Listener Feedback Q&A #40

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-142.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-142-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 142 for May 1st, 2008: Listener Feedback #40. 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!, and we're going to talk about technology and security and protecting yourself online with Mr. Steve Gibson. He is the man who discovered spyware, coined the term, wrote the first antispyware program. He's been writing free security utilities ever since, including ShieldsUP! and Shoot The Messenger, DCOMbobulator, all at GRC.com. He's also the guy behind SpinRite, which is the ultimate disk recovery and maintenance utility. Hey, Steve.

Steve Gibson: Hey, Leo.

Leo: It's May, it's May.

Steve: Nice to be back with you again.

Leo: The lusty month of May.

Steve: We have, yeah, May Day today.

Leo: Yeah. Now, this is - Mayday is, of course, in French it means "help me."

Steve: Do the kids in elementary school still, like, get crepe paper streamers and do the Maypole dance and...

Leo: Funny you should say that. We talked about that this morning on the Giz Wiz. I remember that from school.

Steve: Yeah. Unfortunately I do, too.

Leo: And they'd go over, under, over, under, so they'd braid.

Steve: Exactly. And you end up with this, yeah, exactly, like a streamer braided pole that's really cool.

Leo: Called the Maypole. But yeah, I don't - I doubt anybody does that anymore.

Steve: Okay.

Leo: We're antiquarians. So we've got a Q&A for you today, some great listener questions. We love it that you submit your questions. It gives - what's nice about it is it's still Security Now! in the sense that we still - Steve still talks about security. But it's stuff in response to your concerns and interests.

Steve: Yeah, the way I think of it is things that are, as you said, interactive and responsive, but also topics that really don't necessarily need their entire show. But we can do it in a piece of a show, so it makes sense. And we've got some fun things at the end of this, as well, as I always try to find some neat, wacky things.

Leo: Oh, let me see. I'm going to jump ahead.

Steve: There's even a bonus 13th one. It's very short. I called it the "Quip of the Week." I just got a kick out of it.

Leo: Quip of the Week, okay. Good, good, good. And some sobering truth and terrific observations and questions and answers. Steve Gibson, do we have any errata or anything you want to cover?

Steve: Oh, we got tons.

Leo: Oh, boy. And security news, too, I'm sure.

Steve: Well, that's in there, too. Yeah, I sort of call it all sort of like pre-Q&A stuff.

Leo: Right, right.

Steve: Many listeners have been writing in to - GRC.com/feedback is the page on the GRC site for Security Now! listeners to send me their thoughts and ideas and questions and show ideas and so forth. Many have been asking about a new gizmo called the Yoggie Pico, Y-o-g-g-i-e P-i-c-o, as in very, very tiny. It's a USB system, I mean a full Linux PC running a small Intel chip in a USB dongle.

Leo: Cool.

Steve: And it purports to be a security system. So you plug it in, it installs a low-level NDIS driver, which is down deep in the kernel, that allows it to intercept all incoming and outgoing traffic. Essentially it puts a Linux system in a USB dongle inline to your network connection. So I just wanted to acknowledge all the requests from people about, gee, Steve, what do you think about that? I mean, the idea sounds great. I've noted it, and we will give it a show after I've had a chance to thoroughly scope it out and see how it works and if I see any problems with it.

Leo: I mean, that's a neat idea. I don't know about security-wise, but just the idea that you could run that Linux on a USB key is very cool.

Steve: Definitely neat idea. Also out in the world, unfortunately, as many as half a million IIS, that is, Microsoft's web server-based sites - you've probably heard this, Leo, already - have been hacked.

Leo: Including - this is the punch line - the Department of Homeland Security.

Steve: Yes, yes, and the U.N., and U.K. government. The attack on Barack Obama's site was different than that. They used some cross-site scripting to make some changes to Barack's campaign site.

Leo: You clicked a link, and it'd send you to Hillary's page. But this one is a SQL injection; right?

Steve: Yes. This is, yeah, and we've talked about that before. It's an SQL injection. It uses - it's really not Microsoft's fault. It is the fault of the web coders for not sanitizing the input. It's Web 2.0 fundamentally is more interactive. That's the whole idea, the

notion of, like, posting comments to blogs and all of the Facebook/MySpace stuff where users are able to supply content. But the problem is this content is typically being stored in an SQL, a.k.a. sequel, database. And that's just sort of like the default database. That's not what I use, but that's what everybody else uses.

And so what happens is because - and as we discussed in our SQL injection attack episode, if anyone's curious they can certainly go back and relisten to it, or maybe listen to it for the first time. The idea is SQL is a language, so it's possible to inject language commands and essentially install malicious content on a website. In this case they're installing JavaScript, which then is downloaded into innocent users' browsers, as JavaScript is. But in this case it's not JavaScript the website provider wants you to run, it's JavaScript that's been injected remotely into the website. So then it's downloaded into the innocent user's browser, runs. That installs malware and takes them to a Chinese server, that is, an IP address in China, which then attempts to use known Windows vulnerabilities to further compromise their system.

So it's just bad all the way around. And the only thing you can do is disable JavaScript, or selectively enable JavaScript. I know lots of people have followed the discussion, we've talked about the NoScript add-on for Firefox. And of course, although it's not as easy to use, it's possible to configure Internet Explorer so that it's not scripted by default, and then you selectively enable scripting on those sites where you trust them and/or they need to have scripting in order to be functional.

So, I mean, one of the things we're seeing, and I heard a lot about this of course at the RSA conference earlier this month, is we're seeing a huge move toward web-based attacks because this is so-called "low-hanging fruit." I mean, there are so many vulnerable websites, so many web apps are being written without an eye toward security, that just creates, I mean, it's like a public server sitting there where anyone who knows the tricks is able to install their malware remotely. And then anyone visiting that site gets infected. So it's like it's the next big problem. And of course we've been talking about this kind of thing more from a theoretical standpoint, like this was going to be a big problem. Well, it's arrived to the point where hundreds of thousands of websites are now infected with this junk. So...

Leo: Something to point out, of course, is that even if they're infected doesn't mean the payload happens. In fact, the guys who did the research said, you know, a lot of cases nothing happens when you go to these sites. Also the servers that they point to are currently down, whether because it's so successful or more likely because they've been shut down. And that's the problem from the hackers' point of view is these exploits are only good for a brief period of time. Once they're discovered, the SQL injection still works and the code's still on the site; but it doesn't do anything because the sites that it points to are down.

