SECURITY NOW!

Transcript of Episode #152

Listener Feedback Q&A #45

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-152.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-152-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 152 for July 10, 2008: Listener Feedback #45. 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! Episode 152. And from his bunker deep within the mountain they know as - what is the mountain in Irvine?

Steve Gibson: Saddleback.

Leo: Saddleback. Deep within Saddleback Mountain, Mr. Steve Gibson, in beautiful Irvine, California. Hi, Steve.

Steve: Hey, Leo. Great to be back with you again.

Leo: Yeah, yeah.

Steve: We're rapidly coming up on three years. I love it. 152, four weeks to go.

Leo: That's kind of neat. I don't know what we're going to do for a three-year celebration, our entry into the fourth year, but we'll find something fun to do.

Steve: Well, I read a lot of the feedback we've received from people over the last couple weeks. And it's just gratifying for them to say they love the podcast, and they want another 150 weeks, and they don't know what they would do if it stopped.

Leo: That would be bad.

Steve: We have no plans to stop it, folks.

Leo: No.

Steve: We're going to - we're just getting going. You're in a whole new era now with your studio and your staff and...

Leo: Yeah, and I'm starting to record these video versions that we do. And I don't know if Security Now! really lends itself to a video version. But if people want it, I'll be glad to do it, you know. Certainly the gadget podcast does because then you can see the gadget. And, you know, we're doing a lot more stuff in the TWiT Live realm where we have interest, like Woz is going to be on on Thursday. So those we'll probably start putting out as video podcasts here, yeah. But if you tune in live, 11:00 o'clock every Tuesday morning, 11:00 a.m. Pacific, 2:00 p.m. Eastern, 18:00 UTC on Tuesdays, you can watch us do it live. If that's not a spoiler. Might spoil the show for you.

Let's get to - before we get to - it's a Q&A segment. We've got 12 great ones. Before we do that, do we have anything to catch up on, any errata, addenda?

Steve: Oh, every week there's security news, which was the original concept you had for this podcast.

Leo: Yes.

Steve: Yes, a number of things. Over in the new exploits and problems category, I wanted anyone who is using what used to be called Microsoft's Great Plains Accounting - also known as Microsoft Dynamics. It's now called Microsoft Dynamics GP. They sort of merged them all together. Anyway, this is a very popular accounting program which Microsoft has naturally extended to make it network capable and, in the process, opened it to remote exploits.

Leo: Oh, boy.

Steve: So there are multiple, now in the public, remote code execution exploits for Microsoft Dynamics GP. Updates are available. So anyone who's using them or whose corporation is using this, you just want to make sure you've got yourself updated because the last thing you want is hackers getting into your business's accounting system and rummaging around.

Leo: No kidding.

Steve: I wanted to make sure that Mac people knew that they needed to get updated to 10.5.4 because there were some HTML rendering exploits. I think I referred to them last week. But now we're beginning to see the public appearance of some exploits, not widespread yet, but there were some mistakes found in what Apple calls the "WebKit," which are used by different things that render HTML, like Safari and Apple Mail and so forth. And also 10.5.4 fixed some bugs in third-party apps that Apple bundles in with the whole OS. So definitely want to make sure you stay current there.

And lastly, the common code base for the whole Mozilla family of browsers - Firefox, Thunderbird, SeaMonkey - have a problem. So there are updates available. So if you're using Firefox, Thunderbird, or SeaMonkey, you want to again make sure that you update those. Firefox 3.0 has the improvements that are necessary. But, for example, if you were using Firefox 2 and hadn't yet moved to 3, moving to 3 is a good thing when you're comfortable doing so. I'm always reluctant to push people into new versions. I've really learned my own lesson with Service Pack 3 of Windows XP. It's like, oh, boy, was that a mistake. But so if you are comfortable moving from version, you know, major version 2 of Firefox to 3, that's one way to solve this problem. Otherwise, make sure you're updated.

And finally - this is just, like, browser day - Opera. I just, like last week, updated to 9.5, from I think I was at 9.3. And 9.5 is a really nice sort of a .x update, not quite a major version, but a strong minor version update that changed the UI around a little bit and I think really cleaned things up. I like what Opera's doing. However, even in this period, in this little window, I was surprised when I checked on things that there's an incremental security patch to 9.5, bringing it up to 9.51. And so sure enough, when I checked, you know, I clicked on Opera's menu and said check for updates, it says, oh, you've got - there's a new update available. So Opera users want to bring themselves current, as well.

Leo: All right. Very good.

Steve: In news, the big news - and our listeners are clued in. I can't tell you how many notes I have received in case I didn't know about TrueCrypt v6.0.

Leo: Yeah, I got a few. I got a few of those, too.

Steve: And so I wanted to thank everybody for making sure I knew. This was a release on the Fourth of July, which of course in the U.S. is our Independence Day. And there were a number of new features. People who were using 5 will probably want to move up to 6. Among other things, the volume format was changed to increase the redundancy of critical information in the header. One of the gotchas, the potential gotchas of an encrypted - of any kind of, like, well, really any kind of encryption, as our listeners know, is good encryption turns data which is readable into pseudorandom noise. Absolutely, if it's sufficiently good, it's indistinguishable from pure random noise.

Well, that makes data recovery a real problem because, for example, anything that goes in and tries to read the file system, unless it's able to decrypt the file system, it can't go in and, like, find lost clusters, fix directory entry mistakes and so forth because the entire thing is just random noise. That means that an encrypted file system is more dependent on the encryption header data than a non-encrypted file system. So one of the things that these guys did in moving from 5 to 6 is they've made their volume format, the encrypted volume format, more bulletproof by putting a redundant set of headers at the end of the volume format, and a way to reliably locate that so that if the system is unable to properly read the front, it'll be able to get it from the back and use it just the same.

