Listener Feedback Q&A #53

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-169.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-169-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 169 for November 6, 2008: Your questions, Steve's answers. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

Time for Security Now!, the show that talks about protecting yourself online, your computers, at home, keeping spyware, adware, and malware off your system. And here he is, the guy who coined the term "spyware," knows more about protecting you than anybody else, Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Hello, Leo. Great to be with you for our weekly chat.

Leo: Yes. Did you stay up late on election day? Election night?

Steve: More than usual, yeah. I finally gave up at 10:00, I think, because I'm up at 4:30 in the morning, so yeah. But I feel fine. I'm on six and a half hours, so that's fine.

Leo: Is that all you need? You only sleep six hours a night?

Steve: No, no, no. I normally give myself eight. I've learned, I mean, I'm just useless to myself and the rest of the planet unless I have enough sleep. And so I really do give myself enough.

Leo: I read a programming book once, the guy gives programming classes, and he says to his students, he says, "Coffee is not a substitute for sleep. Don't think it is." There he goes. Now, Steve, how big is that? Wait a minute, how big is that cup of coffee? That's the biggest thing I ever saw. As soon as I said, "Coffee's not a substitute for sleep," Steve pulls out, like, a quart of coffee and starts drinking out of it. But it is a good point. You've got to have, you know, if you really want to use your brain, you've got to have a good night's sleep.

Steve: Yup.

Leo: And a quinti venti latte.

Steve: Quinti venti latte. Keeps everything going, yeah.

Leo: Today our Q&A segment. We've got 13, or 12 great questions from our listeners, including the Sockstress solution and a Sandboxie question. Which we'll answer in just a little bit. We also have the tech news. And I'm sure we have errata and addenda from previous episodes. So did you make any mistakes in the last couple episodes?

Steve: Well, we have no errata.

Leo: See, he's perfect. I knew it.

Steve: Although we did have someone who disagreed with something that we said. And so we've got a nice disagreement question in here, which we'll discuss.

Leo: We'll do that later.

Steve: It's not quite the same. But there was a bunch of security news, or some. Some interesting stuff. I discussed the update to Opera last week and said that probably by the time people heard this, 9.62 would be available. I wanted to confirm that, sure enough, I think it was later that day when we recorded it, last Wednesday, 9.62 because available, which solved a very serious exploit in Opera. So I wanted to make sure that anyone using Opera knows that 9.62 is available and updates themselves to it.

The OpenOffice suite has an also serious image-based remote code exploit. Any OpenOffice versions prior to 2.4.2, and apparently OpenOffice v3, which is just out, also has it fixed. And I'm not sure about StarOffice, the commercial version. But it might very well be that StarOffice has a problem. If you own StarOffice, you'll want to check to see whether this problem that's been found in OpenOffice - it involves the display of WMF

and EMF, that is, Windows Meta File and Encapsulated Meta File format. So that, you know, if an OpenOffice product displays one of those images, there's a - actually it's a heap overflow in the processing code for the image display that can cause a remote code exploit to occur on your machine. So you want to make sure you update OpenOffice, if you're an OpenOffice user.

Leo: And there are Mac users who use NeoOffice, which is a Mac spinoff. They probably should also check.

Steve: Absolutely.

Leo: I'm sure they all use the same Java libraries, so.

Steve: Then Microsoft produced what they call their Security Intelligence Report for the first half of 2008, so the first half of this year. And they've had some interesting statistics. For every thousand runs of the MSRT, that's that Malicious Software Removal Tool, which every second Tuesday one of the things almost invariably on the checklist is update your malicious software removal tool. And then it runs the next time you restart your machine. So for every thousand runs of it, it finds, or in the first half of this year found three bad things in Vista Service Pack 1; found 10 bad things in XP Service Pack 2; and eight bad things in XP Service Pack 3.

Leo: Holy cow.

Steve: So that gives us some sense, I mean, I've always wondered what it's doing. It's never found anything bad on any of my machines. But clearly, so what's that, 10 and eight, that's 18, and three, so 21 things bad out of a thousand runs. So it certainly is finding problems.

What's interesting is, and this was not - it won't be a surprise to our listeners, who've been following along and paying attention, is that eight out of the 10 top problems, that is, 80 percent of everything found relate to ActiveX controls. That is, this really disturbingly ill-conceived technology that I've groaned about in IE from the beginning, the idea that Microsoft didn't implement a secure, a fundamentally secure approach to allowing scripting and add-ons for IE. They basically took their existing DLL technology and renamed it ActiveX so that basically anyone can provide ActiveX controls, which is executable content that your browser runs. And we know what a focal point for security problems web browsers are. I mean, it's the thing you're sticking out onto the Internet every time you visit a website.

Microsoft defended, as part of their dialogue explaining this, they defended ActiveX but acknowledged that it was impossible for Microsoft to police its technology. And the guy that produced the statement said, quote, "You have to enable add-on development for the browser. The question is, how do you extend the browser and at the same time provide guidance to developers on how to write secure ActiveX controls?" And of course my answer is, well, you don't. You use something like JavaScript, which is a sandboxable, fundamentally protectable technology, where you're able to run scripting in a safe interpreter rather than literally downloading executable code that runs natively on the machine. That's just too dangerous. So for that reason we're going to have the author of

Sandboxie on as our guest next week because...

Leo: Oh, good. Oh, fantastic.

Steve: Yeah. He and I have had a dialogue in the past. I asked a question in our newsgroups, GRC's newsgroups, and learned that a ton of people are using Sandboxie with 100 percent good experience with it. So that, okay, it's time to have this guy on to tell us about the notion of sandboxing web browsers. And it goes way beyond. Sandboxie started off as Sandbox IE, but it's an absolutely effective sandbox, for example, for Firefox, as well. So he will be our guest next week.

Also there's a really interesting report from RSA Security about their discovery of the surprising penetration of a trojan called "Sinowal," also known as "Torpig" and "Mebroot." And it's three different names for the same thing. But we spend a lot of time talking about, okay, you want to be careful because you don't want to get one of these on your machine. Well, next week I'm going to describe in detail what RSA found and has made public about this trojan because it really drives home how important it is for people to go to whatever lengths they need to to keep their machines clean. And so it'll be the perfect companion to our talking with Sandboxie's author because his concept is the notion of wrapping protection around the browser.

We know that you could use a so-called "heavyweight" approach, for example, running a browser in a virtual machine, and use that for containment. But that's, again, it's expensive in terms of starting it up, shutting it down. As we know, VMs need to have all of the RAM that they ever might use preallocated. So it's not RAM friendly in terms of sharing resources with your machine. Sandboxie takes a very lightweight approach. And so I want to have the author on to sort of explain to us what he's done, and why what he's done is safe. Because from everything I've heard, and I've used it myself, what he's done is easy to use, and that's really what you want in this kind of a prophylactic wrapper around our web browsers.

Leo: You know, when you say "trojan penetration" and "prophylactic wrapper," you're really making me think it's another subject entirely. But I'm going to keep my mind out of the gutter and remember this is about security. Okay.

Steve: Well, and I'll change the subject quickly to get us away from that.

Leo: Please. Thank you.