Steve: Right, exactly.

Leo: So I think it's right now not a problem. I also, by the way, I just saw - because we've talked back and forth about disabling JavaScript. Just saw a study of the hundred top sites. 80 percent of them use JavaScript. It's almost universal.

Steve: Yup, and it's going to be more so. I mean, it does power the next generation of the web. So, I mean, and it's a mixed blessing unfortunately because, as we've said

many times, you're downloading some web server's code into your browser and running it locally.

Leo: The nice thing about your technique is you can selectively enable it. So once you trust a site, you enable it. The problem is the SQL injection attacks often infect trusted sites. So you could trust a site today...

Steve: Yeah, very good, that's a very good point.

Leo: You would trust the Department of Homeland Security, one would think. But in fact it has the exploit on it.

Steve: Although I guess by disabling scripting by default and then selectively enabling it, if nothing else you are dramatically lowering your attack window. That is, in general, I will follow links in news reports, and you end up wandering off of your well-trodden path all the time when you're out poking around the 'Net. It's just sort of the nature of it. I mean, it's why it's so cool is all that stuff is out there. So unfortunately it's not always safe.

Leo: One would hope that at a site like DHS, in fact they said this, you know, now that we know that that bug exists, we've fixed it. So one would hope that they would become more secure. So a trusted site would be somewhat safer. One would hope.

Steve: Yeah. An old problem has resurfaced. There have been problems with Intel Centrino drivers. Centrino is Intel's laptop WiFi platform. An old, well-known privilege elevation problem has turned into, it's evolved into a remote code execution problem. I bring it up because I just want to make sure that our listeners who are using the Centrino - it's the 2200BG is the affected device driver. There's, like, four different varieties. There's 3459 or something, and a couple others. I checked one of my laptops, and that's the one that I had. I had the 4559 or something. But it's the 2200BG has a known problem.

The reason this is a concern is that it is - the way this works is you - first of all, there's no way to block it. No firewall will prevent this from being a problem because it's an exploit, well, it's a vulnerability in the kernel driver, in the actual WiFi driver which is underneath every other sort of security defense the user can have. So the way an attack would work is that some wiseguy who thought it was fun to do this would have a laptop at Starbucks, for example, and anyone whose laptop had not been patched to the current version of this driver could have malware installed even if they're not, like, hooked up to Starbucks' wireless. You don't need to be even connected to the network, just the idea, I mean, just having your wireless adapter live allows it to receive these malicious frames down at the low level and get code installed.

So the only show notes I had for this week are a bunch of links for this problem to Intel's site. There is one that allows you to run a little app of theirs that identifies the device driver type and version. You need to have at least version 10.5 of this 2200BG wireless device driver. If you know how to poke around in Windows and bring up the driver information for your WiFi, you can just do that. I did that on my laptop. That's how I know what model and version I had. In my case it was at version 11.something or other

on a different wireless device driver.

So I just wanted to mention it to our listeners. It's not a huge big deal. But nobody would like to be somewhere in public and get code installed on their machine. And this is sort of a problem because these device drivers not being mainstream Microsoft problems may be old. It may not be that anything has updated them for some time. So users who have this Centrino 2200BG should make sure they're at version 10.5 or later. And I've got links on this episode's show notes, notes-142, that you can find at GRC. And I imagine that, Leo, Dane will probably copy those also over to your page. So that's a good thing.

Bruce Schneier, the well-known cryptographer that we've talked about and mentioned many times - and I'm annoyed that I didn't get a chance to say hi to him at the show. He was on one of the tracks, but he was on a different one than I was. And so I missed being able to shake his hand and hang out with him and say hi. But I loved something that he wrote. He blogged about the conference. And what he wrote so much echoed sort of what I said last week about some of these booths. He said - I'm just going to quote one paragraph in his blog. He said, "The booths are filled with broad product claims, meaningless security platitudes, and unintelligible marketing literature. You could walk into a booth, listen to a five-minute sales pitch by a marketing type, and still not know what the company does. Even seasoned security professionals are confused."

Leo: I saw that. I thought that was great.

Steve: Yeah, that was exactly the sense I had. That's why I said they all sort of seemed to be the same because they were all saying oh, fantastic new security solution for authentication identity. And then you go to the next booth.

Leo: Fantastic new security...

Steve: Exactly.

Leo: Yeah, yeah.

Steve: Also, after last week's episode, our intrepid transcriptionist Elaine shot me a little note. Remember we were talking about sci-fi and "Andromeda Strain," I think. I don't remember now what the context was. But she said hey, Steve, this coming weekend...

Leo: Oh, we were talking about Michael Crichton, a book...

Steve: Oh, that's right, Michael Crichton books and how good "Andromeda Strain" was, where we weren't that impressed with some of the more recent ones. She said that this coming Memorial Day Weekend, so about three weeks from now, A&E cable channel are airing a new miniseries of a remade "Andromeda Strain" that was done by Ridley Scott.

Leo: Oh, I want to see that.

Steve: Oh, baby, the guy who gave us the first "Alien" movie. Anyway, there's a trailer around. I tracked it down and saw it. It's funny because I thought, oh, wow, I wonder if my newsgroups know about that, because I created - we have a grc.scifi newsgroup at GRC just because I love sci-fi so much. And it turns out many of the people who hang out on our news server do also. Way back weeks ago there was a thread all about this. So it's like they already knew about this. I've got to keep more current with my own sci-fi newsgroup. Because I would absolutely not want to miss this. It will be on DVD. It's being released in June, I think, on DVD. But oh, Leo, the trailer, oh. I mean, it looks like it's everything you could want in a contemporary remade version. Because the original one was, what, back in '75, I think. I mean, so it was - it's dated even though it's a really good story. Well, now we've got state-of-the-art special effects and cool, I mean, just like way much better. So I wanted to let all of our sci-fi-interested listeners know that we've got a new version of "Andromeda Strain" on the way.

Leo: That will be worth seeing.

Steve: A little miniseries. And I did have one really cool, neat, fun bit of SpinRite feedback. This one was titled "Skeptic Is Finally a Believer." A listener, Ralph Montgomery, wrote. He said, "Steve, I've been an avid fan for years, both of your excellent program SpinRite, and now in the podcasts of Security Now!. Working in the information technology field for the past 21 years, I have used SpinRite on everything from MFM and RLL drives to today's EIDE/SATA drives with great success. With these successes I took every opportunity to evangelize the product to friends and coworkers everywhere. One particular coworker has listened to my praise for years with, 'Yeah, yeah, sure it works.' I eventually convinced him to purchase his own copy of SpinRite a few months ago, which he used sparingly to check new drives after purchase.