One of the other cool things they did, we've been talking about multi-core stuff here in the last few weeks because I've been frustrated with my lack of use of my own multi-core workstation, and then I of course built a big multi-core monster for doing media and other kinds of compression stuff. TrueCrypt 6.0 adds multi-core support for compression. And the performance gain you get is directly proportional to how many extra cores you give it. So if you have a dual-core system, the compression/decompression path will run twice as fast. And if you have a quad-core system, it'll run four times as fast. And I heard you over the weekend, Leo, on your weekend show, talking to some guy who had - I think he was buying a dual quad-core system.

Leo: Yeah, yeah. Overkill.

Steve: And it was less than a thousand dollars.

Leo: That was the amazing thing, yeah.

Steve: Coupon or something, yeah.

Leo: Is there a disadvantage, I guess is the question. If you get it for a thousand bucks, should you avoid it even so, just because of problems with the multiple cores?

Steve: Well, there aren't compatibility problems with the multiple cores. I did find myself, as I was listening to your side of the conversation, I found myself thinking, okay, well, it's got to be something has been cheated from the system. I mean, he can't have graphics that's running at high performance for that price. He probably doesn't have a really high-speed front-side bus and not high-speed memory, or not much memory. I mean, you know, that's just a really low price.

Leo: Here's the funny thing, is these quad-core chips are now about 2 or 300 bucks each. And he did actually have a decent NVIDIA graphics card, not the top of the line, but I think it was a 9800. So he wasn't suffering there. I didn't ask him about the bus speed. But I think - I don't know how many choices you have if you put one of those quad-core chips in. I think this stuff has just fallen in price.

Steve: Wow. Well, and of course you really need to provide these things with power. As I think I've mentioned, the heat sink on the new Intel quad-core, I had to literally redesign the fan mounting a little bit because it was like this huge mushroom that wouldn't fit in the case any longer because they - and they were saying, hey, we just increased the efficiency and size of our heat sink. It's like, uh-huh, yeah, and it won't fit in the case anymore.

Leo: Right.

Steve: So, yeah, so that's a downside. Oh, and the last thing is, in TrueCrypt 6, they now support a hidden OS where you're actually able to hide an OS in - remember how they used to have a hidden partition?

Leo: Right, right.

Steve: Where you could have, like, a - you could say, well, that's just noise at the end of the slack space.

Leo: They called it "plausible deniability," where it just didn't look like it was anything.

Steve: And now with 6.0 you're able to create a bootable OS in that space. Which is, you know, I'm not really sure how useful that is, but a lot of people are excited about it.

Leo: How would that work? Because you'd have to decrypt before you could boot. So they'd have to have a little decrypter stub running on the master boot record? How would that work?

Steve: I haven't even looked at it. But yes, essentially you would need to be able to boot into that optionally, but in some way that gave you plausible deniability. I just - I've been so busy I haven't had a chance to sit down and go over it. But enough people were excited, I think we'll give it a little bit more attention in the future.

Leo: Yeah.

Steve: I did want to mention that there was an interesting report, just in terms of sharing sort of reality-based security news, which is what all this is with our listeners, of course, a number has surfaced from a study that actually Dell commissioned. More than 637,000 laptops are lost annually in airports.

Leo: Airports alone.

Steve: Airports alone.

Leo: Wow.

Steve: 637,000 laptops lost every year, 12,000 a week. 67 percent, so two thirds of them, are never recovered. And users who lost their laptops were surveyed in this report. And 53 percent said their laptops held confidential data. Yeah, well, no kidding. I mean, like, whose laptop doesn't have something in it that you wouldn't want people to get. 42 percent said their data was not backed up. 16 percent said they would do - that they could do nothing if they lost their laptop traveling on business because they depend upon it. It's like their portable desktop, essentially. And 77 percent of the people surveyed said that the chance of recovering a lost laptop was less than 10 percent. So I wanted to remind people again, TrueCrypt 5 and now 6 is a robust technology which is highly recommended...

Leo: Encrypt.

Steve: ...for encrypting your laptop. I mean, it's less important, arguably, to encrypt a desktop system that's not moving around, that has no chance of becoming one of those 637,000 laptops lost in airports every year.

Leo: When they say "lost," they don't mean stolen, they don't mean somebody's ripped them off, they mean they just kind of were left behind, I guess.

Steve: Yeah, well, the report said that the two highest locations of loss was just going through the security line.

Leo: Oh, yeah.

Steve: Just the confusion. I don't know if you've noticed, Leo, but I'm feeling under tremendous pressure when I finally...

Leo: Move, move, move, move, move.

Steve: Exactly. It's like you've got to take everything apart. Then you've got to get it all through the little scanner tunnel, and then you've got to put everything back together again. And it's like, you know, there's a lot of pressure. And you can imagine how someone would just forget one piece of their little world in that process.

Leo: You'd think they'd make an effort to kind of, hey, there's a laptop here, hello, anybody?

Steve: Well, Leo, you and I travel a lot. You've seen what level of concern there is from anybody.

Leo: Ooh, a laptop.

Steve: You wonder where they're going, that's the question.

Leo: Yeah, no kidding.

Steve: In another bit of interesting news, and you may - you're clued into all of what's going on enough, you may have heard this. Blizzard, who makes World of Warcraft, has now adopted a bizarrely painted PayPal football for World of Warcraft authentication.

Leo: Yeah, somebody mentioned that to me, and I thought, that's - so when you play World of Warcraft now you can use your football to say this is me.

Steve: Now, I don't know if you can register an existing PayPal token. What I found interesting was that they are offering this at a very low price. Just like PayPal, they're trying to encourage people to use this for authentication. $6.50.

Leo: Great deal.

Steve: Unfortunately, they're all sold out.

Leo: Already.

Steve: You go to their website, it's like $6.50. Oops, sorry, sold out.

Leo: Wow.

