspect files due to their sheer volume."

Leo: There's just too many of them.

Steve: But the DMCA requires that copyright holders issue takedown notices only when there is, quote, "a good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law." So now what we're seeing is, we're seeing that these companies have automated scrapers that are going out and just gathering up thousands of URLs and dumping them onsite, saying remove all these. And when you take a look at them, it turns out they're not, I mean, the scraper has over-scraped, and now this DMCA is being used to hit people over the head.

Leo: Yeah. And that's the issue is that these people who don't like piracy, these companies like Warner Bros., would love to just censor sites right and left. You can see the broad brush and the...

Steve: It's like how they tried to prevent VHS tape from ever happening. They didn't want consumers to be able to have recorders in their homes.

Leo: So this is a good day to participate. It's American Censorship Day. And we just want to encourage everybody who wants to know more, you can go to EFF.org to read more. PublicKnowledge.org has information on this. There are lots of sites you can go to read more. And then absolutely, please, send - electronic is not good. You want to either write to them, or better yet call them.

Steve: Well, you can ignore electronic. It's like...

Leo: Well, they also want to know you're a constituent. So if you mail it to them, they see the postmark. They really want to know that you're a constituent. It's fine to write other members of Congress. But write your member of Congress especially, and do it with a postage mark because that way they know it's you, and you vote.

And we've really got to do this. Today's the day. Everybody, please, who's watching. And it's not too late. It's not too late. If you're watching this later, you can get involved. But I know, those of you who are watching live, we should absolutely do this.

Steve: Well, and one of the SANS editors, Tom Liston, followed up with this on this Warner Bros. issue, with something I thought was just exactly on point. He said, "Warner Bros.' assertion that it 'cannot possibly examine all files' is more than a bit disingenuous. What they're really saying is..."

Leo: They just take down the Internet.

Steve: "...that they don't want to incur the costs associated with examining the files themselves. Media companies are all about enjoying the monetary benefits of their copyrights, but are constantly looking for ways to foist the cost of protecting those copyrights off onto someone else."

Leo: Yeah. Just terrible. Just terrible. You know what I'm going to do? I think we will - somebody's suggesting this in the chatroom. I think it's good. After the show is over, in between this show and TWiG, I'll call my member of Congress on the air.

Steve: Ah.

Leo: And we'll just say, hey, SOPA, [sound effect].

Steve: Yes.

Leo: Because this is just terrible.

Steve: Okay. So last week you surprised me.

Leo: I did. I'm so sorry. But you handled it gracefully. "What?"

Steve: Actually I saw, was it - it couldn't have been the chatroom, must have been a tweet. Someone said, "If we could have a snapshot of Steve's face," which you, on the stream, yeah, exactly, when you said that the sandboxing was going to be for...

Leo: Apps.

Steve: Apps.

Leo: Desktop applications.

Steve: Not iOS, but Mac OS X apps. So, okay. What this is, this is not as onerous as the developers have been bitching and moaning that it is.

Leo: Good. Okay. Okay.

Steve: This is technology which first appeared in Leopard. So this has been since 10.5 of OS X.

Leo: But they didn't require it.

Steve: Right. First of all, all POSIX-based OSes - UNIX, the UNIXes, Linuxes, Apple, FreeBSD, all of these, even Windows - has these things called DACLs, Discretionary Access Control Lists. And you can see them if you right-click on a file and look at permissions. There's this very complex, hierarchical...

Leo: ACL.

Steve: ...ACL which controls who is able to access that file.

Leo: All multiuser operating systems need this. Otherwise anybody could tree walk the operating system's hard drive and see your files.

Steve: Well, and root...

Leo: Has access to everything.

Steve: The root user is god.

Leo: Right.

Steve: It automatically has access to the whole system.

Leo: Right.

Steve: So what this so-called sandboxing is, is actually something called Seatbelt. And Seatbelt has been around for a while, as this has been. It was introduced some time ago. So this sandboxing introduces something called - instead of being a DAC, a Discretionary

Access Control, it's a MAC, a Mandatory Access Control. Which is to say, it even affects root users, which is what it has to do in order to be effective. Otherwise, running as root means that you're able to bypass this whole thing.