"This past weekend, however, a friend of his referred a young lady to him with a nonbooting laptop, a laptop this recent college graduate had taken to all her professors and several other friends with no success. She had a recent job's data which she had not backed up yet (she's a web designer) that she desperately needed for her client. My skeptic coworker tried everything he could think of to get the system to boot, even removing the drive and attaching it to an external USB cable, and still could not access the drive and data. Finally he pulled his copy of SpinRite bootable CD-ROM, booted the system, and watched it work for about 15 minutes on the first couple of sectors, recovering data, then scream through the rest of the drive finding nothing else wrong. After completing the SpinRite cycle he powered the laptop off, restarted without the CD-ROM, and voila, a booting laptop with all the data intact. A quick transfer to a new laptop, and his friend was very happy. And you now have a convert."

Leo: Wow, that's great.

Steve: And then he says, "Great job (but I knew that already)." So thank you for sharing that, Ralph. I really appreciate it.

Leo: What a nice story, yeah. That's really cool. Shall we launch right into our questions? Are you ready? You feel good?

Steve: Oh, I'm ready to go. I feel good.

Leo: Face the music? Start with Jon in Adamstown, PA. He wonders if Vista's User Access Control, UAC, is worth anything. Hi, Steve. I think it's User Account Control, I'm sorry. I always call it User Access Control. Slashdot recently carried an article describing how simple it was to bypass Windows Vista's much-annoying User Account Control (UAC) system. The authors of a utility were annoyed by UAC, so they easily coded around it. If this is true, is there really any security benefit? They claim there isn't. Can you let me know what you think of this? Certainly I think it's good if UAC prompts before install; but if what the author says is true, it seems pointless to prompt on startup. So I guess they're saying not a utility merely to disable it, but a utility that lets you go right around it.

Steve: Yeah. This actually came up, or came to my attention, I guess, I don't know, a few days ago when Slashdot first had the article. A bunch of people said hey, you know, what's the story? Is UAC worthless? And it's like, has it been circumvented? It's like oh, no, now what? So I went off and did the research, figured out what was going on. And the good news is this is nothing. So I wanted anyone else who had seen this on Slashdot, because it got a lot of coverage, to know that this is sort of a bogus report.

The deal is there was some sort of a utility which required admin privileges at startup. Well, when you try to run a utility that requires admin privileges, UAC gets in your face and says do you want this to allow it to happen. The problem is - and this is some sort of like a reboot utility that allows you to do multibooting or something, I didn't even really look too closely at what it does, because they wanted it to run in the startup group. So if you put it in startup, every time you boot it's going to run, and so it's always going to prompt for UAC permissions. So they decided that was an annoyance. So they recoded it so it no longer does that. And that's what was upsetting people.

Well, okay. What they recoded it to do is they split it into two parts. There's a service which you have to be an admin and do UAC to install. And then there's the client that talks to the service. Well, this is the way Windows works. And so this is not - this didn't circumvent UAC or get it out of the way or mean that it's worthless because in order to install this privileged service you have to use UAC to get permission to install it. Now, it's true you're not having to give permission every single time you use it. But, I mean, you couldn't use Windows if you had to give Windows permission every single time any service did anything. So this is just the way Windows works. You install something that you're giving privilege to, like a firewall, for example. And then afterwards it's god because it's down in the kernel doing whatever it wants to. So you're trusting it from then on and not having to deal with it every single time it runs. So this is just UAC the way it was meant to be used, not a circumvention of anything.

Leo: Got it. So don't get your hopes up, hackers. Jesse in Honolulu, Hawaii wants to know more about the YubiKey. This was that thing we talked about the Swedish lady from RSA; right?

Steve: Yup.

Leo: Aloha, Steve and Leo. When I heard the story of Stina and the YubiKey, I immediately went online to do my homework because the thought of a $4 authentication token was too good to pass up. Well, I read a little more; I'm not as

excited. YubiKey's ordering page has two products available: a single key you have to agree to use for evaluation purposes only, and the "pilot box" which comes with 50 keys. A small business would never go through that many keys, but it doesn't look like Yubico offers any smaller packages. It even costs 4 euros more per key when you buy them in bulk. More. My other concern with YubiKey is how they're locked into Yubico's web service. Sure you can purchase the low-level C or Java SDK, but for how much? I took a look at the open source APIs. They all seem to rely on the subscription-only YubiKey web service. The YubiKeys only come with a one-year subscription, according to the site. Am I missing something obvious? YubiKey does sound like a good alternative to SecurIDs, but not the holy grail. Do you know otherwise? And by the way, thanks for Security Now!.

Steve: Well, okay. First of all, there's been a lot of interest in the YubiKey surfaced by our users. I wrote to Stina, and we set up a little - we've got a little dialogue going. She reported, I mean, she was really happy with my mention of it last week. More than 50 users and companies who listened to Security Now! have contacted them via email.

Leo: Wow. Wow.

Steve: So it's been very good for her. And many people also in the Security Now! newsgroup at GRC - I do have a Security Now! newsgroup in addition to a sci-fi newsgroup at GRC. And they had a bunch of really good questions because it's sort of unclear from the website exactly how this works. So I said to her, gee, you know, a lot of really good questions are being asked. I don't have the answers. I'd like to find out. So she has sent me one of the patents that they've applied for, an in-depth security analysis, an independent security analysis of how this thing all works. I'm going to figure it out and probably do an episode to explain what this is and how it works because it's got a lot of interesting characteristics.

So I sort of wanted to acknowledge Jesse's frustration. And the sense is that this is still just beginning to happen. Stina said - I asked her, like, for all the developer documentation. She said, well, we're still working on getting the server documentation done and putting it all together. So this is a relatively new thing. Ultimately I'm hoping that it'll be available in a way that makes sense affordably. And I don't have any firm pricing on things like the subscription where you use the back-end service and all that. I certainly like the idea of being independent of that, in which case there's no one-year expiration on the key.

Leo: Well, and yes, you're dependent on it. Besides the fact that you have to subscribe to that, if their server went down, you're kind of out of luck.