Steve: So I don't know how many they had, how quickly they sold out, or any of the stats for that. But if we have World of Warcraft listeners, you should know that there is a way to increase the strength of your authentication using the technologies that we've talked about here many times. And it may well be, I mean, it does, it looks like the same technology that PayPal is using. I don't know, but it's worth exploring, whether an existing PayPal football might be transportable so that you'd be able to register that and wouldn't need to set up another one. I would think, I don't know, whether Blizzard is using, like, a VeriSign backend or whether they've implemented their own backend servers. It's impossible to say.

And lastly, in a completely non-security-related topic, this relates to a question that I heard you answer, again during your Tech Guy show.

Leo: You've got to stop listening to the radio show. Hey, by the way, I have a warm line I could give you. If you ever hear me say something really stupid, I'll give you this number, you can call in and correct me.

Steve: Oh, okay, well, you don't ever say that, Leo, but I don't think you - I've heard you say things...

Leo: But it's always good to have an extra opinion in there.

Steve: Well, we know I'm a media guy. I love media. So the question was, it was a question that you spent some time on during the show about - it was a guy who wanted to record Flash video. He wanted to record, like, YouTube videos. And there have been times when I have wanted to do that. And so I've searched around, I've looked at plug-ins in web browsers. I've found nothing until now which is incredibly robust. And this thing is robust because it's some serious technology which brings, you know, causes me to respect it a little bit more. It's www.wmrecorder.com, as in Windows Media Recorder dot com. So it's just www.wmrecorder.com. However, it's way more than just Windows Media. It does grab Windows Media and also Flash and many other formats.

What's cool about it, Leo, is, get this, it installs into your system the most popular Windows packet capture library, WinPcap. So what it does is, and this is the reason this thing is so robust, there's never been anything I've encountered that it can't get because it's literally installed a tap into the network interface so that it's watching all the traffic going by. And it sees anything that your system, while it's running and while you have it primed, it sees any media that your system starts to receive and pops up a little capture window and just starts sucking it in. So it's literally, it's like watching your computer receive it, parsing all the network traffic, seeing the media streams, and capturing them.

Leo: Does it save it, Steve, as a FLV file in its native form? Or is it capturing it and saving it as a Windows Media file?

Steve: It does no conversion.

Leo: So it literally saves the FLV.

Steve: It's doing a stream capture, and you end up with absolutely identical, for example, FLV files.

Leo: So you could capture the Stickam stream that we do using this, and you'd have a copy of it. That is really great.

Steve: And when I saw they were installing WinPcap, it's like, whoa, wait a minute, this is serious rocket science.

Leo: Right.

Steve: So, I mean, they've done a lot of work in order to make this thing work as well as it does. And in my experience it pays off. It's not free. I did buy it because I wanted to be able to capture stuff.

Leo: How much was it?

Steve: It's not expensive.

Leo: Let me click on the button, it'll say.

Steve: They've got a family of tools.

Leo: Do you do WinCapture, is that the one you want? Or that's the one that has - the capture is just the simple capture tool.

Steve: Yeah.

Leo: And you can get WmRecord if you want. So the full package is 80 bucks. And if you just want WinCapture, 40 bucks.

Steve: Right. I think that's correct.

Leo: Yeah. Wow, that's cool. Somebody also said that the free - and this I know you're - don't choke. Don't get mad at me. The free RealPlayer and now Real 11 apparently doesn't come with anything else, it's just a standalone, also will allow you to right-click and save.

Steve: And did you verify that? Because I thought on the show...

Leo: Yeah.

Steve: Oh, and it did?

Leo: Well, it was something about my system I think that wasn't doing it. But yeah, apparently it does. And I do - what I did verify is that you can download the free RealPlayer and not get, if you're careful about what you check, not get a bunch of extra stuff on there. It's just the RealPlayer, which I guess means Real has finally seen the light on that one.

Steve: Only took them, what, five years.

Leo: That was just awful, yeah.

Steve: Oh, in fact there are some places, for example C-SPAN will produce videos of their stuff that for a while I was watching. And it's only in Real format. Or I think maybe now it's changed. But it used to be only in Real format.

Leo: It's hard to believe that somebody in this day and age would still do that. Awful.

Steve: Anyway, so there is, of course, a set of codecs called Real Alternative that you're able to download, and it's just the core Real codecs that allows your Windows Media Player to then play Real content.

Leo: Right, right. That's probably a better way to go. Although they've clearly seen the light, and they say, oh, people don't download our stuff because we have all this extra stuff, bag and baggage we bring along. So maybe if we just give them the player. And if you're careful and you don't get the premium and the platinum and all the doohickeys with it, you just click the live free, who knows?

Steve: And then you tell it, no, I don't want these Explorer bars and add-on bars, Google desktop and everything.

Leo: Yeah, you have to be a little vigilant. Now, let's move on, Steve. First, before we have a question, do you have a fine Security Now! SpinRite letter of any kind to tell us?

Steve: Well, you know, so many people who ask questions in this week's episode refer to SpinRite and their...

Leo: Uh-oh.

Steve: I felt a little guilty putting in another little one. It's like, okay, we're going to hear enough about SpinRite this time.

Leo: All right. Well, let's get right to the questions there. This is starting off with Chris Simpson from Simpsonville, South Carolina. He says: What happens when I die? Do you have an ans- oh, no, there's more. Okay, let me elaborate. Because I just wanted to let you answer that one. Steve, I would like to have your opinion on something that's recently affected my life. In May my grandfather passed away - I'm sorry - from a completely unexpected heart attack. In the days following, my family and I spent hours hunting important financial, insurance, and medical-related information. I'm sure this is something that all families go through, but it did help me realize something very important. What happens when something like this happens to me? Being a network engineer, security plays a very important part of my job and my personal life. I encrypt virtually everything. I use TrueCrypt to encrypt all of my hard disks on my laptops and desktops. I'm trying to figure out the best and most secure way to document my encryption keys should anything ever happen to me. This is actually a really good question. I'd like to know the answer to this one.