So the idea is that, in an operating system, at the API, you deal with everything with handles. You have handles to files. You have handles to sockets, which allow you access to the Internet. You have - basically everything works with you wanting, you asking the operating system to open access to something, whether it's a directory or a file or a communications pipe or whatever. The OS gives you back a token, if you have permission, if you have rights. And so what Apple has done is they've created sort of a set of useful rights, which applications can request access to.

Leo: They're called "entitlements."

Steve: Entitlements. And the idea would be, is an application will only request the entitlements that it clearly needs. And when the App Store is looking at your app and...

Leo: Validating, approving it, yeah, yeah.

Steve: ...validating it for approval, they'll look to see whether you're asking for unreasonable things. And so they'll say, wait a minute, why do you need access to the local network if you are just doing things on the Internet? And so the idea would be that hopefully the authors will only ask for the things they need. There may be some negotiation between Apple and the authors, where the author explains why they need access to the local network. So, for example, applications that don't really need local network access would not have that entitlement.

Leo: They'd uncheck the box that says "allow incoming network connections" and "allow outgoing network connections."

Steve: Or local connections. So there would be, in this final version, and Apple is still working on making this granular enough, there would be a differentiation between local and Internet. But in this example, if an application didn't explicitly have reason to require local network access, then Apple would put up a little resistance to...

Leo: So they're going to look, when they're validating the app, and say, what did you request? Will they - and this I would love to do, and this is certainly something that happens on Android - will they then publish that when you download the app, saying, by the way, this app has requested these permissions? Android does that, and I like that feature.

Steve: Nice to be able to see.

Leo: Apple has not traditionally done that.

Steve: And so the beauty of this is, when the application starts up, it puts itself voluntarily into the sandbox, only having those entitlements which it has been - which its code is written to require. And if anything goes wrong with the app, it, for example, couldn't get local network access, if it didn't have that agreed-upon...

Leo: It just never can.

Steve: It never can. And that's a good thing. Clearly that's a good thing for security.

Leo: So if people were hacked, or a bad guy got into it, or it were a bad guy application, doesn't matter. You can't write it that way. But they have to enable sandboxing, which isn't necessarily required.

Steve: But we now know that it will be as of March 1st of 2012.

Leo: And they have to be fairly specific about what entitlements they're requesting.

Steve: Right. And they have to be able to justify those, show that their app actually needs the rights that they're asking essentially Apple and the OS to give them.

Leo: I presume somebody will write an app that watches installs, or you could run it after the fact, that says here's the entitlements requested. Because you do create an entitlements file that says here's what I need, here's what I'm allowed to do.

Steve: Correct. And you are able to use that in order to make them additionally granular and then - so anyway, it's a good thing overall, not the end of the world. And developers are just complaining because they're going to have to do a little more work.

Leo: But you can still get access to all the things you would have before. You just are announcing that you're going to do it.

Steve: Yes. And they're...

Leo: That is not bad at all.

Steve: No, it's not.

Leo: That's fine. I could totally tolerate that. Thank you for looking into that.

Steve: So we've talked a lot in our How the Internet Works series about whether there's going to be a need for a second Internet. I talked about how someone at Microsoft was

talking about the Red and the Green Internet, where the Green Internet would be somehow secure from the start, whereas the Red Internet would be the way it is now. And at a recent talk, Vint Cerf, who is one of the fathers of the Internet who designed these protocols, who is now an Internet evangelist at Google, made a point of saying that there isn't a need to scrap what we have. Don't throw the baby out with the bathwater is exactly what he said during this conference. He said what we have is an underlying framework, upon which anything we need can be built.

Now, I would argue there are problems that the fundamental packet processing nature of the 'Net doesn't allow us to solve, like denial of service attacks, because if you have autonomous routing, and anybody who wants to can put any packet they want to on the Internet, and the Internet's routers will attempt to send it to its destination, well, you have a bandwidth aggregation problem that creates the possibility of denial of service attacks. So that's not a security problem, but it's a problem with the architecture of the Internet. So it's like, well, okay, yes, certainly we can fix security. But there are things like traffic flow problems that we're not going to be able to fix unless we re-architect. And we're not going to do that, either.

Leo: I guess, I mean, look, it's his baby. So what he's really saying is, look, we did a good job. Just...