Steve: Well, it's funny because I got a notice from VeriSign the other day to, like, major accounts, saying that for four hours their VIP system was going to be done for, I mean, like, major maintenance and cleaning out and upgrading and all that. The problem is, imagine if you were dependent on that for authenticating something in mission critical, I mean, during those four hours you need to do something that requires authentication. I mean, that's really...

Leo: You can't even...

[Talking simultaneously]

Steve: No, that's not okay. So, I mean, it is the case that, well, and I know for example that Hamachi users similarly - Hamachi had to be in the loop. Anytime the Hamachi servers were down, the whole Hamachi - you could maintain your existing Hamachi connections, but you couldn't initiate any during that window. And it caused people huge pain because they were in love with Hamachi, and suddenly nothing worked that they needed to have work. So these sorts of things, I mean, it's one of the reasons for my own, you know, I've talked about CryptoLink, the VPN that I will be working on as soon as I get the current project finished, that it's going to have a full, not only TNO, meaning Trust No One, but RNO, Rely on No One. So that it'll do its job without needing any sort of a third party because it's just - you can't have that with reliability.

Leo: Right, right. Yeah. Of course you running your own server could be unreliable. But at least it's your own damn fault.

Steve: Well, yes. And if in fact you're trying to connect to your own server, if it's down, well, you can't connect to it anyway.

Leo: Right. Well, that's a good point. Now, would that be a security flaw, to have your authentication running on the same server as the thing you're authenticating?

Steve: No.

Leo: No. Just thought it might. Nick Bauer in Newmarket, New Hampshire wonders about Killing Bits: Hi, Steve. I noticed this patch to Windows come down the pipe last Update Tuesday, and I wondered what it is. Sounds like it might be a DEP for ActiveX. Are ActiveX controls now a lot safer? This guy must be a cowboy. He's very terse. So what's this patch to Windows come down the pipes last Update Tuesday?

Steve: I saw that, too, and I was wondering what it was because they were talking about a kill bits...

Leo: Oh, that's what it's called, kill bits?

Steve: ...update. It's called kill bits. This is a feature which, you know, thank goodness it's in Windows. As we know, Internet Explorer is able to load ActiveX controls. That's, for example, what Flash is. Flash is an ActiveX control that is able to embed itself into Internet Explorer web pages. And, you know, there are some utilities - I actually have one sitting here on my taskbar, I'm looking at it - which is able to disable Flash on the fly because sometimes Flash is a little more Flash than you want, when you're just trying to look at a web page and little bunnies are jumping all over the place or whatever it's doing. These things do everything they can to get your attention, when in fact it's like,

okay, fine, can I just look at the content please.

Anyway, what this thing does is this manipulates Flash's kill bit. Every ActiveX control has a kill bit which the user can flip. And what it does is it denies IE permission to load that ActiveX control. And in the past, and this is like a couple years ago I'm remembering from Security Now! episodes, there have been really, really bad exploits where Microsoft had no patch. And so our advice was, and we gave people links and...

Leo: Oh, yeah...

Steve: ...go into the registry...

Leo: Kill bit, yeah, I remember that.

Steve: ...here's the key, and set the kill bit because that way it'll turn it off until Microsoft gets it patched, then maybe you want to turn it back on, if for any reason you need the hairy eyeball ActiveX control. I mean, some of these things are not anything anybody wants. And so it's like - and in fact you can even turn them off without your system having them. You can turn them off preemptively. Then if it comes in or installs or reinstalls, the kill bit stays set, and IE is unable to run this thing. So what happened is that a third party asked Microsoft to please set the kill bit for them.

Leo: Oh, interesting.

Steve: And that was Yahoo!. The Yahoo!, shoot, I had it in my head just a second ago, now it's gone. The Yahoo! something or other.

Leo: Messenger?

Steve: No, it wasn't Messenger, is was - can't remember now. It was something we talked about actually in the last couple weeks. It was a known exploit in a Yahoo! ActiveX control. The problem is they don't have the facility to notify and download updates on the fly. So this is a widely exploited problem, and they asked Microsoft please set our kill bit for this thing for us.

Leo: Can you believe that.

Steve: So that's what that was. It's not an improvement in ActiveX controls, however much we wish there could be such a thing. It's just it's Microsoft doing Yahoo! a favor.

Leo: Maybe - I wonder if that's part of their courtship. It's a little test.

Steve: Yeah, we'll see how that works out.

Leo: Yes, dear. Will you turn on the kill bit for me, dear? Yes, dear.

Steve: The Hatfields and McCoys at the moment.

Leo: Yeah, well, they're not getting along too well together. But they did the kill bit, which was nice of them.

Steve: Yes.

Leo: All right. Amir Katz in Kfar Saba, Israel, figured out how to grab all the SN episodes. Actually somebody Twittered me a shell one-liner for it. But I'll see what Amir came up with. In Episode 140 you looked for different ways to enable your listeners to download many, or all, SN episodes. You did not have a good solution, in my opinion. There's a very simple way. Since GRC.com/securitynow page has all episodes, you could use Firefox with the Download Them All extension - oh, yeah, that'll work - and download all links of certain types, including the - using the DTA filters. It doesn't have a predefined filter for PDF files, so I created one. And then with a few clicks you start a download of all PDF files from the page. Of course we don't want the PDFs, we want the MP3s. But if you want the PDFs you could do that. Regards, long-time SN listener and proud owner of SpinRite. Thank you, Amir.

Steve: So I just wanted to pass that tip on.

Leo: You could also use CURL and a little regular expression parsing and create a one-liner that would download any of the TWiT podcasts because we use kind of a regular format for the names for this very reason. So Security Now! is always SN-0 - well, not necessarily zero, could be number number number. Could be in this case 142. But I don't know what's going to happen when we get to a thousand episodes. We'll have to add a zero. The whole thing's going to break down. But right now you could write a little - you know, it's funny, I'll put this in the show notes because somebody Twittered it. It's short enough that they were able to send it in 140 characters to me using CURL, a little probably SED or something like that to parse it out, maybe AWK, I don't know, to create this kind of repeating - and which is a little shell script and would get them all. For any of them. All you have to do is provide the base URL, and you can get them all. It's kind of clever.

Steve: It's funny, you were talking about what happens when we go to 999. I'm reminded that I think it's in 2032 or 2036 or something, the 32-bit seconds counter in the NTP, the Network Time Protocol, wraps to zero.

Leo: Really.

Steve: Yes. And that's going to be a problem. We survived Y2K, but...

Leo: When's that going to be?