The problem is, I don't want to have my encryption key floating around. I absolutely hate the idea of writing a password down. In previous episodes of Security Now! I remember you talking about having your attorney hold onto your CD full of information, while your mom held another. While this may work well for you, I have a hard time trusting a lawyer to hold the encryption keys to my entire life. You know, I guess I understand that. But if you have, I mean - while I certainly do trust my mom not to snoop, she's not the most security-minded person. She'd be likely to leave the information sitting around for anyone to see. I'd appreciate any ideas from the Security Now! crew or Security Now! listeners. Thanks, Steve and Leo, for a consistently great show. What a great question, Steve.

Steve: Isn't that great? I actually ran - I ran across this question a couple weeks ago and didn't have any more room for it. So I moved it down into today, the first question on today's show, because I thought it was a really good point.

Leo: Fantastic, yeah.

Steve: All of us are all, we've got everything encrypted. And the problem, of course, is if for whatever reason, it may not just be if we die, but if we're incapacitated or some tragedy befalls us of some sort, how do other people gain access to this stuff that we arguably would want them to have access to. You can imagine that this guy's grandfather, I mean, they scurried around trying to locate information that they didn't have put together. So, I mean, having some plan to deal with encrypted content is right up there with having a will to deal with the other consequences of your lack of presence on the earth.

Leo: This is something totally new. I mean, we've never had to deal with it before. But I think about this all the time, frankly. How's my wife going to find out all my accounts? They all have passwords on them. I don't even use TrueCrypt, and I think it's an issue.

Steve: Yeah. Well, now, one thing, first of all, I saw you stop in reading this where I stopped when I was reading it the first time, with this guy not trusting his attorney.

Leo: Right, right.

Steve: I just wanted to say, I mean, I know my attorney. I've got a great friendship with the guy. And, I mean, he's my lawyer because I trust him.

Leo: If you don't trust your attorney, you might want to get a better, a different attorney.

Steve: Sort of what I'm saying, yeah.

Leo: There must be somebody you trust.

Steve: Well, there are a couple interesting hacks that could be put together to essentially maintain privacy, yet not being required to trust a single person. For example, you could take a long key that, for example, is a master key to a file that's on a CD or on a floppy, if you still have that. Or it probably makes more sense to put it on a thumb drive because a thumb drive is going to be more reliable. And chop the key up into several pieces. For example, if you just chopped it in half you could give your attorney half and your mom half or your sister half or something. Now, the point is that you no longer have to trust a single person because the attorney only has half the key. He can't do anything with it unless he gets the other half from the other person. So he can know who the other person is. They can be instructed not to release their half unless whatever criteria are met. Neither do you then have to absolutely trust the other person. That is to say, it takes everyone getting together in agreement in order to assemble the full key.

And you can do, of course, you could chop it into more pieces and give it to more people. The problem with doing that is that then, if any one of these people are for whatever reason unable to provide their piece of the puzzle, essentially, the key being the puzzle, then you're completely locked out. So you can do something a little more clever. You can chop it into many pieces and then allocate the pieces so that there's some redundancy, so that one person has piece one and three and maybe five. Somebody else has, like your attorney who's more reliable, only has piece two. But you see what I mean, you could give multiple pieces to multiple people so that a subset of the total number of people would be able to reassemble the key in - of course they'd still have to have the file, so that's in a safety deposit box or something. And when they unlock that, then they've got all the other keys that you use. So you can do...

Leo: That's a good idea.

Steve: ...some simple, clever things to maintain your privacy and to make the probability of that privacy being breached very, very low while still creating some redundancy so that you're sure when you want someone to have access to this information, they're able to gain it.

Leo: One of our chatroom participants, Jmath, suggests a site called DeathSwitch.

Get this. Imagine that you die with - this is DeathSwitch.com. Imagine that you die with computer passwords in your head, leaving coworkers without access to critical files. Imagine your loved ones can't find your bank accounts or that you die with a secret you longed to reveal during your lifetime. Doesn't just have to be passwords. DeathSwitch is an automated system that prompts you for your password on a regular schedule to make sure you're still alive. When you do not enter your password for some period of time, the system prompts you again several times. With no reply, the computer deduces you are dead or critically disabled, and your prescripted messages are automatically emailed to those you named.

Steve: I love the Internet.

Leo: Is that wild or what?

Steve: What a bizarre thing. But, I mean...

Leo: It is so strange.

Steve: You can imagine there are people who are like, oh, this is exactly what I need. You know?

Leo: If you set up - now, you'd have to have some sophisticated friends. But if you knew your friend's PGP key, you could encrypt a message, save it on something, a system like this. They wouldn't be able to read it. Only your friend would be able to read it. That would actually be a secure way of doing it, as well. As long as you could use PGP.

Steve: And the one thing you would want to absolute- presumably the reason DeathSwitch has this content for you is that it has secrets you want to absolutely make sure are not released while you're alive. Otherwise you're...

Leo: You want to keep entering that password.

Steve: You want to be very sure you don't have a false-positive DeathSwitch event.

Leo: That would be pretty bad.

Steve: Yeah.

Leo: Isn't that interesting? I'm sure there are other sites. But that was, I thought, very interesting. Thank you, Jmath, for passing that along in our Stickam chatroom.

Peggy Willingham in San Marcos, Texas, wonders about blocking Phorm. Phorm was that system we talked about last week.

Steve: Oh, yes.

Leo: Oh, yes, that caused such consternation in our audience. Steve and Leo, this is probably a stupid question. I'm wondering at what level Phorm intercepts itself into your data stream and if a hosts file would bypass the process. I've been a listener for two years and have been an avid SpinRite fan since version 2. The happiest day of my life is when you created a version that supported NTFS as SpinRite v6 does now. I came to Security Now! through GRC.com and now listen to almost every podcast Leo does. Thank you, Steve. Thanks for brightening and enlightening my days. Thank you, Peggy. What a nice email. So could she just change - could she block Phorm by just changing her hosts file?