Steve: And I don't disagree. I think it was brilliant. It just didn't solve all the problems.

Leo: Right, right, right.

Steve: And we mentioned a little bit Honor Harrington. I've been very good, Leo. I've been very good the last few weeks.

Leo: Sci-fi book group time.

Steve: Kris Thurston sent me a note. He said, "Curse you, @SGgrc, with your sci-fi novel recommendations. I'm now bound and determined to finish the Honor series. Second book was ridiculous." So I thought I would just briefly tell our listeners...

Leo: Wait a minute. Ridiculous good, ridiculous bad?

Steve: Oh, ridiculous fantastic.

Leo: Ah.

Steve: Like over-the-top ridiculous.

Leo: Oh, boy.

Steve: Like, you know, forget about sleeping.

Leo: I'm almost through with book one. I've been diverted by the Steve Jobs book and other things.

Steve: Yeah. And Mark Thompson read the Steve Jobs book. He doesn't read anything.

Leo: Yeah. Well, it's fascinating.

Steve: And he, apparently, was - I guess Isaacson was pretty ruthless.

Leo: Oh, yeah. It's not in any way...

Steve: A whitewash.

Leo: ...a whitewash. But it's what Steve - I think it's what Steve wanted. He wanted an honest book. He said, "I'll read it later."

Steve: Yeah, well, and Steve asked, he said, "Am I going to like - are there things in here that I'm not going to like?" And Isaacson said, "Yeah, there are." So it probably all worked out for the best with the timing of all this. But anyway, I am 40 percent, I think, into book seven of Honor Harrington.

Leo: Great.

Steve: My legs have never been in better shape.

Leo: Because you only read...

Steve: No, I don't.

Leo: ...on the treadmill.

Steve: I could not, I could not keep that promise to myself. But I also read on the treadmill.

Leo: How many are there? How many are there?

Steve: 12.

Leo: 12. Well, you'd better slow down, dude.

Steve: I know.

Leo: You've only got five more.

Steve: But we do have Hamilton. I never did read, I never got into the Dream Void, whatever that thing is.

Leo: The dream, the void? Oh, that's quite a bit. That'll keep you busy for a while.

Steve: That'll keep my legs in good shape, yeah.

Leo: All right. Well, I have to redouble my efforts to read more.

Steve: So I wanted to share a listener report. Daniel White, a listener of ours in Bristol, England, caught me, caught my eye with a subject of "SpinRite cost me a laptop."

Leo: Uh-oh.

Steve: "But that's okay," he says. "Hi, Steve. Here's yet another testimonial for you, if you want to use it on the Security Now! podcast." Well, and what do you know. "Last month a friend of mine mentioned that his old HP Pavilion laptop had just given up and was producing the dreaded 'boot device not found' error. He was a bit annoyed because he had some family photos on there, and naturally he didn't have any backups. Ordinarily I would understand, but the friend in question has a master's degree in computer science." So he should know better. But then, shouldn't everyone.

"He was ready to toss the laptop out, as he said it had been running like a dog for months and had been running so hot that the adhesive holding the rubber feet on the bottom had melted. I suggested that there was probably a way to fix the hard disk and get his data back, and it would be a lot cheaper than buying a brand new machine. SpinRite could have a try at recovering the disk; and, if it couldn't fix it, then the drive was definitely toast.

"My friend made me an offer. He said he would pay for a copy of SpinRite to use on his drive; and, if it worked, I could keep the copy of SpinRite. If it didn't work, I could keep the dead laptop so I could buy a new drive and resurrect it myself.

"I purchased a copy of SpinRite, burned a boot disk [meaning a CD] and set it running at Level 2. At 18 percent of the way in, DynaStat kicked in and churned away for a while before reporting the sector had been recovered. I left SpinRite to complete the disk, just to be sure, and two hours later" - okay, not two months, Leo. I've done some testimonials here that I think have scared people. It's only normally a couple hours. "... [T]wo hours later it completed with no further errors. I rebooted, and voila. Windows

Vista booted right up the first time. I was so pleased to have got a free copy of SpinRite.