Steve: It's like in 2032, I think, it's 2030 something. And I've sort of kept my eye on that, it's like oh, goodness.

Leo: Well, you know what's interesting, UNIX runs out in 2038 because UNIX uses - the start date is 1970.

Steve: Well, that's what I'm talking about, Leo. That's the date.

Leo: Oh, you're talking about the UNIX. But NTP - oh, because NTP is running UNIX.

Steve: It's 32 bits of seconds. 32 bits of seconds starting on January 1st, 1970...

Leo: Oh, okay, yeah. It's not just NTP, dude, it's everything.

Steve: That's what I'm saying, I think it's bad.

Leo: It's not just the time servers, it's everything. Yeah, because, well, I mean, I presume by then somebody will have had a 64-bit UNIX. I don't know.

Steve: Yeah, we'll see how that goes.

Leo: They'll have to rewrite it, I guess, because a lot of, I mean, wow.

Steve: I don't know how we're going to contact each other.

Leo: 2038, will we still be around? I think we'll be up in heaven looking down.

Steve: I hope so. But wait a minute. 2038? 30 years from now I'm going to be kicking. I'm going to be going strong.

Leo: You probably will. I'll be looking down on you saying, "It's Steve's problem now."

Steve: And we will have dealt with the 999 podcast number by that time, too.

Leo: Yeah, that's another question. Okay, so that means we have another 860 to go.

[Muttering]

Leo: If we're still doing this in 860 shows...

Steve: If we still have any listeners left...

Leo: Oh, my goodness. That's more than 10 years. So, good, all right. My plan is to do this for 10 years.

Steve: Okay.

Leo: That's probably what I was thinking. Although, you know, with TWiT I gave it four zeroes. I thought TWiT would last longer, I guess. Not so. Joe Rodricks, listening in Massachusetts, has been clicking on a keyboard.

Steve: I think it's the Giz Wiz you need to give about nine...

Leo: I know, that one needs more. It only has 999. You're right, it's going to run out next year or the year after.

Steve and Leo, I came across a new log-in method I thought I'd share. Oh, another one. This one's from an ING Direct account which I opened. Well, the Dutch do it right. Let's see what they've come up with. When you log on, it first asks for your ID. Then it prompts for two security questions. Then it asks for a PIN. It's this PIN that's interesting. Your PIN is a 40 - I'm sorry, it's a 4 to 10-character numeric password. However, you never type it. On the log-in screen there's an image of a keypad which you click your PIN based on its numbers, or you can type your PIN's code. The keypad has a layout just like a telephone, three rows of three numbers, the zero's on its own row at the bottom. On each number there's a single letter. The letter assigned to each number changes with each log-in attempt. Oh, that's clever. It's probably a Flash or something, too. So if my PIN is 12345, I would look at each number and type the corresponding letters, which may be QOSPX for this log-in, then next log-in could be SLCUG, and on and on and on, each time you log in a different set of numbers. Or letters. I think this is an awesome idea, just totally fool a keystroke logger. I won't access my ING Direct account very often, perhaps just weekly, so I don't find the security questions that bothersome considering the extra layer of authentication they provide. I may not have explained this well, but I think it's worth creating an ING account just to see. It seems to be a pretty simple solution that would fool all but the most sophisticated keystroke loggers. Love the show, keep up the good work. What do you think?

Steve: Well, I think it's a really interesting and neat idea. Essentially what he's described is he's got a fixed PIN which is not changing. And what it's presenting him with is a

translation table which changes every time. So on the screen is a translation table. And he looks up his PIN by number, but he types on the keyboard the letters, the alphanumeric, I mean the alphabetic letters corresponding to the numbers. And so they change every time. And so it's clever. The problem is, and there was a discussion of this at RSA a couple weeks ago, is that keystroke loggers really are absolutely doing screen captures now. And so...

Leo: So they would see the keys. But it's a one-time deal; right?

Steve: Exactly. The problem is it's reversible. They would capture the screen and see the mapping table. And then, knowing what was typed in alphabetically, looking at the mapping table, they'd go backwards through it and get the numbers out. And the numbers are what never changes. And at that point they would be able to log in...

Leo: They'd know. They only need to get it once, in other words. Of course.

Steve: Exactly. Exactly. So it's a nice idea. But, I mean, unfortunately - I mean, it would take a sophisticated keystroke logger. But unfortunately, sophisticated keystroke logger is now an oxymoron because...

Leo: They all are.

Steve: They really are getting very sophisticated.

Leo: It's actually the opposite of an oxymoron. I don't know what that is, though. A noxy...

Steve: OxyContin.

Leo: Noxymoron. Ryan Benz in nearby Irvine - hey Steve, he says, he's waving as he drives by - wonders about cell phone authentication. Hi, Steve and Leo. In the last episode of Security Now! you mentioned that Bank of America now allows its online banking users to add an additional factor of security for their log-in process through the use of a one-time code sent via cell phone text messages. I've been using that. I love that. I love that. It seems as though this mode of security is becoming more and more prevalent, but I'm curious about the security of sending cell phone text messages. I remember Steve saying he doesn't discuss sensitive issues with his attorney on his cell phone. Are cell phone text messages any more trusted and secure? Is it possible for others to sniff this traffic? Thanks for the great podcast. Listener since numero uno.

Steve: Well, it is a great authentication solution. I should clarify that when I was talking about not discussing sensitive issues with my attorney on the cell phone I was specifically referring to the old original era of analog cell phones because they were literally just open analog radios, and any police scanner or radio scanner could pick them

up and listen. You could listen to typically one side of the conversation, and some of them were quite fascinating. And I decided I didn't want to be part of adding to the fascination of anyone listening to me talking to my attorney. So today's cell phones are digital. And on my list of things we will get to is a discussion of the cryptography used, and unfortunately its relative lack of strength, meaning that both systems, both CDMA and GPS - GPS? GPM. GPRS.

Leo: I don't know where you're going. GSM, is that what you're trying to say?

Steve: GSM, that sounds right. I'm thinking, wait a minute.

Leo: We're in acronym hell here.

Steve: CDMA and GSM both have been cracked, that is to say it is possible, by somebody who really, really, really wants to, to intercept conversations. The question, though, is whether even that really represents in this case a problem because you are being sent by somebody who wants to authenticate that you are the owner of a cell phone and you have it in your possession. So that's what the cell phone loop really does is they send you a text message which you type into the web page saying "just got it," meaning I have that cell phone. So even somebody eavesdropping, and it's really difficult to do so on today's era of digital phones, not impossible, I mean, unfortunately possible as opposed to, like, really, really good crypto...