Steve: Just sharing a quick little note from someone, Jake Oswald, who for a change is not a Security Now! listener. But he wrote to us just to tell us that he was really happy with the way SpinRite works for him. He said, "I recently had a system failure after an automatic update of Windows XP from Microsoft which required a system restart. When I turned on my monitor, the screen displayed 'Windows is shutting down,' which it wasn't because there was no hard drive activity, and it had been trying to do that for hours. So I pressed the reset button and eventually got a screen that said there was a corrupted config file, and the system could not restart. I contacted my employer's technical support service. And as soon as he learned that it was my own home computer and not one of the office computers, he said, 'Log onto GRC.com and buy SpinRite because it repairs,

quote, nine out of ten disk failures, unquote.'" So he says, "I did, and it did. SpinRite ran for about five hours. And when I rebooted, it was fixed. Thank you for a great product."

Leo: Very good. Very good. Once again, SpinRite to the rescue. It's like the Dudley Do-Right of software programs.

Steve: You did that voice well.

Leo: We'll save you, Nell. Just turn on SpinRite, and all will be well. Sorry about that. I apologize profusely. We've got questions for you, Steve. We've got some great ones, 12 questions from 12 listeners, strong and true. Are you ready, Steve, for some questions?

Steve: Ready.

Leo: We've got us some good ones. Actually a similar question from two listeners. So if you don't mind, I'll read two questions in a row for you here. First, from Guillaume Auclair in Sherbrooke, Quebec, Canada. He wants to crypt his links. He says: Hello, Steve and Leo. Now, I've re-thought about your forthcoming project CryptoLink. And we talked about that on a previous show. I relistened to both the PPP Security Now! episodes, the Perfect Paper Passwords. And I've just got to have at least an idea of when this product's going to be available. And I'd like to know if split-tunneling will be a part of it? I'm sure you'll explain that, Steve. Well, I guess he's going to explain it. If I'm at a remote location, plugged into an insecure link, I want to be able to VPN tunnel home, ask for a web page, then home fetches the page, sends it to me through the VPN tunnel. I have some customers who'll be ready to pay for that kind of setup, especially if it's going to be in Assembly and small and fast. Which is your specialty, Steve Gibson. So he wants to know when we're going to see CryptoLink.

And Rich Schreiber in Erie, PA, says - it's a question - "CryptoLink?" He says: Dear Steve, I know you're extremely busy. I wanted to thank you and Leo for your devotion to keeping us all informed and secure. I also want to know if you could mention on a future show the status of CryptoLink, maybe even some of the features you plan to implement. Many of us are waiting with great anticipation. OpenVPN works great, but too difficult to walk someone through on the phone. Hamachi forces disconnects if you don't continuously upgrade every time they come out with a minor upgrade, and you can't route through the host. Other options aren't secure enough, or don't offer true VPN connectivity. Thanks again.

So, Steve, what's the story? CryptoLink in your future?

Steve: Well, this is representative of a bunch of questions, so I finally just today I thought, okay, as I was reading through these, I ought to just take a minute to sort of explain to people where we are. You may remember, Leo, I think it was a little over a year ago, you and I were - it's the time we were in Vancouver, sitting at the table on that patio outside.

Leo: I'll never forget. It was a beautiful night. That was a lovely bottle of wine. And you told me something very interesting.

Steve: Well, I recited to you just by memory three pages of bullet-point features for the upcoming VPN-ish thing that I wanted to develop. And at the end of that third page your mouth was hanging open, and you said something like, wow, you know, if you pull this off, Steve, it'll be the most significant thing you've done.

Leo: I had the same reaction these guys are having, you know, when?

Steve: Yeah. Well, and that's the problem. It's just me doing this. And my style is much more the tortoise than the hare. It's not that I'm slow. But I hope that I'm thorough. And my approach is to really want to get something done, I mean, get it done, finished, really to a point where I never need, or not soon, need to look at it again. SpinRite 6 has - not a single byte of its code has been touched since it was released in 2004.

Leo: Which, I want to point out, is not a bad thing. It means it's there.

Steve: It's done. It's bug free. There's nothing that I know that needs to be changed.

Leo: And you don't - this is what I admire about you. Your tight code, you know, the feature set is there. You don't feel the pressure that many manufacturers or vendors seem to to add unnecessary features just so that there'll be an upgrade every year.

Steve: Right, exactly. So, yes. So I'm not, like, nickel-and-diming people. SpinRite 5, I think, lasted for five years before 6 came along because I needed to add compatibility with unknown partition types.

So last summer I was really anxious to get going on CryptoLink, but there were a couple of things that I had left undone. There was the whole third-party cookie initiative that I feel strongly about. I wanted to add the technology to the site, to GRC's site, to sort of automatically in the background let people know if third-party cookies were enabled because it's so easy to turn that off in all contemporary browsers. The problem was, strange as it sounds, sort of due to the organization or disorganization of the site, I didn't really have a place to put those pages. That is, there was already sort of everything there, but no real good organization.

So I thought, okay, before I do that, I need to do a menu. And so I developed over the course of several months the world's only really bullet-proofed, 100 percent script-free, non-active anything, non-JavaScript anything, menuing system. Well, it took much longer than I expected. But when it was done, it was done. And it's perfect. I haven't touched it since. All kinds of people have used it and do adopt it continuously. I get email from people with a question here or there, or they'll often post a question in the newsgroups, and somebody there will answer it. So that gave me sort of the structure that GRC was missing, that allows me now to hang new things off of the menu, which I didn't have before.

Then I switched back and plowed into finishing wrapping up the third-party cookie technology, which I had written all kinds of substrate, but had never gotten it finished because something else came along and interrupted me. So I thought, okay. My point was that, when I start on CryptoLink, because I am so resistant to changing what I'm focused on, I just - I didn't want to have to be pulled away from CryptoLink. So I thought, okay, that means I have to have menuing on GRC, and I've got to get the cookie system finished, like finish these things that I had invested in heavily but hadn't had time to get back to.

So what ended up happening was, we found bugs in every browser's handling of cookies. And I've ended up with an amazingly thorough cookie-handling analyzer. Several things already happened. Firefox 3 is substantially better as a consequence of the Firefox guys, who were tuned into what was going on. They, for example, realized that when this thing came out and was going to require people, I mean, tell people you need to turn off third-party cookies, they had removed that from the user interface in Firefox 2. And they realized they're going to be in trouble if they don't have that in Firefox 3. So that's the reason that simple checkbox was returned in Firefox 3, making it easy for people to disable third-party cookies. And there were some problems, there was some cookie leakage that the technology at GRC discovered in header assets, page assets, page headers. Turned out you couldn't turn them off. Even though you said disable third-party cookies, they kept happening. And IE, both 6, 7, and 8 have problems, as well.

So all of this was - so all that technology finally got finished. And I was just starting to work on the documentation, and Dan Kaminsky happened with his DNS exploit. And remember, I think that was in May, I think. Well, in June I decided, okay, this is a problem. It'd be useful to do a really thorough analysis of DNS servers. Well, that was four months ago. And so I suspended the work on documenting and getting the cookie system public in order to do this test of DNS server operation.

What we have is something phenomenal. I mean, it hasn't - it's not public yet. All of the guys in the newsgroups have been testing it. Turns out all kinds of DNS servers are still vulnerable. They have not been patched by their ISPs. I will be making this public to our Security Now! listeners before anybody else, probably maybe two or three weeks from now. Essentially, all the technology is finished. Now I've got to explain it all so that people aren't left with more questions than they started with. But once that's done, then I go back and write the documentation for the cookie system, which is also completely finished. And at that point I get to start on CryptoLink.