"I asked my friend if he wanted to speed up his system, and he said I could try. I found to my horror it still had all the crud that HP preinstalled on it, as well as two antivirus packages and only 1GB of RAM. I deleted all the HP crud, removed the out-of-date AV suite, and installed an extra 2GB of RAM for him.

"He now says his laptop runs better than new, and I have SpinRite to thank for getting his drive back. Thanks to you and Leo for such a fascinating podcast, and thanks so much for making SpinRite such a great product. It may have cost me a laptop, but at least I got a free copy of SpinRite. Dan White, Bristol, England."

Leo: Hey, when it's broke, it's broke; right? What are you going to do? There's nothing you can do about it.

Steve: And it worked.

Leo: We were mentioning the SOPA hearings that are going on right now, and I just wanted everybody to know, if you go to EFF.org, they have a big banner on the front page. I know it's up and down. There are so many people doing it right now. And if you look at my screen right here, they'll take you to a page where you enter your zip code. And they give you, they couldn't make it easier, the phone numbers of each of your representatives and senators, and they even give you texts, suggested texts. You can send an email, but I would suggest instead, and I would like everybody watching this show, that you call that phone number and just say I'm calling, I'm a constituent of, in my case Rep. Woolsey. And I would just really strongly ask Rep. Woolsey to not pass the Stop Online Piracy Act, the SOPA Act. It is bad for the Internet. It is bad for the country. Please ask her to vote against it. That's all you have to do. They just keep track of all the constituents who call. And I think it's a very valuable thing to do. And we will do it after the show.

EFF - see that bar, by the way? I put that on my website, as well. In fact, we should put this on the TWiT website. If you go to Leoville.com you'll see this big thing pop up. And this is what we're talking about, folks. We don't want to allow this kind of censorship to happen. So when you go to my site you'll see that. And I think every - by the way, if you click that link, "Stop Censorship," you can get the code to put on your site. Let's get everybody. Let's get everybody today to put this on their front page and let everybody know about it. This is a great way to spread the word.

Steve: So there's a lot of tension, and this is an example of what you're talking about, of the tension that exists between content providers and content consumers. And the conference that I attended yesterday spent a lot of time talking about the tension that exists in the privacy side of this. And...

Leo: Well, I have this - I am a kind of living example of this because we - this is a free product. And in return for this free product we sell you advertising. And the more we - if we know a little bit about you, we can sell more appropriate ads. We don't actually have to pry. But you're getting Facebook for free, and the trade is you give them some information.

Steve: Yes. And one of the things that - one of the speakers yesterday made the point about the phenomenal amount of value that targeting brings.

Leo: Sure.

Steve: Because, I mean, in the old mass mailing days, the rule of thumb was maybe a fraction of a percent of the people who received a mass mailing had an interest in it. So your effective cost was hundreds of times what it would be if you somehow had a way just to send something to the people who are actually interested. So...

Leo: And, not only that, you're getting bombarded with mail you couldn't care less about.

Steve: Yes.

Leo: It adds to your junk mail. So targeting is not just good for the advertiser, it can be very good for the consumer.

Steve: Yeah. And I would say overall the conference raised more questions than it answered. It was heartening to see a bunch of people gathered together, talking about this. I mean, there were people in the industry who were on the side of talking about solutions to the problems. There were companies who were looking for guidance, like what they should do from a policy standpoint.

And one of the points was made that was obvious to all of us, but it was good to hear it explicitly stated, was the degree to which mobile devices are a source for far more personal information than PCs ever were because the device itself knows much more about you. It's got your contact list. It's got - so much of your personal information is being stored on this device, more so than a PC, which traditionally has been more of a workstation where you did documents and web surfing and kept your - you weren't merging it with your phone. Well, now the phone has subsumed a lot of the functionality of the PC. So, and of course it also knows your location, which is additional information.

Now, the other thing that there was a lot of discussion about was this whole concept of reputation, which is one of the things we're beginning to see more and more. There was an acknowledgment that there's a lot of noise, that there's a fundamentally high signal-to-noise ratio, or a low signal-to-noise ratio, meaning that a lot of users try to find the signal amid the noise. And one of the reasons is, for example, that there's no notion of who it is, for example, who posts a blog comment. Anybody can post a blog comment. And they're all equally rated. So wouldn't it be nice if there was, like, some feedback system, some way for people to be authenticated, thus the identity side of this, and for people to carry a reputation around that they don't have control over because what a reputation really is, is information about you that other people have, rather than just being your own data.