Leo: Which is impossible, yeah.

Steve: Next to impossible. Anyway, the point is that even somebody who happened to catch, you know, a random text message, well, they're not - they don't have your established HTTPS secure SSL session with the bank. And any cookies you've exchanged hopefully are secure cookies, so they're in that secure tunnel. They have no ability to get to the page to enter what you just typed in. So even if it, like, had a banner, I mean, if it was skywriting and said, you know, here's my one-time code, well, nobody else can use it except you at that moment, and then it's not going to be good again. So this really is, I mean, it is a clever, nice means for doing a multi - adding a factor of multifactor authentication. And I just hope, and I presume, that these text messages are sent quickly. I know that many times, for example, I'm seeing sites where they require an email loop. And it's like, okay, we'll send you a link to click to authenticate. And then you sit and you sit and you sit. And it's like, okay, this is really not working if I don't receive my link immediately.

Leo: Right. Email can be slow. Email is unpredictable. I have found using this text messaging system, at least with T-Mobile, who's my carrier, and Bank of America, that it's every time. Actually a number of other things, services use this. And I haven't yet waited. You can always resend.

Steve: I think it's going to be very popular. I mean, it's a nice way of doing authentication for people who have cell phones with them.

Leo: I love it. I mean, it seems to me very much like the Secura Key. I mean, it's a one-time password; right? And I'm getting it by the phone, so I don't have to have a dongle with me. I just really like that idea. Moving right along, Neil Roberts in Liverpool, England, uses a literal firewall. Oh, come on. Literal?

Steve: Well, kind of. I didn't know how to describe it. But we'll see what I mean here in a second.

Leo: Hi, Steve and Leo. I mean, he's not putting bricks between himself and the Internet, is he? Being paranoid about security, I've been an avid listener of every episode. How about this for the ultimate security answer for online banking, PayPal, eBay, et cetera? I have my regular PC which I use for day-to-day use, web browsing, email, Word, et cetera, but never banking or whatever, you know, secure stuff. For the few highly sensitive applications I use an old G3 Mac running OS X v10.4.11. I keep the OS up to date, as well as the Firefox browser. I have it bookmarked with my bank sites, et cetera. I only ever visit these sites via the created bookmarks - good, right, because those are always secure unless somebody's hacked in and changing your bookmark. And I never use this Mac for anything other than visiting these bookmarks. What do you think of that?

Steve: Well, it's funny, for a long time, and I'm sure our listeners have heard me say this, one of the pieces of security sort of advice I've had for, like, moms and dads is never let your kids use, like, the important computer that you have your banking and your checking and your stock portfolio and stuff on because...

Leo: Because kids mess stuff up.

Steve: Well, and kids, lord knows what they're going to click on or where they're going to go or what they're going to do. And so this notion of, I mean, literally having separate computers, it's like, give the kids their own machine. And this is in Dad's den, the adult computer, the parents' computers. And under no circumstances, even when Susie and Johnnie both want to be on the computer at the same time and she's desperate to use your machine, it just has to be no, it has to be off-limits. So I really do, I really like the idea, if you've got an older spare machine around, to segregate its functions. It's going to be pretty good.

Leo: And he's - excuse me, I'm eating a cookie.

Steve: I stopped when you weren't expecting it.

Leo: Usually you talk longer than that. And by only going to the link as he typed it out, so he bookmarked it and typed it out, he prevents phishing.

Steve: Yup.

Leo: He prevents getting infected by these kinds of cross-site scriptings or the SQL injections by not going to other sites.

Steve: He also prevents phishing because he's not ever...

Leo: He's not even getting email, right.

Steve: There's no email on that machine. So there's - literally it's what he uses as his clean, uninfectable, like his browser interface to his financial things.

Leo: Would using a virtual machine in VMware have the same effect? I mean, does he have to use discrete hardware?

Steve: It has very much the same effect, although you could have something on the outside which is filtering or involved in his traffic somehow. And there have been some questions about whether virtual machines are really as secure as they - as being completely virtual.

Leo: If something can cross the border between the real machine and the virtual machine. So I'm running my Mac, and I'm running Hardy Heron, the new Ubuntu in a virtual machine of VMware. Is that Ubuntu completely isolated from the Mac? No, because I can see the Mac drive. I don't know if a virus could go across the barrier, but...

Steve: Well, and again, seeing the Mac drive is a perfect example of, you know, one of the nice things about, again, an older machine that you - well, and the other thing, too, is the kids probably wouldn't want the old machine because you can't - it doesn't do anything, barely runs a web browser, which is just all it needs to do.

Leo: Now, it's theoretically vulnerable because it is on the network. If it's getting online, it's also on the LAN.

Steve: Yes. And so, I mean, you really wanted to do it, you would use the triple router, the Y-connected triple router approach to give it its own LAN segment such that it can't reach the family LAN, and the family LAN cannot reach it. And then it's a matter of discipline. But again, good security is always a matter of discipline. Under no circumstances would Neil ever go or do anything with that, no matter how tempting it is to compromise the security of it. So it's up to him to maintain it. But that's great security.

Leo: Nice job, Neil. And by using a Mac he's kind of, you know, even if it's a Windows network he's kind of - it's a good idea to do a different operating system, maybe using Linux in a Mac network just because then...

Steve: Speaking of which, speaking of which I put the following question after this one just for that reason.

Leo: Ah. Well, that comes from Dave Mulligan in Calgary, Canada. He shares his own tip for super safety. On a few occasions you've spoken about using a VMware image of Windows to access questionable websites or do other risky activities. I would suggest trying a Linux Live CD rather than going through the effort to reinstall the VMware image. Modern Live CDs like the new Ubuntu install disk work on almost any hardware and have a very recent copy of Firefox to do your surfing. Yup, it's 3.0b5 on Hardy Heron. Since the Live CD does not mount your hard disks, it doesn't even - now, I don't know, wait a minute, I don't know if that's true. Hmm, maybe they don't mount your hard disks. Your working install is safe, but it also means that any files you want to transfer will have to be put somewhere else on your network or a USB key. The safest way to surf, not to have any way for malware to persist on your machine or network. Because a Live CD generally doesn't save state of any kind.

Steve: Correct. Now, he mentions your network. You would really like it also not to mount your network.