Leo: So you haven't even - you've mapped it up, but you haven't started writing code; is that what it is?

Steve: Correct. I have - no code is written.

Leo: Because you had a very - you know what you're going to do.

Steve: Oh, it's so simple. It's just a matter of sitting down; and, I mean, there's nothing I want to do more than to say, okay, I get to start on something new. Now, there's three - at least three patents are going to come out of this. One of them I already started. In fact, one of them is finished, done, submitted. I've got serial numbers and so forth. And to give people an idea, I mean, to answer our second, Rick's question, like some of idea of what it's going to be. First of all, it can be anything we want. I mean, my intention is

that it is an incredibly easy-to-use VPN product that, for example, supports the YubiKey natively, supports Perfect Paper Passwords natively, supports OpenID. It has a fundamental TNO, the Trust No One model, so that there's no third-party involved. So, for example, in our first questioner's instance, you'd be able to run your copy of CryptoLink at home, and you'd also be able to have it on your laptop. And so your laptop would connect to your home. And then your home would reissue the traffic coming from our laptop out onto the network. So it'd be like your own personal hotspot VPN, with the advantage being that your traffic is decrypted only at your home, not at some central point like on a TOR node or at a hotspot VPN that might tend to be a magnet for people who want to do traffic analysis to see, oh, who's using the system for what purposes to encrypt their traffic? So it'll do that.

It'll also do NAT router penetration the way Hamachi does, so that if you don't want to set up a system at home, if you just want to, like, mail a copy to a friend whose desktop you need access to, you can just email it to them. They can run it, and it'll connect in the same easy way that Hamachi does. But, for example, unlike any other SSL VPN, even though it has an open port, the port is not open, which is the first of the patents that I have underway. I don't want CryptoLink's open ports to be visible. So I have a way of cryptographically stealthing open TCP ports. That'll be part of what CryptoLink does. And, for example, CryptoLink will also be able to open an array of ports, and your client will send an array of packets to them so that, if any intermediate ISP is blocking some of them, other ones get through.

I mean, the idea is I'm going to do everything I can, and that's a lot, essentially anything, to come up with a product that just works. I was having dinner with some people about six months ago. Two couples were in the car, driving to dinner. And both of the gals, by bizarre coincidence, were complaining that their corporate VPNs wouldn't connect. One had been in the hospital with her husband, and she said, yeah, I couldn't use the - I was able to get online in the hospital, but my corporate VPN wouldn't work. And the other one said, oh, yeah, I have the same problem. I'm never sure if it's going to work or not. Well, my goal is, this thing, I mean, I'm not going to stop until this thing manages to find a connection no matter what it has to do.

So anyway, that's my plan for it. My development arc is - what I intend to do is to very quickly get something working. That is, I'm not going to just sit, the hermit in the cave, for who knows how long until I believe that I've got something fully finished. The technology just isn't that hard for me to develop. I've got so many pieces that I've worked out already that I'll be able to get something going soon. So it'll be in pre-release but usable condition. And then we will start adding features. I say "we" because a lot of this is going to be done with full visibility to the people in GRC's newsgroups. They're just a phenomenal resource. I've used them with SpinRite and with the cookie development and with this DNS name server testing. It's just so tremendous for me to be able to put some code up and say, okay, guys, here's something new. Tell me if I got it this time. And in very short order I've got a really good, broad-spectrum testing. And it also allows people to say, hey, what about this, or what about this? Or, hey, I need this, or I need that.

So anyway, I'm very excited about it. I have no idea at all when it will be done. There will be a "done" because everything I am is about saying, okay, this is Version 1.0, and it is complete. It is finished. What I can say is that lots of people will be able to use it as it goes along. And basically what I'll be doing is adding feature after feature after feature. My intention is to actually write the UI in something very plastic, like Delphi, just because I don't - what I always end up doing is I paint myself into a corner by designing the user interface first. Then, because I want everything tight all the time, and that then tends to limit me from adding features. So my development arc is to write the core in Assembler.

Ultimately, once we know what it wants to be, once every feature that we can think of and is useful is there, then I will cast the UI portion in Assembler. So it will end up being 100 percent Assembly language, super tight, super small, with a ton of features that everybody wants, that nobody has taken the trouble to do before. Because I look at these VPN products, and they're just like, okay, well, that's fine. But that's - I can do something way better, that is way more robust and way more secure, with all kinds of authentication, Trust No One or use a third party, a rendezvous server for NAT penetration, it's just - it's going to solve the problem.

Leo: And unfortunately it's going to be Windows-only.

Steve: Yeah.

Leo: Just thought I'd throw that in.

Steve: Yeah.

Leo: When it's Assembler, you don't have a choice. Actually, you know, you could write the low-level code, well, I guess you're going to make calls, though, to the Windows API, even from Assembly.

Steve: Well, yeah.

Leo: So you really can't write the low-level code in portable fashion.

Steve: It'll have, I mean, in my wish list, as I've been brainstorming this, so many cool things. For example, you'll be able to maintain plastic connections to remote instances of CryptoLink, meaning that, if your 'Net connection goes up and down, it's not going to give you dialogues; it's not going to complain. It'll just wait until it's back on the 'Net and then reconnect to the things that you said you want to make a persistent connection to. So that, for example, you could have resources like your printer at home. Your printer at home will just look like a printer on your laptop. And you can print to it, seamlessly, no matter where you are. And CryptoLink will take responsibility for maintaining and repairing and keeping its connection to your printer at home, transparently.

You'll be able to run in what I call a "full enclosure mode," which actually is what one of these guys was asking about, where all of the traffic that you use on the Internet is encrypted through the link to the remote point. And then it's decrypted, whether you're accessing machines in that network or going back out over the Internet. But maybe you don't want to operate that way. Maybe you only want to talk over the link to your network at home. Otherwise, for whatever reason, you're fine with the greater performance you would get going directly to the 'Net. So you'll be able to specify that. I mean, all kinds of things. You know, one of the problems OpenVPN has is that it's router table based. And so if the network you're connecting to happens to be in the same network as the one you're on, that completely fails. Well, CryptoLink solves that problem. So just one thing after another, after another. Problems that I've experienced, problems that other people have experienced, I'm just going to solve them all.

Leo: Sounds great.

Steve: So that's my plan.

Leo: Looking forward to it.

Steve: And I've got some things I have to get finished first. But there's nothing I want to do more than to get working on it. So as soon as I can, that's what I'm going to do.

Leo: Very good. Question #2, Dan Gardner - "Disappointed" Dan Gardner, I might add...

Steve: Oh, very disappointed.

Leo: Very disappointed in us. In San Antonio, Texas; writes "I'm very disappointed." He says: In Episode 167 - the last listener Q&A that we did - regarding the response to Dave in Perth about his ISP blocking port 25, if incoming SYN packets get blocked, then those of us who run small home-based web servers will be totally up the creek. That's right. Besides that, what impact would incoming SYN blocking have on remote desktop access, desktop and other services like that? I assume remote access, remote desktop uses TCP/IP.

Steve: Yup.