So one of the other little tidbits that I thought was interesting was one person commented, and I jotted it down because I thought it was a little frightening, that data which the government cannot legally get without a warrant, it's able to purchase.

Leo: [Laughing]

Steve: So there are laws...

Leo: Because you gave it to some site.

Steve: Exactly. And it turns...

Leo: So it's legal to purchase it, even without a warrant.

Steve: It turns out...

Leo: Because you gave it up.

Steve: ...that the government is a huge customer of all of the data that we're trying to keep control over because it...

Leo: That's why the CIA investment arm put some money into Facebook. It's a good thing for government.

Steve: Precisely.

Leo: Yeah. Oh, man.

Steve: So I thought, whoa, there's a little takeaway.

Leo: That's really interesting. So it's legal for them to buy information without a warrant if you have made it available somewhere.

Steve: If it's available on the market.

Leo: If it's publically available. Wow.

Steve: If it's - yeah. And so aggregators are pulling this stuff together and selling it to Uncle Sam.

Leo: Sure. I know they go down to courthouses now, and they scan real estate

records. Those have always been public, if you went down to City Hall or the courthouse. But by scanning and putting them in a database, they're making public to everybody, anybody who has the buck 50.

Steve: There was an interesting story, actually, that came out yesterday. There's a company called Reputation.com that special...

Leo: Yeah, Reputation Defender, yeah.

Steve: That specializes in helping people. And back in 2009 someone came to them and asked for some help. He was in his mid-50s and had been unable to close the deal on getting a job. And he finally - and he, like, would go through interviews, and everything would seem fine, and then they would hire somebody else. Turns out, when you Googled him, the first link that came up was to a crime which this person had committed in his youth, that he had been convicted for and had served a year of hard time for. And so the question was, well, he wasn't getting the job because this information had been scanned in about him as records were being put on the Internet.

Leo: Exactly.

Steve: So this was back...

Leo: You used to have to go to the courthouse. Not anymore.

Steve: Right. And so this was online. And the guy who told the story said, you know, our justice system, this person, when he was young, made a mistake.

Leo: Paid his dues.

Steve: Paid his debt to society. But now - that was offline. How does he ever make up for that, now that this information is online?

Leo: It's something that I'm very aware of, and I know when I talk to kids they're very aware of. The problem is, with sites like this, is they can only do so much. And one of the things I tell kids today is you need to - the reason this worked is because this guy had nothing else on the Internet. If he had a blog, if he had other stuff...

Steve: The link would be pushed down.

Leo: It would have been pushed down. But because it was the only link about him, it was the No. 1 result. So I think really important as kids, I tell kids this all the time,

you need to - I hate to say this, but you need to start creating your reputation online now. If you did something great or made some great music or scored a touchdown, start a Tumblr log - it's cheap, it's free - and have it there with your name on it because the more stuff you put online now, the more likely that's the good stuff that will surface about you.

Steve: And there was actually some commentary about that yesterday. There was somebody who talked about going through a process of interviewing people. And what they said at some point of the process was, give us your Twitter handle, your Facebook ID, your LinkedIn ID, because they want to do research on you. And the point was that they were finding that they were better able to hire, that is, they were hiring people who turned out to be better than they would have hired if they didn't have access to that. That is, somebody who perhaps didn't interview that well, or didn't have an impressive rsum, but when they looked at who they actually were over time, they said, wow, look what this guy can do. Or, like, wow, he writes poetry. I want to get to know him a little bit better.

Leo: Right, right. So unfortunately, if you haven't been doing that, I guess these sites like Reputation.com are useful. But there's only so much you can do after the fact. I mean, I don't know about Reputation.com. What Reputation Defender does is they'll create a lot of sites with your name on it and recipes and things, just kind of random fake sites.

Steve: Oh, so they're spamming.

Leo: In effect they're spamming the Internet to try to bring your reputation up. Much better for you to start today and do it. And I think everybody who watches our show we don't have to worry about. But that's an important thing for kids as they're even in high school now, start making a reputation for yourself.