Leo: Right. It does.

Steve: And that the only way then would be like a USB key. So you would use the Live CD to start clean every single time. It definitely does not want to mount your hard drives. Because again, the idea is containment. So, I mean, I really like the idea of a workable OS that you boot from a CD, and it's got a browser. Of course, it has to be on the network or it's...

Leo: Right, right. So it's going to mount your network. It's my sense that some Live CDs allow you to write to drives. You're allowed to save data. So you could really look on the Live distro to make sure that that one in particular does not save data to a hard drive.

Steve: Right, right. But I like this because, again, it's another - on the other hand, no one wants to reboot their system. That's a big pain, too. So maybe an old - here Linux makes even more sense than Windows because it's so much leaner in terms of processor need and RAM footprint that you could just use Live CD on a real old PC and just use it to do your banking and stuff. And again, that's got the advantage over what Neil is doing with his old G3 Mac in that every time you boot it, it starts from a clean slate from a CD.

Leo: Right. And then we've talked about those Windows - what was the name of that Windows thing where it starts over each time?

Steve: Ready, no, not Ready.

Leo: Anyway, we did a whole thing on it. You'd think we'd remember.

Steve: SteadyState. SteadyState.

Leo: SteadyState.

Steve: Windows SteadyState.

Leo: That would do the same thing; right? Kind of?

Steve: Yeah, kind of. I mean, in theory it looks like it does a good job. And, I mean, it's built for public environments and public access terminals where no matter what anyone does, when you restart the system, it flushes everything away that they did. But again, you've got bad stuff in there, hopefully the isolation holds and it's not able to do something. But if it had access to a USB key it might be able to jump out through there. I mean, again, it's still up to the user to make sure that they've got the various holes closed. And the idea of using a separate old machine with a Linux Live CD, for somebody who's really concerned, it's a great solution.

Leo: Steve Barta in Rowlett, Texas, likes tiny URLs, too: I'm a big fan of TinyURL.com and recently discovered SnipURL.com from Steve on a previous podcast. Steve and I both use that one because you can make your own tiny URLs, which I like.

Steve: Yeah.

Leo: I work for a large defense contractor, so security is a serious concern for us. The problem I have is URLs on our Intranet, our internal Internet, are often huge, with long text strings in them. I've noticed that these monster URLs don't always travel well, and sometimes word wrap, breaking apart in emails. I've found that TinyURL works fantastically for shortening these behind-the-firewall links. For instance, I can copy/paste a long URL into TinyURL, and the result, though the link resides outside my firewall, will still take me to the intended destination, but with a much tidier hyperlink. The question is, is there a security risk here? If I'm inside the firewall, and I click on a TinyURL public link that directs me to an internal website, is there a problem with this ping-pong behavior from a security standpoint? Always a big fan of Security Now! and an avid supporter/owner of SpinRite.

Steve: Well, this is an interesting question. I'm assuming that the URLs are not useful on the outside of the corporate...

Leo: That's key; right? Because if you could enter that URL outside the Internet, then it's insecure anyway.

Steve: Correct.

Leo: You're relying on security through obscurity.

Steve: The technology that all of these TinyURL and SnipURL and so forth use is an HTTP redirect. There's the ability for a web server to return, like, essentially an updated page to the web browser. I think it's code 302 permanently moved or moved permanently is the code. So what happens, the way this works is you click on snipurl.com/ - well, the example I gave last week, I created one that was rsa2008. So your web browser goes out of the corporate Intranet, across the corporate firewall, out to the SnipURL server, and attempts to bring up that page, literally snipurl.com/rsa2008 page. What is behind that is a database of correspondences of short URLs to long URLs. So the page that is retrieved by the browser is one of these 302 pages that says that page you asked for has been moved permanently to this URL. And that's the big nasty long one. So the browser gets that, and then it immediately, instead of showing you that other page, it brings up the page where the short URL has been in theory moved to, which will be this internal URL that then allows somebody inside the corporate network to bring up the page.

So when he talks about it breaking in email, I'm thinking, okay, well, he must mean internal email. So he's sending internal email to a colleague saying check out this new update to our internal Intranet page or whatever. And so the only exposure that I could see is from an information leakage standpoint. That is, many times URLs have interesting stuff in them. I mean, what could you learn that might be a compromise? He says he works for a large defense contractor. So the question is, is it just gobbledygook, GUIDs and random nonsense in the URL? Or could these URLs contain human readable content? Because they are passing in the clear outside of the corporate network. Other than that, I think it's pretty secure.

Leo: Yeah. So I think he's more worried about this translation issue and does it somehow open it up. But the real key is that your Intranet should not be accessible from outside your network.

Steve: Correct.

Leo: Richard de Tarnowsky, Senior Systems Administrator of LiveWorld, Inc., takes issue with the idea of running everything over SSL. We were talking about that a couple of episodes ago. He says: There were several points brought up in this episode regarding running SSL security on a website that I have to disagree with. Well, this guy's a senior systems administrator, so I'm going to listen to him. It might be reasonable to run entirely encrypted on a low-traffic site, hosted on a single machine. That configuration is not appropriate for a large commercial site. Remember that SSL certificates - yes, I'm aware of wildcard certs - are only valid for a particular host name. When building a high-availability, high-traffic site, there may be many servers hosting various bits and pieces of content. Often a front-end device like a load balancer may handle all the SSL traffic, only one cert per URL required. This simplifies certificate management and avoids per-server charges. If the site has lots of graphics or video, there might be a significant performance hit for applying encryption. Don't forget, if you embed nonencrypted content into an encrypted page, your visitors get that lame popup from their browser unless they've been convinced

to turn them off. I could go on and on for several pages, but I'll just stop here. SSL is expensive in hardware costs, certificate direct and management costs, design time, and - and I think this is probably the key - operations overhead.

Steve: Well, I wanted absolutely to share Richard's feedback. I'm sure there's some validity to it. I wanted to take issue only with this idea of its being a performance overhead because certainly certificate management is an issue. I mean, I've got my own little site, and I have a number of certs because I need - I mean, and I have, like, GRC.com, it has its own certificate; www.grc.com has to have its own certificate. So I'm paying to allow people to connect securely either with the www or without. That's two certificates. And then I have another server, GRCtech.com, and it has to have a certificate. So, I mean, I'm very sympathetic to the idea that dealing with all of these certs is a problem.