Leo: I couldn't believe Leo when he said, "I love this idea of blocking SYN packets. It would eliminate all this stuff." It won't "eliminate all this stuff." It might eliminate some stuff, like botnet operators from contacting bot-zombied machines via TCP packets. But will it prevent bots from receiving UDP packets on standard open ports? I don't know a lot about how UDP works, so you'll have to answer that one. I don't think you can have a conversation with UDP, but I guess they could - well, I'll ask - we'll ask the expert. Will it prevent the spread of virus through malicious Java code on websites or through emails? Either way, blocking incoming SYN packets will affect a lot of people in a bad way. So why are you and Leo salivating over the idea?

I don't think we salivated. In fact, I think we were very clear that there would be problems associated with it, including people running servers.

Maybe Leo and you can afford to pay for a web host, but there are lots of folks who can't and just want to run a noncommercial, low-traffic web server from their homes. And dropping incoming SYN packets will eliminate that ability. Yeah, there are free hosts with tons of ads and pop-ups, I suppose. But maybe we don't want all those ads. Anyway, I'm very disappointed in you and Leo. I am a SpinRite 6 owner, promote it all the time. I'm probably one of the few who actually made an in-office purchase of SpinRite. At that time I lived in Garden Grove, California, and drove to your office to get it. Wow. You don't get a lot of people in the office buying SpinRite,

I would imagine.

Steve: There's no office anymore. We're completely virtual.

Leo: Well, that was version 5. He said, I picked up ChromaZone - wow - at the same time. I've been a big fan of GRC and a loyal listener of Security Now! for over a year, ever since I found out about it. But when you and Leo take positions like these, which restrict our use of the Internet, it really hits a sore nerve with me. Feel free to use this on the netcast if you wish. "Disappointed" Dan Gardner.

Steve: Well, I wanted to let Dan vent, and I also wanted to clear up any misconception that any other listeners might have. I wasn't saying I thought this was a good idea. I was saying I was sort of seeing it as inevitable. I could sort of see the handwriting on the wall. At the moment, ISPs are blocking incoming SYNs on specific ports. But sort of the general nature of an ISP's customer, the end-user is as a client of servers, rather than as a server of clients. And so I completely understand what Dan said. Of course, I mean, I'd be up the creek myself if I didn't have...

Leo: As would I. But those of us who run servers maybe should be buying different service or, you know, we have a higher responsibility. Now, here's the fundamental, I think the crux of his question. If it doesn't significantly improve security, then he's right. There's no point in doing this. What about, you know, does it completely thwart botnets? Does it thwart viruses in any way? Is it really an improvement in security, is the real question.

Steve: Well, first of all we know that the word "completely" doesn't have any place in any kind of a discuss...

Leo: How significant is it?

Steve: The problem is, it's trivial to do. It's literally a command entered into a router, into a filter list in a router. I mean, it's incredibly simple for an ISP to do. We know that, as I mentioned when we discussed this, I guess it was two episodes ago, in 167, we know there are ISPs that are already NAT-ing their customers. Customers don't have publicly routable IP addresses, like 25.26.27.28, for example. They've got something like 10.something something something, which we know is a non-publicly routable IP. It's in that 10. reserve space, just like 192.168 something something. So we know there are already ISPs that are not offering those services to their customers. And we do know that there are some ISPs who don't offer that service, but for an extra price you can purchase that. I mean, I can see that happening.

I mean, again, Dan somehow really got the wrong, I believe got the wrong impression of where you and I stand, Leo. We don't, you know, you and I are all for absolutely nonfiltered, nonrestricted use of the Internet. And my concern is that, because the majority of ISP customers don't need to serve, they only need to be clients, and because it's so simple to block incoming SYN packets - even though it isn't, as Dan challenges me on this, even though it isn't a solution for so many things - it's so simple to do, and it

would solve such a large chunk of problems, that I'm worried we're going to see the time when that happens. But I said "worried." I'm worried we're going to see that happen. Not that I...

Leo: You weren't advocating it.

Steve: ...can't wait.

Leo: You weren't advocating it.

Steve: No way am I advocating it.

Leo: Yeah, I think if you listen closely, we merely spoke of it as a possibility. And maybe even a probability, but not necessary something we were saying should happen.

Steve: Yeah. I'm afraid at some point we're going to start - we're going to hear about it, and we're going to see it, and we're going to say, well, yeah.

Leo: People were very upset when Comcast started blocking port 25, which I think is a perfectly reasonably thing; but a lot of people say, but I want to run my own email server. I think that there are, you know, there's a balance. And frankly, if you're running a server, I think maybe you should be buying a different class of service. Maybe the solution is to offer tiered service.

Steve: Yeah. And you can certainly imagine a point where this price gets you a client-only connection, and this point allows you to host services.

Leo: Right. And then maybe they'd have to vet you more carefully, or monitor you more carefully. But most people would get the less expensive one, and that would eliminate a whole category. You couldn't do a botnet without SYN/ACK. Because you need...

Steve: Oh, sure.

Leo: You could?

Steve: You absolutely can because typically bots are phoning outwards from the infected client. So it's the SYN packet going out. And that you have to allow because that's how anybody connects to a remote web server.

Leo: But you also have to allow incoming commands, or a botnet is useless.

Steve: Sure, but those commands come in over the connection that was established first outbound.

Leo: I see.

Steve: So this would do nothing to thwart botnets, for example.

Leo: Well, if it doesn't stop botnets, it's not that useful.

Steve: Well, see, and that's the other thing, is that I don't think ISPs are really seeing much cost of problems at this point.

Leo: Right.

Steve: That is to say...

Leo: It hasn't hurt their pocketbook.

Steve: Right. If it was really expensive that customers were able to run servers, then there might be - you could imagine a motivation for the ISP to tighten things down. But there just isn't. It doesn't really matter to an ISP whether you're running a web server or a mail server. Well, except in the case of a mail server where it was expensive because then they were getting blacklisted as a source of spam.

Leo: Right.

Steve: And so there's another good example. ISPs are blocking 25 because they were finding their networks were added to blacklists, and that was causing a problem for all their customers. So their ISPs responded. When something causes pain, the ISP will deal with it. At this point, in general, running services doesn't cause an ISP any pain, so we're not seeing any consequence.

Leo: Well, I imagine so few people are doing it. I mean, it's not something most users do.

Steve: Right, right.

Leo: Ward Reed in Pensacola, Florida says, "Don't do it." Steve, sorry for the overstated subject line, but do not use your PayPal card - we were talking about the one-time credit card feature of PayPal. And he says: Don't use it as your primary credit card. It's acting like a debit card, or as one radio host calls it, a "fake" credit card. Even though Visa isn't a show sponsor anymore, the zero liability is relevant for a credit card only. That's not true, but we'll talk about that. The only problem with debit cards is that the vendor or scammer has your, as opposed to the bank's, money. You may or may not get it back. You are giving up far, far too much to use a debit card. Getting up one-time use isn't worth it. Discover has a one-time use option. I've used it many times. Citibank does, as well, for some of their cards. Our listener said American Express does.

But the banking laws have changed for debit cards. For a long time debit cards were very dangerous. But the banking laws have changed. I think a debit card is pretty much treated as a credit card now. Used to be they were only - you could take out a thousand dollars out of somebody's account, and the bank would say, yeah, sorry.