Steve: Well, and be conscious of the fact that a reputation is...

Leo: Everything you post...

Steve: ...online.

Leo: ...is going to be seen.

Steve: Yeah, and people do care about that.

Leo: Even stuff that you wish weren't online.

Steve: So two really interesting products. One is, like, top of the list. This was on my

radar. It's on my list of things to get to one of these days. And I had the really unique benefit of two of the main developers of this thing appearing and presenting. The product is called Disconnect. If you just Google the word "disconnect," it's the first link that comes up. The URL is Disconnect.me, as in, obviously, Disconnect Me.

Leo: Oh. Look at this.

Steve: Brian Kennish and Casey Oppenheim presented. Brian started at - I don't see it here in my notes, so I've thrown myself off the track. I'll just remember. He started at DoubleClick.

Leo: Oh, okay. So he certainly knows about this stuff.

Steve: He knows about privacy. Or lack of. Or information gathering. Then he was at Google and worked on Chrome development. And while doing that he was poking around at what Facebook was doing and was alarmed at how much - at, like, the amount of information about you that was going - that your browser was involved in passing between Facebook apps and your Facebook persona and the Internet. And so he first created something called Facebook Disconnect, which was a Chrome-only extension, and then broadened it to just Disconnect, which is now Chrome, Firefox, and Safari.

Leo: And free.

Steve: And free.

Leo: Love this.

Steve: I am very impressed. This thing disables third-party traffic.

Leo: Now, aren't we supposed to be able to do that anyway, just by checking that box in the preferences, say no third-party cookies?

Steve: Well, third-party tracking is different than third-party cookies.

Leo: Ah, okay.

Steve: So tracking is more pervasive than just cookies. So it disables third-party tracking, truly depersonalizes searches, shows blocked resources and cookies, lets you easily unblock services, and it's free. They have tried not to have it break things. Sometimes it may be a little too aggressive, in which case you can tell it to back off if there are things that don't work, a little bit like NoScript, that can be too aggressive. But anyway...

Leo: Is it mostly through cookies?

Steve: No, referrer headers, for example, and other headers. It'll sanitize the browser transactions in order to pull out any personally identifiable information and just things that, from taking a look at it, look questionable. So I haven't yet had a chance to play with it because, as I said, it was on my radar. These guys talked about it. It's Disconnect.me. And to me it looks like a win.

Leo: I just installed it.

Steve: So I'll know more about it next week, but I wanted to give all of our listeners a heads-up about it right now. And the second thing that...

Leo: How is it different from Ghostery? Strengths [ph] in our chatroom wants to know. Well, Ghostery lets you know what's going on.

Steve: Yes. Ghostery is a viewer only.

Leo: Right. That doesn't block anything, but this does.

Steve: Right. Ghostery shows you what tracking is going on. This thing actively works at blocking tracking.

Leo: It will show you, though, what it's blocked.

Steve: And it also does show you, yes. So you have visibility into it.

Leo: Right, right.

Steve: Yeah. Okay. So they're also involved in another project, which I think is really interesting. They call it the Privacy Icon Project. And after they got it up and going, they started talking to Mozilla. And Mozilla has gotten themselves involved in this. What they realized was - and it's the same guys. You can learn about this at Disconnect.me/db. The goal of the Privacy Icon Project is to convert all companies' inscrutable, un-understandable, fine print privacy policies into just four icons.

Leo: Oh, that would be nice.

Steve: They used to have five, but they managed to distill it down to four. And you can read about and see the icons. So the idea would be that this would be crowd sourced; that people would read companies' policies, figure out what they mean and which icons

they deserve, and then collectively put this into a database.

Leo: This is great. So your data may be used for purposes you did not intend. You data is used only for the intended use. Your data may be bartered or sold. Your data is never bartered or sold. Your data is given to advertisers. Your data is not given to advertisers. Your data may be given to law enforcement even when legal process is not followed. And then how long is your data kept for. Interesting.

Steve: So the idea would be that...

Leo: I like this.

Steve: And what Mozilla is looking at doing - because there would be a JSON API that would allow automated access to this database. So Mozilla would end up adding this to the UI of the browser. So when you go to a site...