Steve: Yes. Last week's episode went long, was long in length, because I wanted to squeeze my Bill Gates anecdote in and so forth. And so I didn't want to make it any longer by talking about Phorm blocking approaches. But remember from our discussion that your browser is told to go to the website that Phorm is using, Webwise, in order to induce it to give up its Webwise cookie. If you block Webwise in your hosts file, your browser will be unable to do that. Now, that's a problem because the redirect will fail, and you'll go nowhere.

Now, they've got technology in there so that the system will learn if something has happened to cause this whole redirection dance that we described in detail last week, remember there's three different redirections where your browser is bounced around between sites or servers pretending to be the websites you're going to for the purpose of tricking it into giving up and accepting cookies in a first-party context. So you can also ask the question, for example, well, what would happen if my browser gave me the ability to blacklist cookies by domain? Could I blacklist the Webwise domain and therefore not have my browser accept such a cookie? And yes, you can do that, too. So this system is vulnerable to blocking, and it's not difficult actually to block because of the way they've implemented this. It would have been more difficult if they were injecting, for example, JavaScript into the page as they tried to for the first couple years of this, in '06 and '07. Now it's not so difficult to block.

However, the problem is, well, how does that mess things up? What happens is their technology notices something is wrong. You keeping trying to get to the same page. You never come back from a redirection. No matter how many times they try to give you a cookie, you never give it back to them. And what they do is they then put you on an "okay, I give up" list that lasts for 30 minutes. And for 30 minutes from that time, while you're on that connection, they no longer bounce you around. And so you just have normal Phorm-free access to the Internet. And then after 30 minutes they're still wanting to try to get their hooks into you, of course, so they're hoping something has changed. And whatever it is that was broken has been fixed. And so they will again intercept a web page, bounce around a little bit, see if they can now relock their tracking technology onto you. And if not, they back off again for 30 minutes, and you are Phorm-free. So there are things that could be done to block these guys. My problem, of course, is that savvy people are going to be aware of this, but the bulk of ISP users won't, and it's not an opt-in process, it's an opt-out process.

Leo: But you can, in fact, rather than changing your hosts file, a better procedure would be to go to your ISP and opt-out.

Steve: Yeah, that's a little annoying, too, because opting out means that you get a special Webwise cookie which is then, similarly, you still have the same dance. That Webwise cookie is implanted in every website that you visit so that, when it comes out, they're able to say, oh, this person doesn't want to be tracked. Well, you've already been tracked in order to have them know you don't want to be tracked.

Leo: Right. But they're not saving the information is the difference.

Steve: Correct.

Leo: Mainly I would say, if somebody starts using - is there any way to know? I guess if you see Webwise cookies, that's how you know you're being Phormed.

Steve: Ah, we've got a couple good questions about that.

Leo: All right, we'll get to that, we'll get to that. Let's get to our next question. This is from Jeffrey T. Darlington in Beckley, West Virginia. He takes a webmaster's view of Phorm: Greetings, Steve and Leo. I know it's highly unlikely I'll get this to you in time to make it into this week's Q&A episode, but I'll send it regardless.

Steve: Surprise.

Leo: He did make it.

Steve: Yes.

Leo: Surprise. I just finished listening to your latest episode, #151 about Phorm, and I thought I'd share a tangentially related experience and hopefully solicit your thoughts on the matter. I maintain a moderately popular website which has enjoyed a rather lengthy, decade-long lifespan, an eternity on the web. Unfortunately, it is largely ad supported - pauses to allow the boos and hisses to subside. Hey, we're largely ad supported. I'm not hissing. Being privacy and security conscious, I've always wrestled with this issue, but I've never enjoyed pushing ads on my visitors. But being a small-time, one-man operation means I need to make concessions to pay the bandwidth bills. While I could easily debate your statements in previous episodes about bandwidth being cheap, suffice it to say that none of my other revenue streams come anywhere near paying my hosting costs. And if it weren't for advertising I would have folded up shop years ago. Online ads are like politics. Sometimes you have to go with the lesser of two - or more - evils.

Recently I was able to change my hosting arrangement and, in the process, become truly the master of my own domain, giving me full control over what advertisers show ads on my site. I've carefully surveyed many of the third-party advertisers out there, found a few I believe to be more reputable than most. As yet I haven't run into any glaring privacy or malware issues reported by my visitors. It should be noted, however, that I make that statement with every available digit and limb tightly crossed, and maybe even a pair of eyes.

However, after listening to Episode 151 and hearing about Phorm's odd cookie-setting habits, it reminded me of some odd observations I had noticed among my own cookies. My site uses cookies for various services such as a subscription-based premium service that allows subscribers access to exclusive content for a fee. This service is based largely on the presence of a cookie which contains, of course, numerous security features to protect both my users' privacy and access to my protected content. However, upon examining the cookies in my browser associated with my domain, I've noticed several unaccounted for by any of my code or any third-party applications I've installed.

That's right, just like Phorm, some other third party, likely an advertiser, has installed cookies linked with my domain that were not set explicitly by me. Unlike Phorm, however, these cookies don't appear to be intercepted anywhere before reaching my site because they show up in the list of cookies returned to my server. Google searches for the names of these cookies have shown that they crop up all over the web in similar situations, all set to the first-party domain, but not set explicitly by that domain. To date I haven't figured out what usefulness these cookies might serve. If they were set for my domain, how would the third party that set them even read them? The cookie specification should prevent that. It wasn't until your explanation about how Phorm works that I saw the possibility of such a system working. However, I know my ISP doesn't use Phorm, and these cookies have existed for a lot longer than the Phorm storm has raged in the media. As a developer it burns my biscuits to think that someone else is polluting my domain's cookie space with junk I didn't set; as a web surfer, it annoys me even further to think somebody other than the domain I'm visiting is infiltrating my browser. Either way I'm not a happy camper. And I'm not sure that my visitors know about this. I'm sure if they did they wouldn't be too happy, either.