Steve: Well, it's interesting that this question hit at a time when just a couple days ago I found myself, like, at the PayPal site, ready to move forward; and I stopped because I remembered that it is impossible to override the source of the account. That is, PayPal will only take it from a checking account. And unfortunately, in my case, that's what I've got registered. I don't have a source of funds sitting in PayPal. And I remember there was - I wanted to briefly join for something, I don't remember now what it was, but it was a very sketchy site. And it was like, oh, there's no way I'm giving them my real credit card. So I thought, okay, I'll use a one-time PayPal.

But then I thought, wait a minute, I mean, I mistrusted this site so much that I didn't trust them even to withdraw the $4.95 or whatever they said they were going to. And I realized I was letting them, because PayPal doesn't give me an upper limit capability, I couldn't say create a card and set a limit for $5.50. It's just it's open-ended until you close it. And I thought, there's no way I can use this. Now, I do know - because many people have written in with their solutions for my credit card dilemma. One did say that American Express had withdrawn that service.

Leo: Oh, interesting.

Steve: So I don't know whether that's still available.

Leo: Oh, that's too bad. I'll have to check.

Steve: He was using it, and then they said it was no longer. However...

Leo: Why would you stop? That's such a great service.

Steve: Yeah, well, and apparently both - many people recommended Bank of America and Citibank, with both Visa and Discover cards. So I'm going to track that down. Someone said that Citibank has a downloadable piece of software. And I do like the idea

of using a piece of software just for ease of use instead of having...

Leo: You need to go to the website and...

Steve: Yes, exactly.

Leo: Although the website keeps all transact- all the card numbers and so forth, so you can kind of - you do have this record. I've just checked Visa and MasterCard, which is the kind of card that PayPal uses. Do stand by the zero liability for debit cards. So that - banking law apparently does give a little more leeway on debit cards for the bank. But both MasterCard and Visa have the same zero liability policies for your debit card as they do for your credit card. So Ward brings up certainly a good point, and one to pay attention to. And you might check. But according to MasterCard, which runs the program for PayPal, you do have zero liability.

Mark Bentsen in Dallas, Texas wants to transfer his risk: Hi, Steve. Can you recommend ways to transfer the risks associated with enjoying the conveniences of an online life? Wonder what he means? Well, let's find out. I do about everything that could be done online. And there's something in me that feels like I'm playing Russian roulette when I make a purchase or complete a form requiring personal information. I know that feeling. Since listening to the show, Steve, I have the same feelings, like what am I doing? I'm extra cautious now. As a project manager, we could spend a great deal of time considering what to do with risk. I follow the ATM methodology of managing negative risks: Avoid, Transfer, or Mitigate. Had you heard of that before? I've never heard of that before.

Steve: No, I thought that was neat.

Leo: Much of what I've enjoyed learning on your Security Now! podcasts are behaviors that I would classify as avoidance or mitigation of a negative event happening to my computer or personal data. In a recent financial course, I learned of insurance for identity theft that seemed reasonably priced. I know I'll not be out any money with charges made against my Visa card. But the loss of time it takes to repair personal identity theft increased on average to 600 hours - wow - 300 percent over previous studies of the Identity Theft Resource Center. That's true, though, when I hear about people having to clear this up, it does, it's just a time...

Steve: Oh, it's just unbelievable, Leo.

Leo: With my time and my attention being very valuable, do you agree this type of insurance is a good measure? Identity theft insurance. Do you see other ways of transferring the risk of identity theft when it comes to protecting your personal information? So he's saying we teach about avoidance and mitigation, but what about transferring the risk by buying insurance?

Steve: Yeah, the problem with that is that I'm not exactly sure what it is you're buying. As I understand it, the individuals who are victims of identity theft have to spend their

own time and resources. And, I mean, just writing letters and explaining and just jumping through hoops. And, I mean, really, we've all heard stories about how it just, like, ruins their life, and they end up with their credit messed up, and no one believes them. And it's like all of the burden is on them. I don't know how you insure against that.

Leo: Well, there are companies that do this.

Steve: You mean, what, like take over the responsibility of doing all that for you?

Leo: Well, the one that comes to mind is LifeLock, which has gotten a lot of advertising. That's the guy who gives out his social security number. And by the way, you know, here's the point of it. Basically they do what they can to mitigate. But then the real point of this is they, if you get your stuff stolen, they have a $1 million service guarantee, and they take care of it and so forth. I would investigate thoroughly.

Steve: So, okay, but that's prevention rather than...

Leo: No, it's both.

Steve: Oh.

Leo: It's both. So they do the prevention part, which I think is very important, although, you know, they do things like put credit locks on the various secure, like Equifax...

Steve: On the three different security services, yes.

Leo: The credit reporting agencies and so forth. But then - so they do all the proactive stuff. But then they say we'll pay up to a million dollars to cure the failure or defect in our service. See, I'd read these fudge words carefully. But the idea being, if you should lose your identity, we'll take care of it, and we'll reimburse you. I don't know if he's talking about LifeLock. I think that's the best known of these services. And, you know, there was some criticism of LifeLock.

But then Bruce Schneier, whom I know we both recognize as a real great security expert and very reliable guy, kind of came to their defense, saying that it's the credit - he wrote an article which I recommend reading called "The Pros and Cons of LifeLock." He said that the credit agencies hate these guys because they don't like these fraud alerts being placed. It's a pain in the butt for them, et cetera, et cetera. So they've kind of tried to pooh-pooh this. But he says, I think it's more an economics thing.

So Wired magazine's "Security Matters" column by Bruce Schneier, he talks about this. It came out in June of this year. I could put a link in the show notes. You can

read about the pros and cons. I would say his bottom line is, well, you can do all this yourself, so I don't know if it's worth paying for it to do it. But what the service claims to do, he says, get LifeLock if you want, or one of its competitors if you prefer. But remember you can do most of what these companies do yourself. You can do the fraud alert. You can put the credit freeze on your account. You know, you can check it regularly. I guess the real question that they, you know, you can do all that, is the insurance then worth it. And that's exactly what our question is about.

Steve: Well, and it's interesting, too, because I liked how Mark started off by saying, look, you know, I'm doing everything I can online, and I'm feeling very vulnerable. I mean, and you commented that just participating in the podcast for the last four years has heightened your awareness. And it has mine, too, because, I mean, this stuff is going on. And it is unfortunate that at this point in time we're sort of in this strange place where we are filling out forms, giving our name, address, fundamental information about us, spreading it far and wide to all kinds of entities that we know nothing about. We know not where they are, not who they are, nothing about their reputation. It's like, oh, I want what you have. So I'm going to tell you all about myself. I mean, it really is, it's something that doesn't scale well. And I don't think in the future that's going to be the way the model works. There will be models more like Google Checkout and PayPal, where they serve as a front and protect a lot of this information for us.

Leo: Yeah, ultimately that's probably a better way to do it. Google's doing it with medical records, too. And so they're really kind of investing in this kind of thing. Bruce's bottom line is it's 120 bucks a year. That's a lot of money. He doesn't think the risks you run are great. He says you can do it yourself. He does say they've paid out their guarantee 113 times in the four years the company's been around. So they do pay it out. He says, and by the way, most of the time it's been problems that occurred before the LifeLock was used. So he's saying what LifeLock does is effective. So you can do it yourself. Maybe the best thing to do is figure out what they do, read this article, do what he says to do, protect yourself, and then not worry about getting in trouble because you won't.