Leo: Love it. Much easier.

Steve: ...the appropriate privacy notification icons appear. And after a while you would get to know what they meant.

Leo: Brilliant.

Steve: Just a fantastic idea.

Leo: Brilliant. Now we've got to get the people crowd sourcing it.

Steve: And what they found was, as they began to do this, there was true differentiation among sites. That is, I mean, Yahoo! was very different than Google in the way they handle user data and the whole privacy domain. So this is Disconnect.me/db for where this effort is at the moment.

Leo: And it's green if it's good, and it's yellow if it's bad. So, for instance, PayPal retains data indefinitely, may share with law enforcement without legal process, but your data is not shared with advertisers, bartered or sold, but it may be used for unintended purposes. So that's great. It's very clear. Love that. Love that.

Steve: Yeah, yeah. It's a nice step forward. Now, final little piece of something very tantalizing is called OneID. It's OneID.com, or you put OneID into Google, it's the first link that comes up. We got a presentation yesterday from Steve Kirsch, who is - he describes himself as a "serial entrepreneur." He was the money behind InfoSeek; FrameMaker back in the day.

Leo: Oh. Love FrameMaker.

Steve: I know. He says about every six years something comes along that motivates him.

Leo: What an interesting guy.

Steve: He is tackling the single sign-on problem. That is...

Leo: He won't be the first. I mean, Microsoft tried this with Passport.

Steve: And VeriSign with...

Leo: VeriSign, everybody.

Steve: ...VIP and SecurID and so forth. So it's why it's easy to be skeptical. It's easy also to get caught up in his enthusiasm because he does, he comes across as a high-energy, we can make this happen, we've got the money, we're going to do this guy. There's a video on his site which is only about a minute and a half, which is worth watching. It explains the concept. And what they've done is they have a website, and then the installation of a client on your system, which talks to a remote repository of identity, and then that talks to a device. And in his example he was using, for example, an iPhone. But there would be different clients for BlackBerries and iPads and so forth. And the idea being that, if you globally turn your access on, there's like a big - it looks sort of like Hal's eye on "2001: A Space Odyssey." It's got a big "ON" on it. If you turn that on, then you're able to log into sites with a single click.

Leo: I like that.

Steve: And you're able to specify...

Leo: So it's exchanging a token behind the scenes.

Steve: Well, it's exchanging a myriad of tokens. This thing's got arrows pointing in every direction, every which way. I mean, I drew the diagram, and he just gave a very quick overview of the way the thing works and what the process is. I mean, he's going to - if you go to OneID.com, you can register to be notified when you're able to register nicknames. And if this thing takes off and succeeds, you're probably going to want to have a cool nickname. So it's like, don't we wish we'd gotten into Twitter from, like...

Leo: I'm going there right now. I'm going to get my nickname, yeah, yeah.

Steve: Exactly. So it's supposed to be in beta early next year, I think March is what I remember, and pre-beta or alpha, like, next month. So this is not years away. He did show an impressive slide of all the different organizations that he has interested in this so far. And so we'll see. I mean, there's a little bit of a chicken-and-egg problem.

Leo: Yeah, because you'd have to have Amazon or whoever participate; right?

Steve: Yes. You'd have to have enough people involved that it was worthwhile for you. And I raised my hand, and my question was, okay, what are the economics? Like, why are you doing this? Who pays? And the answer was, it's free for you, and it's free for them.

Leo: So who pays?

Steve: Until you are using it so much that it is clearly beneficial. And then some sort of a micropayment or a charge a buck a month thing, something kicks in. And he wasn't clear. And other people said, well, what about if I lose my iPhone, blah blah blah? And he said, yes, we know, we know. There's, like, 50 different scenarios for bad stuff that can happen, and we've got it all taken care of. So it's like...

Leo: Yeah, it's interesting.

Steve: ...well, I hope, you know, we can cross our fingers.

Leo: There have been a lot of people trying this and failed.

Steve: It's been tried before. So I just wanted to give our listeners a heads-up, on the chance that this is the one that works. And it has...

Leo: I get some of these benefits from LastPass.

Steve: Yes.

Leo: But not all.