The thought occurred to me, I don't particularly want my visitors to be tracked without their knowledge. Assuming some third party like Phorm is inserting cookies for my domain, what's to stop me from poisoning their cookies, stirring a little of my own arsenic into their dough, so to speak? After all, if these cookies are set for my domain, I have the capability and every right to overwrite them with whatever I want. I've toyed with the thought of testing for the existence of these cookies and, if present, resetting to something hopefully benign, such as all zeroes for hex data or a common string for all users. I suspect that if the mysterious third party were then able to read these cookies somehow, all users who visit my site who previously had these cookies installed would then appear as the same person, or at least they'd get garbage in the cookie they would hopefully not be able to use.

I wanted to do some code - this is a long - let me take a breather. I wanted to do some code tests with myself as a guinea pig before sending this to you, but unfortunately I haven't had time. I wanted to get this to you ASAP in hopes it might make it to you before this week's recording session. I do plan to carry out my experiments; and, if you're interested, I could send you the results. The worst-case scenario I can foresee is that the third party and I will constantly overwrite each other's copy of the offending cookies. While this may taint the third party's data, it could also annoy the neck out of visitors who have their browser set to notify them every time a cookie is being set. I certainly don't want that. Another possibility is I might be breaking some unseen usage agreement between myself and the third party. Personally, that might be a risk I'd rather take under the banner of protecting my visitors.

I'm curious to know if you have any thoughts to share. If you're curious, I've included the cookies at the bottom of this message - oh, good, because I want to know what they are - if you'd like to investigate them further. I'll also keep you updated on the results of my tests if you'd like to hear them. Thanks for many great episodes, hopefully more to come, from an avid listener and happy SpinRite customer. So what were those cookies, Steve Gibson?

Steve: Okay, Leo. Now you can take a break.

Leo: Wow.

Steve: Yeah. I really liked his posting, I thought it was well written, and I thought it was an interesting view, that is, sort of the view of this issue from a webmaster's perspective, someone who's noticed that something is infecting his domain with their cookies. I have a sneaking suspicion that this is something he's probably put on his site without recognizing the consequences. I saw exactly this during the period of time that I had Google Analytics installed at GRC. There is something known as a client-side cookie which is distinct in browsers' minds from server cookies. And interestingly enough, servers cannot change client cookies without injecting code into the page in order to give them access to client cookies. So what's happening is, you know how Google, for example, just to use them as an example, I don't know that these are the cookies that this listener was seeing, but they bought some technology, I think it was Urchin.

Leo: Yeah, Urchin is a statistics program, yeah. That's what Google owns, yeah.

Steve: Exactly. And so if you look at your own browser's cookies for many sites, you'll see _ut something, like utm, ut different things. And this is, unfortunately, the tracking technology which anyone using Google Analytics, which is extremely popular, and maybe Google Ads - I have not looked at it closely, but I wouldn't be at all surprised if this is not similar technology. Essentially, you have links on your pages to JavaScript which comes from Google's servers. And that script runs, and it's running in the context of the page, which is to say in the context of the server that you are visiting that has hosted this page. And so script is able, JavaScript, for example, is able to set cookies as well.

And I did some experimenting with this. It is not possible for the remote server to change those cookies because its cookies sort of exist in a separate name space. They are server cookies as opposed to client cookies, client cookies being set by scripts. So it is likely that, you know, we know that this guy's site is advertising based. If the ad insertion technology is script-based rather than just link-based, that is to say, sometimes all you put is you put a link to an image on the page, and then the remote advertising server simply supplies an image that fills in the box. However, naturally we've seen an evolution of this technology so that increasingly people are putting their - essentially, advertisers require you to put some script on their page. Even VeriSign, that little "Secured by VeriSign" seal, I'm not using it in this dynamic fashion because it's script they want me to run whenever this little animated...

Leo: Oh, it's not just a little banner.

Steve: Right. And it's like, I'd like to avoid that if at all possible. And that's why, frankly that's why I removed the Google Analytics stuff from my site because I just - I felt uncomfortable inviting Google to run whatever code they wanted on my pages. It's not static code that Google provides. I provide a link to their server, which every time the page loads goes and gets the code from them. So it just sort of seemed like something I didn't want to do. But it seems very likely to me that that's probably how these first-party cookies are getting stuck into this guy's domain.

Leo: Did you look at the cookies that he sent you?

Steve: No, unfortunately he's unable to attach things...

Leo: Oh, he can't attach things, yeah.

Steve: ...on our online form.

Leo: So that's the difference between a server-side cookie and a client-side cookie.

Steve: Right.

Leo: If you have a tracker on your site, it's setting cookies client-side. Is that right?

Steve: Exactly. If you have a tracker that runs in a scripting way, it is setting client cookies. Essentially your browser's running the code there on the page that sets the cookie locally, rather than it being sent back and forth across the Internet where the remote server sets the cookie.

Leo: Okay. But from the point of view of privacy, that doesn't make any difference.

Steve: Correct. It's...

Leo: It's still a cookie.

Steve: Yup.

Leo: Okay. Number four, Gilbert Langevn - looks like there's a missing vowel here. Gilbert Langevn in Le Gardeur, Quebec, Canada. Another Phorm-mitigation idea: Hi, Steve. First, great podcast. This is my first source of information about security. Now, about Phorm. If we're using cookies allowed for session in Firefox - I'm not sure, is that a setting? - I think it would reduce the effectiveness of Phorm. Firefox could still remember that it will accept the cookies for a specific site, but deletes them when we close Firefox. Do you know what he's talking about here, Steve?

Steve: Yeah, essentially there are sort of two classes of cookies. Cookies can contain an expiration date where the cookie says keep me - telling the browser, keep me, or I am valid until the following date.

Leo: Right.