Steve: Right.

Leo: One hopes, anyway. It is scary. I mean, I understand what Mark's saying. It's scary these days. Mike in Ohio has an idea for hassle-free clickjacking protection. I used NoScript, by the way, and it's such a hassle I turned it off. It's like, every site, every site says, you want to use these scripts? And that's like, I gave it up. He says: After listening to the clickjacking episode last week, I had a question regarding NoScript. I have not used this plug-in prior to listening to the netcast, so I gave it a try. I quickly came to the conclusion - as I did - that this wouldn't be that easy to recommend to friends and family, who are nontechnical, based on the high potential of fatigue and frustration they may have in using the plug-in.

I remember you mentioned that NoScript would still protect you against clickjacking, even if you chose to use the option to allow scripts globally, which they say, dangerous, danger. So my thought was to get my family and friends to download the NoScript plug-in. If they experience any fatigue or frustration using the plug-in, then I'd have them enable the option that says just turn on all scripts, thinking they're

still protected against clickjacking. Your thoughts on this would be greatly appreciated. I also want to say I've listened to every episode, and I greatly appreciate all the work you and Leo do every week to produce a top-quality netcast. So that's what I'm doing, Steve, right now. I'm using it, but only with all scripts on because it's such a pain.

Steve: I did verify that what I had said last week was correct. And that is, with NoScript present, the current version of NoScript, if you do choose to allow scripts globally, then you still get full clickjacking protecting. The second link on the show notes for last week's clickjacking episode is a demo, a simple clickjacking demo. And if you go to a browser, either a non-Firefox browser or Firefox without NoScript installed, you don't see what's really going on. You go there with NoScript installed, even if you have decided to allow scripts globally, and instead what you see is what would normally be hidden, which is in this case the little Flash configuration dialogue asking for permission to turn on, to give the other end access to your camera and video. So yes, I wanted to let Mike know that strategy works.

Leo: And Leo. Because Leo's using it, too. It's like it's worse than User Access Control. I mean, oh, my god, every five minutes.

Steve: We have a couple more questions about that later on.

Leo: Okay. Jared in Australia, Washington - wait a minute. Or either in Australia, Western Australia, one or the other. I don't think there's an Australia, Washington. I'm guessing he's in Western Australia - is getting SSL certificate errors from Google's Gmail. He writes: For people who access Gmail over SSL using IE7, they might like to be aware of a certificate error page that IE presents you with before entering Gmail's page. If you didn't know this, you do now. You'll see, "There is a problem with this website's security certificate." Really, I haven't seen that. Of course, I'm not using IE7. "The security certificate presented by this website was issued for a different website's address." One of the two links is to "continue" - not recommended. Can you explain why this happens only with IE7 and not previous versions of IE? He's using the beta version, the new version of - oh, no, no. IE7 is the current version.

Steve: Yeah. It's weird. When he wrote this, I thought, well, okay, this doesn't sound right. On a hunch, I put in https://gmail.com. And I got that error message.

Leo: Oh, all right.

Steve: And so here's what's going on, is for some reason Google has grabbed the Gmail.com domain and has that pointing at the regular Gmail domain, which is mail.google.com.

Leo: Oh ho. So a little mismatch of the names.

Steve: Yes, exactly. So what Jared is doing is he's using Gmail.com, which is not the official website. I mean, that's not the domain name for Gmail that Google is offering. But it happens that it works. The problem is, since he's using https to go to Gmail.com, the first thing that happens during the connection is the name of the certificate sent from Google's server is compared with the URL, and they don't match because he's not supposed to use Gmail.com over a secure connection. So that's the cause of confusion. But I thought it was an interesting question for all of our listeners because the idea is that, as we've discussed before, the certificate of the server that you're connecting to, the exact name has to match what you've got in the URL, or the browser says, whoa, wait a minute, I've gone to the IP the DNS told me to go to. I've established an SSL connection. I've exchanged credentials. Yet the server is saying it's a different server than the one you're expecting.

Well, this is crucial for avoiding man-in-the-middle attacks because a man-in-the-middle attack would, I mean, it would intercept that. And what the man-in-the-middle cannot do is give you Google's certificate signed by an authority you trust. That's the critical link. And so it's important that the browser complain if there's a security certificate mismatch. But in this case Google doesn't have a different IP and a separate certificate for Gmail.com. Instead they just dump you on their regular IP. And sure enough, the certificate does not match.

Leo: Interesting.

Steve: Yeah, I thought that was sort of an interesting glitch. So Jared, you can avoid that by going to mail.google.com using https, and it works the first time, every time.

Leo: Yeah, I think I've seen that happen before when, you know, it's a mismatch of domain names. It's fairly common. So that actually would happen not just with IE7, with any browser would do that.

Steve: Yes, it should.

Leo: One hopes. If it doesn't, get a better browser. Kevin Lampo in Lebanon, New Hampshire was thinking about secure ways to vote using SSL: Steve and Leo, I've been listening since Security Now! was known as This Week In Tech.

Steve: I don't think that ever quite was, but...

Leo: Never happened that way.

Steve: But you launched your show first, and then Security Now! came along as number two, I guess.

Leo: So it's always been part of the TWiT network. It's a confusion because This Week In Tech is the Sunday show that's the roundtable with the journalists, which

you've been on. And TWiT, which stands for This Week In Tech, is the name of the network. So you're a member of the TWiT network, but the show is Security Now!. I know, I don't blame him for the confusion. He says, whatever the name: It's stimulated much gray matter, to the chagrin of my wife. As I sit here pondering what Tuesday's election will bring, I began to wonder how else people can securely and fairly vote. I also began to think about the long lines, the ordeal many have and the lack of polling personnel. I came to one question: Could a secure website, using SSL and a credit card, be structured to provide the mechanism for the a state to collect votes? There already exists the means to check authentication. The whole validation process can happen behind the scene as one is filling out the voting forms. The process could be done with little need for human interaction at home or at work. And that's what scares the hell out of me. What do you think? Thanks for all the info and the incredible and valuable SpinRite.

Steve: Well, it was an interesting question. My take is that the technology is not the problem.

Leo: Right.

Steve: You know, we've got the technology. I mean, we've got technology coming out of our ears. As soon as you have a public key technology where you're able to have one key encrypt something that only the matching key can decrypt - and vice versa, that other key can do the encryption and only your key can do the decryption - once you have that, that's an incredibly powerful piece of technology. And we've seen all the different ways that it can be used. But that's just the technological enabler. The problem is everything else. I mean, we could just sit here, and I'm sure our listeners could, too, just sort of tick off all the things that could go wrong with anything where we, like, try to come up with a non-person-present voting technology. And unfortunately, there seems to be a high motivation among some people to game the system, to come up with a way of exploiting any sort of weaknesses. So I just - I don't think - I think we're a long way away from anything happening. Not at all because we don't have the technology, but because we don't have anything else. So much else of what we would need to come up with a trustworthy voting system just doesn't exist.

Leo: You know, the temptation for technologists like us is to say, well, eVoting. And as we've learned from eVoting, which is even one step less removed than online voting would be, without a paper trail it's very, very dangerous. And even with a paper trail, people have to know enough to look at the receipt and say, is that what I voted for? And I suspect it's a problem. Doing it online, I wonder if we'll ever have online voting.