On the other hand, he talks about mixing content. And it is the case that the only overhead is the initiation of a connection. He was saying that, for example, running large content like videos and large images and things would create some encryption overhead. But that's not the case. It is the establishment of the connection that involves the public key exchange. Once they've agreed, using random number generation, they then have a symmetric key which is extremely fast, I mean, faster than reading the content from the hard drive or, I mean, like just not a problem in terms of overhead. And modern browsers leave connections up over time. So a browser will establish typically up to two connections to a remote web server. It would bring up SSL connections on them both. And then all of the interaction with the web server for a great deal of time would be over those connections, with multiple assets of the pages going back and forth through those established connections. So, I mean, I absolutely empathize with this notion that having everything be SSL would be expensive in terms of management and costs and sort of operational overhead, but not actually performance hit for encryption. That's just not there.

Leo: Okay. Good to know. Actually I was curious about that. The encryption process itself is pretty fast.

Steve: Right.

Leo: Now let's move on, ladies and gentlemen, to the Terrific Observation of the Week. Tyler Larson does it from Arizona: I'm not sure who caught onto this, but the keynote given on Hierarchical Temporal Memory that Steve pointed out from RSA 2008 makes one thing very clear: This is the beginning of the rapidly approaching end of CAPTCHA. The type of problems that this new type of AI, this Numenta AI, is already able to solve are exactly the same set of problems posed by websites in trying to determine whether or not you're human. For example, read the text in the noisy background, identify words in this noisy audio, or even identify which of the following pictures are kittens. That's what they did, didn't they.

Steve: Yeah, it's so good. I mean, it's remarkably good.

Leo: As this new AI technology gains footing, we're going to have to rethink our approach to guest authorization. Gone will be the days where we could simply sort based on human versus machine. We'll instead have to grant authorization based on whether the human or machine is acting on behalf of an otherwise allowed party. That's a good point. My agents might be logging in and creating that email account automatically for me, and that's intended. Obviously the implications to the security world are significant. This is an extremely difficult problem to solve. But if we don't get a head start on it, we're going to find ourselves woefully behind when the bad guys start catching on. I think security certifications everywhere. You'll need a personal cert to do anything on the 'Net.

Steve: Well, and our listeners will remember from the coverage that we gave to CAPTCHA how surprisingly difficult it is at the other end of a Internet connection to tell whether somebody is a human or a machine.

Leo: The Turing test.

Steve: The Turing, exactly, the classic Turing test. And so I think what I liked about Tyler's observation is, I mean, if anyone's interested and did not have a chance to yet go look at Jeff's tremendous presentation of his Hierarchical Temporal Memory at the RSA conference, it was in the keynote, again it's that SnipURL, snipurl.com/rsa2008. That'll take you to the page of all of the keynotes. And Jeff just does, I mean, he shows pictures that this technology of theirs is able to correctly identify. I mean, it's just - it's jaw-droppingly impressive. And so it truly does make the problem of performing this kind of differentiation much more difficult.

Leo: Interesting, yeah. Well, it's a brave new world. I mean, if Jeff Hawkins can create these chips that work like the human brain, all bets are off in every respect. I mean, we've got a whole new, I mean, CAPTCHA, losing CAPTCHA is the least of it.

Steve: That's true.

Leo: I mean, everything changes all of a sudden. And he talks in his book "On Intelligence," he talks about the implications, the last chapter talks about the implications of a chip that thinks like humans. And, I mean, he says they're not going to - it's not like we're going to suddenly be faced with robots that want to take over the world, he said; but things like air traffic control, you know, weather forecasting, a lot of stuff can be done by machines that humans do right now.

Steve: Yeah, good stuff.

Leo: Good stuff. Not bad stuff. Well, maybe some bad stuff. Mr. No Name in Detroit shares some additional sobering truth: I have a small computer repair company while I finish up my computer science degree. And like the listener that wrote in during Episode 140, I, too, maintain small mechanics shops' computer systems. One

day when I was updating the office computers the service guys called me out into the garage to look at a computer. And lo and behold, they were ripping shop clients' CDs to the computer and wanted to know how to get the data onto an external hard drive so they could take it home. They were also getting data from thumb drives left on key rings and MP3 players. I worry less about the music data and more about the personal photos that anyone may have left on a thumb drive they don't want to get out. We talked in Episode 140 about a mechanic. Actually a guy sent in a note saying a mechanic that stole everything. If you leave data in your car, it's gone.

Steve: Yeah, I thought it was just worth refreshing one more time. I mean, this was not necessarily anecdotal. Apparently this is just what goes on. And, I mean, no offense to mechanics all over the planet. But it's clearly something that is happening, and our listeners ought to just be aware of it.

Leo: Get yourself a valet key and lock everything in the trunk, kids. Or take it with you. And we're going to do a bonus one. This is the Quip of the Week from listener Roger. You ready for the Quip of the Week? Funny how VeriSign's EV certification has VeriSign authenticating itself. Surely you'd think they'd get someone else to vouch for them, even if they are - supposedly - VeriSign. Hmm.

Steve: I got a kick out of that. You know, we've talked about the chain of certification or authentication where you have an SSL certificate that is signed by somebody you trust to have done their homework, to have done due diligence to verify the identity. And so what does it mean when VeriSign signs VeriSign's own certificate? I guess they're very sure about who they are.

Leo: Yeah. But are you sure about who they are, and should you trust them? I don't know. I don't think so. That's why we have key-signing parties. It's that chain of trust. We go out and, here, I am who I say I am. You see my driver's license, everything, could you sign my key, my PGP key?

Steve: Yup.

Leo: We've reached the end of this fabulous episode. But it's just the beginning of your quest for security. If you want more, you can get more. Use that Download All Scripts for your Firefox, or CURL and SED. But somehow you can download all the shows ever recorded. Steve's got a list of them all at GRC.com. And along with that you'll find the show notes. You'll find transcriptions of every show in PDF form. I mean, it's just a great treasure trove of security information, all 142 episodes. GRC.com. While you're there, make sure you take a look at SpinRite, Steve's baby, his pride and joy, that program that saves hard drives right and left. It's the ultimate disk recovery and maintenance utility. I use it; so should you. SpinRite, it's at GRC.com.

Steve, we'll see you on the radio show. Steve joins us every Saturday on the Tech Guy show to talk about security. And of course next Thursday for Security Now!. Have a great week, Steve.

Steve: You, too, Leo. Thanks very much.