Steve: Well, so-called "persistent cookies" have dates far in the future because they want to be kept around as long as possible. There's another class of cookie, though. Any cookie that does not contain an expiration date by definition is known as a "session cookie."

Leo: Session. So it's only for this session.

Steve: It's only until you close your browser window. And by sort of universal agreement, and I've been pleased with how widely this approach has been adopted, session cookies are never written to permanent storage. They're never written to hard disk. They're only kept in RAM. So what Firefox allows, and some other browsers allow this also, or some add-ons do, they allow you to force what would otherwise be persistent cookies containing an expiration date, basically they strip the expiration date off the cookie, forcing it to be regarded as a session cookie.

Leo: All cookies would then expire at the end of your session.

Steve: Yes. And so Gilbert is very right. If you were to configure this in that fashion, for example, or if your browser allowed you to, for example, force the Webwise cookies to always be session cookies...

Leo: Ooh, wouldn't that be nice.

Steve: Yeah. Then what happens is, it always thinks you're a new person, every time you launch a new browser session. And it assigns you its random 16-byte ID and profiles you only during this one session of using the browser and attempts to serve you useful ads if you happen to go to anyone who's using its advertising service. And then when you shut your window down and start it up again later, again, you've lost the Webwise cookie. It says, oh, here's a new person, gives you a new random cookie, and basically it breaks the profiling into individual browser-length session, and which is - it allows everything to work, yet no longer term tracking is being done.

Leo: And, well, can you, is there any browser that'll let you do that? Is that unheard of?

Steve: Oh, there are allow-for-session features. We're going to be talking about cookies in painful detail here not long from now.

Leo: Okay.

Steve: Because I think it's something that has been known about for a long time, different browsers have different features, and we'll be covering those in an upcoming episode.

Leo: Great. Rick Nyman in Virginia had a clever Phorm detection idea: I love your podcast. It got me into podcasts. I listen to it on my Treo every week. He uses something called Resco News to stream it, I'm not familiar with that. That's cool, though. How about adding an HTTPS link to ShieldsUP! that will look for any unknown cookies and flag possible Phorm? Oh, interesting. The only issue is Phorm may stop setting up cookies for GRC.com in order to avoid detection. If they could figure out you were doing it, they might not let you do that.

Steve: Well, this was under the category of great minds think alike. I had posted this to our newsgroups sometime last week because it had occurred to me also that anytime a user came to GRC over an SSL connection, as we said last week, the Phorm system is unable, thank goodness, to penetrate Secure Socket Layer, SSL connections. That is to say, HTTPS, secure browser connections. And anytime someone comes to ShieldsUP!, they are briefly taken through an HTTPS session, as I also mentioned recently, in order to avoid an ISP's proxy. And in the process it avoids all of this Phorm stuff.

So what occurred to me was, the query that I receive from them for the secure page will show all the cookies, all the GRC cookies, including any Phorm cookies that may have been set by their, you know, anytime they were in non-SSL pages at GRC. And I could proactively notify visitors that they had non-GRC cookies from anywhere that GRC had not set, but something potentially nefarious had. And that's a feature that's coming.

Leo: Well, good.

Steve: And I ought to mention also that we crossed the 80 million mark in uses of ShieldsUP! It was a couple days ago. Since we last spoke we went from...

Leo: Congratulations.

Steve: We're over 80 million. And uses of ShieldsUP! is way up, too. We're running like around 95,000 individual users per day. So...

Leo: Why do you think that is?

Steve: I know that several Linuxes are now including a mention of ShieldsUP! in their, like, test your firewall, test your security sort of thing. And I just think the word is spreading, you know, it takes time.

Leo: That's really interesting, huh. We've got a Steve Bradshaw in Bobbington, U.K. He wonders how Microsoft knows so much: Hi, Steve. Just finished listening to SN-151, our last episode. You mentioned that the Malicious Software Removal Tool, or MRT, had encountered and removed two million copies of this game-password-stealing software on Windows machine. Whilst this is good, of course, how does Microsoft know this, unless MRT is phoning home to report what it does? Am I being nave here? Does XP phone home with such statistics often? If so, did I agree to this one night after a glass too many of brain tonic? Thanks for the show. I genuinely find it invaluable and am often amazed by how much I find useful in my everyday job working with IBM Power Systems and Blade Centres. Steve from Bobbington, U.K., proud SpinRite owner.

Steve: Well, this was an interesting question, so I did a little bit of research. And sure enough, in the fine print which you click on, it informs you that Microsoft will be sending statistics back to them. I did a little more digging and found the Knowledge Base article where, under the topic of "Reporting Infection Information to Microsoft," it reads, "The Malicious Software Removal Tool will send basic information to Microsoft if the tool detects malicious software or finds an error. This information will be used for tracking virus prevalence. No identifiable personal information that is related to you or to the computer is sent together with this report.

Leo: So that's exactly it.

Steve: Yup. They are doing some profiling just so they get feedback about what the MRT, the Malicious Removal Tool, is doing.

Leo: Hmm, very interesting. James in Vancouver, B.C., Canada, our old stomping ground, Steve, wonders about Phorm-induced surfing overhead, or PISO: Hi, Steve. I really enjoyed the podcast with Leo regarding Phorm. After listening to your discussion of how this tech works, I cannot help but wonder how much of a hit this will have on Internet browsing performance. This must impact the ISP's overall bandwidth, as well, yes?

Steve: Well, it's interesting. One of the reasons that they run your browser through this dance is actually to minimize, well, to maximize tracking and minimize overhead. Certainly if this was really providing or creating substantial overhead for all of the customers who use an ISP, the ISP would be pushing back on this, saying wait a minute, you know, this is going to increase our bandwidth cost more than it's going to justify itself in the money, the revenue that we receive as being a Phorm-hosting Internet service provider.