Steve: I'll be surprised. I have to say, though, I'm very disappointed in so much of what I see. I saw yesterday, because we're recording this on Wednesday, and yesterday was Tuesday, November 4th, Voting Day, the examples that were being drawn of the butterfly ballot, where how you're supposed to join two boxes by filling in a black mark, and it creates an arrow? And, I mean, in a recent small election something like one out of 10 people did it wrong. It's like, my goodness, folks, how can it be so messed up as that? And the other problem, the idea, for example, that a company like Diebold has a proprietary system that is closed source, closed technology, and they're selling it saying,

trust us. I mean, really, that's the kind of thing that can really get me going ballistic because it just seems so wrong.

Leo: In the state of California, I think we have a very enlightened Secretary of State. Debra Bowen, who I've interviewed before, is very technologically savvy. Last year she had the University of California assess these machines, and they were all decertified because they were all hacked. They could hack - they hacked them several different ways, and they said if you'd given us more time, we could have hacked them in more ways. So let's solve the security problems we have with online banking and the Internet first, and then we can think about voting.

Steve: Well, and for example, Leo, I mean, somebody is making a tremendous amount of money selling these machines to municipalities and the U.S. government. It seems to me, I mean, given all the technology we have, the proven capability of open source with a lot of oversight to vet problems, I know that if a requirement were put together saying, okay, whatever, manufacturers, you have the right to make the hardware following these specs. We're going to force everything else to be open, and let academicians and hobbyists and security professionals plow into this and come up with a robust solution.

Leo: Yeah. Still don't think it's going to happen.

Steve: I know.

Leo: And this is too important to mess with. You know, going to the polls, validating your, I mean, by the way, the secret of voting anyway is that a significant percentage of votes are lost, miscast, messed up. It isn't a perfect system as it is. And I don't think making it electronic is going to make it more perfect.

Steve: No. And although not wanting any more nightmares, it was nice that there was such a decisive result because now we're not in the margins, having to recount hanging chad.

Leo: And that's where it becomes problematic. And the thing is, as we go forward, elections are going to continue to be close. I don't think in this country, the way it's constituted, that any party is going to have such a strong majority, that many elections are going to be razor thin. And that's when all this stuff really becomes an issue.

Steve: Yeah, well, in fact, I think right now in California, here we are, it's the next day, and there are still a number of propositions and ballot measures that have unknown outcomes because they are very close.

Leo: Right. Virginia, I think, is still out there unregistered. Let's go on. Another question. And this one comes from Athens, Georgia. Bill Rakosnik writes: Thanks for your explanation about the latest updates to NoScript. I was using NoScript on a

couple of my computers already, but I wasn't using it on the family computer because my wife and children have too much trouble functioning online with scripting disabled. Sorry, Steve. After your explanation last week, I now have it installed on the family computer with scripting allowed globally. That's how I'm running it here, too. However, I've always wondered what the other updates to NoScript do.

Steve, you've used IE with scripting disabled for years. You didn't need regular updates to that feature of Internet Explorer. Why does NoScript get so many frequent updates? I currently only understand what the last update to NoScript was for. I don't understand what any of the previous updates did. I mean, scripts are on or off; right? I would have thought NoScript either disables scripting or it doesn't, and that it wouldn't need an update to block a script that it didn't block before. That would just leave updates to make sure that NoScript was compatible with the latest version of Firefox. And I know I'm getting more updates to NoScript than there have been updates to Firefox. What's the story, morning glory?

Steve: I think the problem is, I did notice sort of the same thing, a long trail of point, point, point updates and versions. I think that the author is nailing down problems that he encounters that users report. I don't know if he's writing it hastily, if it's not being tested by a large group of people, I mean, I can attest to the fact that the people in my newsgroups are a tremendous asset for all the work I do because they're able to really pound on stuff quickly. And I'm not putting out half-baked versions that haven't been heavily tested. And unfortunately, in this incredibly heterogeneous environment of all kinds of operating systems and browser versions and operating environments, there is just no way not - there's no way to get around the need to really test. And so it must be that the problems are being found, and NoScript's author is fixing that problem. Then another one is found, and he fixes that. And another one's found, he fixes that.

The other thing is, he's not doing something that is as simple as it appears. He's getting himself much more involved with the browser in order to give us the features that we're asking. So NoScript is really evolving beyond something that simply turns scripting on or off. In fact, these latest features are not about scripting being on or off. They're completely tangential. But because NoScript is so popular, he's giving us new features in this existing tool.

Leo: Almond McClain - love that name. Almond McClain in Yuma, Arizona wonders why netstat is bailing: Hello. Longtime listener since numero uno. I just noticed today when my PC was running a little sluggish, I did netstat, and as soon as it finished loading its last address it closed itself, as if it didn't want me to see it. So hit my print screen button and went to paint. Somehow I'm connected to nine connections. Time to format? I'm always running Skype and an old version of Hamachi since LogMeIn messed it up. They bought Hamachi, of course. Perhaps an old version of something I'm running is giving me issues. Why is Almond having nine connections? Is that an unusual number?

Steve: Well, it's been a long time since we've talked about netstat, the netstat command. And we have described it. I wanted to just sort of refresh our listeners, or to pick up any who hadn't heard this description. It's a very handy command built into Windows, every version of Windows, and

other operating systems, as well, that gives you a status of your network connections. So

you launch a so-called "DOS box," or command prompt, and type netstat. And it will immediately give you sort of a listing of what's going on.

Now, as to how or why this thing is crashing or closing the box, I can't really respond to that. I have no idea why netstat would run and then terminate itself. It should not have the ability to do that. It shouldn't be able. So it may be that the particular instance of the netstat command is buggy, and it's crashing the DOS box. But even that I wouldn't expect really would close the command prompt window. So I don't know what's going on there.

As for why he's got nine connections, when you run the netstat command, you'll see the status of a bunch of stuff over on the right-hand side. The word "established" is indicative of a connection, meaning that a connection has been established between your computer and another computer. And so you can look at the IP addresses and see if you recognize them. Many times you'll see 127.0.0.1 on the "from" side, and the same 127.0.0.1 on the "to" side. What that just means is that processes inside your own system are using the IP technology in your computer to talk to themselves or to other processes. So that just means a connection has been established within your own computer, not to anything outside. So that's nothing to worry about. It may very well be that that's what Almond is seeing when he talks about these established connections, is these things are just connected to themselves.

The other thing you can do is to add some additional features. For example, I use "netstat -an," as in alpha Nancy, "an" to get my normal - that's normally the way I run the command. But if you put "abn," the "b" option was added in XP. It does not exist in Windows 2000. So in XP you can say "netstat -abn," and it finds out and displays which process is responsible for each of the line items in the netstat display. And that quickly allows you to determine who is establishing these connections. Likely, I know that one of my concerns, when we talked to Alex, who is the author of Hamachi, was gee, he's got TCP connections established to every single Hamachi client running on the planet, which seemed like that would be a problem. So I do know that Hamachi will be responsible for some of those established connections. Skype may well have a static connection hooked up to Skype Central in order to perform its various housekeeping and management tasks.

But if you do "netstat -abn," you should see Skype.exe, Hamachi.exe, and you'll be able to determine what it is that is responsible for making those connections. And if you see things you don't recognize or you're surprised by, that's a great place to start in doing research to find out what's going on inside your system.

Leo: Very useful tool, netstat.