Steve: Some from LastPass, some from SecurID, some from VeriSign's VIP. But not all. And he makes the point, he is able to attack every one of those as what's wrong with these solutions.

Leo: Why people don't use them or whatever.

Steve: Well, exactly, that this doesn't have. So the idea would be that you're able to globally enable or globally disable this system. So if you know you're not logging into anything, you press Hal's big red eye, and it just shuts the entire network down so nobody anywhere...

Leo: I like this.

Steve: ...is able to log in as you.

Leo: I like this.

Steve: And you're able to also, with granularity, say certain sites need, like, second-factor authentication. So, for example, a banking site could say we want to support OneID, but we want to require on-the-fly verification that it's you. So when you try to use OneID to log into the banking site, it will send a prompt to your phone that requires you to acknowledge it on the fly, type in a PIN, or respond to something that you saw on the website in your phone to confirm that you've got multifactor authentication.

Leo: I'm liking this. I'd love to see this work.

Steve: There's a lot of benefits to it.

Leo: You know what's changed is that we all have smartphones - or not all, but many of us have smartphones now. That was something that didn't happen...

Steve: It was a gating factor. And so there's a zero cost aspect to it because it's a matter of...

Leo: Right, you don't need a token.

Steve: Right.

Leo: Steve, it's so nice to have you here. Would you just come up every week and do the show?

Steve: Yeah.

Leo: Normally Steve's down in Irvine. You can catch him at the Starbucks there by UC Irvine, reading his Kindle.

Steve: Having my 12 shots.

Leo: Wearing his little cap, drinking a big tall latte. And of course he joins us here every Wednesday at 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1900 UTC. So you can tune in, watch the show, learn about security, learn about privacy, keep yourself up to date on everything that's going on and a few little side things like Kindles and sci-fi.

Steve: I'll have a review of...

Leo: I'll be very curious what you think of this.

Steve: I'll have my opinion for our listeners next week. I won't drag everyone through a...

Leo: Doesn't it feel good, though, in the case? It's a little heavy, but it feels solid.

Steve: Yeah, I like it.

Leo: Feels like a book.

Steve: And I'll just remind people that the first Kindle was an ugly duckling, too, and they fixed it. And so if they could, I mean, remember, this thing has so much potential...

Leo: I'm taking it back.

Steve: Oh, he wants it back. Well, mine's at home, so...

Leo: Okay, you can play with it.

Steve: That's all right. I'll have it in a few hours.

Leo: It does have a lot of potential. And with Amazon behind it...

Steve: I wouldn't rule that out.

Leo: Wouldn't bet against them, yeah.

Steve: I wouldn't bet against them, no. And so I'll talk about that briefly. And I'll have some more information about Disconnect.me, or Disconnect next week. I wanted to give our listeners a quick heads-up. And I'll be following OneID because, as we said, we're

going to want to be part of the one that works, and it might be this one.

Leo: Yeah. We will, of course, answer questions, too, next week.

Steve: Yes.

Leo: It's a Q&A. So if you have a question for Steve, go to his website, GRC.com/feedback. There's a form there. Not email, that's the way. So GRC.com/feedback. You'll go through the most commonly asked questions, answer them all next week on our next episode, 328. You can also find SpinRite there, the world's best hard drive and maintenance utility.

Steve: Yay.

Leo: Sis boom bah. You'll also find lots of freebies and information about Password Haystacks (better passwords through padding), his Perfect Paper Passwords, and a whole lot more.

Steve: Oh, Off The Grid is all finished.

Leo: Is Off The Grid done?

Steve: I haven't put the link, I haven't made the grid, I haven't made the pages public. I'm still working on the documentation. But all the technology is nailed down. Anyone who wants to begin playing with it, the grid printing technology is all there and finished.

Leo: It's like having - you're like our Xerox PARC. You're our little research R&D lab. And he's got his hands in a lot of different things. He's always doing something interesting, and we get the benefit of it. So it's all there at GRC.com, including 16Kb versions of this show for those who want the smallest possible version; transcripts, as well, if you like to read along. I guess that's an even smaller version, really. It's just text. We have the audio and video on our site, TWiT.tv. Thanks for joining us, and we'll see you next time on Security Now!.

Steve: Thanks, Leo.

Leo: Thanks, Steve.