Steve: We did skip No. 9, Leo.

Leo: Oh, sorry, let's go back. More NoScript. I got confused because of all of these NoScript ones. Esbjorn Larsen in Denver, Colorado is fighting and losing with NoScript. Steve, first I wanted to thank you so much for all your dedication and knowledge. You've added to my own experience. I love NoScript, but I actually end up disabling the add-on more often than not because most sites I visit use scripting. That was my experience. It even makes the Google search page unusable, even if I specify Google as a safe site. So what are your suggestions on effectively using

NoScript? Right now my experience with NoScript is very similar to my experience with Vista UAC, which I immediately turned off. Oh, boy. Low tolerance for pain. I'm a very secure user. I work with security issues. I've never had a virus or hard drive problem, knock on wood. But I do own a licensed copy of SpinRite just in case. You and Leo are awesome. Keep up the good work. Well, if he knows what he's doing, I guess UAC doesn't matter. How do you use NoScript without having it drive you absolutely bazooti?

Steve: The reason I didn't want to skip this question was this was when I planned to confess.

Leo: You turn it off.

Steve: I've turned it off, too.

Leo: It's just, I mean...

Steve: It's running in Firefox. But I've got a little exclamation point on my little red S down there in the tray because I've enabled scripts globally.

Leo: Yup. It's just because there are so many scripts on every page. And I don't know if it's a flaw in NoScript. But it just seems like when you click yes, yes, use anything on this page, or everything on the site, it doesn't seem to remember it, and you still have to, I mean, it just drives me crazy. So, yeah, finally I use it, I'm using it like that, too.

Steve: Yeah. What I'm doing, my compromise is, if I am in a mode where I'm going to sketchy places, I mean, this isn't - this really, you know, it's not the way to be the most secure, but it's the way to keep your sanity, is I turn it on when I'm going places I don't - where I may be exposing myself to some sort of problem. And again, it's another reason that I'm very excited to have the author of Sandboxie on next week is we need a solution that allows scripting to be left on and still protect us from what websites may be doing to us.

Leo: Well, I'm glad we put this one in there, then. Because I was feeling like, oh. I think a lot of us, oh, we're bad security people. We're going to take a little break here and come back in just a bit with Sheldon, who has a simple solution, he says, for the Sockstress problem. That would be welcomed by the entire security community. And Dominik in Stuttgart, who has a question for Sandboxie's author, which will lead us into next episode.

Now, Steve Gibson, our ninth and, oh, I'm sorry, our 11th and 12th questions, starting with Sheldon Smith. He's in Apple Valley, Minnesota. He says, oh, no problem solving this Sockstress thing. First he says: Thanks for a great netcast and SpinRite. By the way, "Dr. Who" is supposed to be cheesy. I know. It's part of the

fun, the humor. Listening to the Sockstress episode and thinking of past episodes where Steve explains TCP and the TCP protocol, we're talking about an exploit based on how the initial handshake works; right? So a miscreant sends a SYN. The target servers reply with a SYN/ACK. The miscreant sends an "Oh, wait, my buffer is full." And then everything grinds to a halt.

So why can't the target have a timeout, and just send a NAC and drop the connection? If some clown calls me and says something like, "Oh, wait, someone's at the door, I'll be right back," I either tell them to call me back or wait maybe a minute, then simply hang up. If it's that important, they'll call back. Anybody would do that. In addition, don't the packets also have sequence numbers? The earlier we are in the sequence, the shorter the target system's "buffer full" timeout timer. That would be a good way to solve it. What do you think? Is that a solution? Didn't we address - I think we addressed a timeout as a solution.

Steve: Well, yeah. And the problem is there are many different ways that this problem can be solved. The problem is, none of them are in place today. So it's certainly the case that there are a number of ways that TCP could be hardened against this kind of exploit. You have the potential problem for false positives, that is, for TCP being expected to function in, for example, a patient, forever way because there are some situations where you want that, where in fact TCP by definition establishes a connection which it maintains forever. At the same time there are, I mean, all kinds of things that could be done to minimize the window of exposure to Sockstress sorts of problems. But they're not in place right now. So it's like, yes, we can certainly do things. But the point was, we need to do them. And they're not done yet. So anyway, I wanted to sort of respond to Sheldon...

Leo: He's right, the answer is good.

Steve: Yeah.

Leo: That would work.

Steve: Yeah, he's right. But it's like, okay, well, we've got to do that. And the good news...

Leo: It's on the list.

Steve: Yeah, exactly. And the good news is the guys that came up with this are getting traction now. They've got the vendors' attention. And I expect that these kinds of problems are going to get solved because they succeeded in bringing this to the attention of the powers that be that are in charge of managing the development of our core low-level protocols over time. It is just going to take a while.

Leo: And it takes so long because you've got to get all these clients to work

together. I mean, it's a complicated blanket of interacting servers.

Steve: Well, it takes a while because anything takes a while. I mean, just making a change...

Leo: Well, you don't want to break the Internet, either.

Steve: Well, and that's the other part. It's not just it takes a while. It's that the problems with side effects, you absolutely have to make sure that what you do doesn't make things worse.

Leo: Right. And finally, Dominik in Stuttgart, Germany. Dominik writes he's got a question for the author of Sandboxie: Dear Steve, I was at the edge of buying Sandboxie, really great tools. But then I read in the forums it's not working in Vista 64, for reasons the author has explained. That's a killer for me. I'm planning to switch from XP to Vista 64. When you have Sandboxie's author on your show, maybe you could ask him about his plans for 64-bit support. Great show. Haven't missed one. And I bought SpinRite.

Steve: So we will absolutely put that on the list of questions. We'll have a great episode. I'm going to talk about some really interesting details next week of the trojan that RSA Security has provided a great deal of documentation about, talking about penetration and the nature, detailed nature of the damage that it's done. And these were infections that came in through people's browsers. So that's the perfect opportunity to have Sandboxie's author on, as we will, and talk about a very nice, lightweight solution for solving this problem.

Leo: Very good. Can't wait. It's going to be fun. Steve Gibson, you're the best. Always fascinating to go through these questions and answers with you and get some insight. I think it's a really - I like that we do this every other show because you talk about some heavy-duty stuff. And so to get some clarification, the opportunity to get some clarification is valuable for everybody, I know. And I include myself in that. So thank you for doing that.

Next week we're going to talk to Mr. Sandboxie. And we thank you for being here. Don't forget you can go to GRC.com to get SpinRite, the world's best disk maintenance utility. I use it on every drive before we use it. We SpinRite ahead of time. And of course should anything, you know, we have any trouble, that's the next time it gets SpinRite. Very often saves our bacon. And, as you know, you can save yours. GRC.com to get that. And also, while you're there, that's where to get all the Security Now! show notes, the 16KB versions for the bandwidth-impaired. Steve has transcripts online there, too, which is very helpful a lot of times to read along as Steve talks. That's all at Gibson Research Corporation, GRC.com. Thank you, Steve.

Steve: And I will remind people to go to GRC.com/feedback in order to submit their questions. All the things that I've been reading from people are from people who went to GRC.com/feedback. There's a web form there. Fill it out, and I receive it. And in two

weeks we'll go through that.

Leo: Very good.

Steve: Thanks, Leo.

Leo: We'll see you all next time on Security Now!.

Steve: Bye bye.