So what they've done is, by the first time you go to a site you've never been to, when you attempt to go there, you will not - the cookies for that site will not include one of Phorm's own cookies. So it'll run you through this triple redirection dance which is - actually it's very quick. I don't think most users would even notice it. But the result of that is, of course, they get the Phorm Webwise cookie from your browser, and then they use that to plant that as a first-party cookie in the site you were trying to get to. Then they let your browser try to get there again. Phorm sees that you've got the cookie and lets it go by. After that point, after that one triple redirection dance, the first time you visit a new site you will have their cookie for that site. And then there's no overhead at all. Essentially your query goes to the ISP, it sees the cookie, strips it out, and passes it on with virtually no delay. So they did do this in order to minimize the impact in surfing performance and the consumption of ISP bandwidth. The bottom line is it ends up being negligible. Doesn't make it any better, in my opinion, but at lest it's not a constant problem.

Leo: Very interesting. Let's see here. Andrew Steer near London notes it's not just PayPal that makes life awkward for people who block DoubleClick in their hosts file. In the U.K. the bank, Abbey, now uses DoubleClick link-throughs on its home page. See the lower graphics links to saving products on Abbey.com. It's becoming pretty insidious. Wow. That's bad when a bank's doing that.

Steve: It really is. I went to his link. It's www.Abbey.com. And sure enough, up comes the little happy home page for a bank. And there's an ad down in the lower right of the page that's offering you some interest rate, something or other, 6.5 percent is the number that I remember from looking at it when I was assembling these. And if you float your mouse over it and look, and you have a browser that shows you the link, sure enough, there's ad.doublelick.net and a bunch of mumbo-jumbo afterwards. Which is truly disturbing because exactly as Andrew says, here's an ad on the bank site which is redirecting you through DoubleClick and then back to the Abbey site. And I was curious to see whether the link took me to a third party, to somewhere else, but indeed it's back to Abbey. So, I mean, that's really troublesome.

Leo: Yeah, no kidding. Santiago Rivero in Miami, Florida mentions a very nice Free Pascal. We were talking about Pascal, remember, and Turbo Pascal in your Bill Gates anecdote. And he says: Steve, on the last Security Now! episode I heard you express your love for Pascal. I remember seeing a while back there is still an open source, still-supported Pascal compiler, Free Pascal. It's available at FreePascal.org. Did you give it a try?

Steve: I did not have a chance to give it a try. But I checked it out, and I am very impressed.

Leo: Oh, that's neat.

Steve: It is supported across a huge array of platforms - Windows, Linux, Mac.

Leo: Not surprised, by the way, that the open source community would do this.

Steve: Oh, and it's like state-of-the-art, syntax-compatible. It mentioned TP7, so I assumed that's Turbo Pascal 7. And there's an object Pascal version. It's also very compatible with Delphi, that is of course Borland's commercial version. And it's still alive. I think the most recent version is last month. So I think it was June of '08 that they were working on it and adding new features to it. So this is a project that is very much there.

The reason I wanted to include this is that many people wrote saying, gee, you know, I really loved Pascal. They felt the way I did. They were happy to hear me mention it and said I wish there was one, that I'd like to kind of poke around at Pascal again. So I wanted to tell all of our listeners about FreePascal.org, where there is an open source, very nice-looking project.

Leo: That's really good to know. That's really neat. I'll download it and try it. I haven't written in Pascal in ages. You know, most of the original Macintosh stuff was Pascal. If you worked on the Mac, you worked in Pascal pretty much.

Steve: Yes, in fact all of the Lisa stuff was Pascal.

Leo: That's right, yeah. Although they were basing it on Smalltalk because it was all Smalltalk originally. Chris Noble in Wellington, New Zealand, asks the Important and Obvious Question of the Week. I need a drum roll. Hi, Steve, thanks for your recent episode on Phorm. Scary, but good to be informed. The trouble is, now I want to know how to tell if this is happening. Is there a way to tell if your ISP is doing something dodgy by inspecting cookies or some other process such as header data inspection? Thanks again for all your hard work and a wonderful resource.

Steve: You know, that's a great question. And that is, I mean, and I'm sure listeners of last week's Phorm episode and the one two weeks before are saying, wait a minute, how do I know if this is happening? Well, all browsers except maybe IE, I don't think IE has a cookie viewer. There is a very good cookie viewer called, not surprisingly, IECookiesView. I think it's by the guy at Nirsoft.

Leo: Oh, yeah, he's good, yeah.

Steve: I like his stuff a lot.

Leo: He does a lot of good stuff, yeah.

Steve: Very good and lightweight. In fact, I'm using it with IE during the cookie development work that I'm doing because it lets me see what's going on. But I know that Opera and Firefox and all of the Mozilla-descendent browsers do give you, even Safari does, the ability to see your cookies. What you can do is, if you just look at the actual cookies that your browser has for a bunch of domains, you know, CNN, CNET, MSNBC, Microsoft, whatever, if something is there that is installing first-party cookies in every domain you visit, you will see a common link between all of the cookies that you've got. That is, most sites have an arbitrary cookie format that they made up. GRC is using cookies only for the sake of this technology that I'm developing, which will shortly be notifying people if third-party cookies are enabled on their browser when they come to GRC. And so I made up my own format for my cookies, my own cookie names and cookie values. And pretty much everybody does. So if you saw something that was common in the cookies that your browser had across many different websites, that would immediately tip you off that there was some common factor that was linking otherwise separate sites together, and it would have to be something like a Phorm technology.

Leo: Very interesting. Calvin, maybe not his real name because you put it in quotes, located at an international airport, recounts the Interesting Story of the Week: Hello, Steve and Leo. I'm an IT person in a medium-sized international airport, and I have a story to share. One day recently I noticed that our pool of DHCP addresses were completely used up. This is unusual as we normally have about 20 percent of our addresses available at any given time. That's not a lot. I mean, I guess he's using most of them. Upon closer inspection, I saw all kinds of computers and devices I didn't recognize taking leases from our DHCP servers. An abnormally high number of devices were iPhones, but there were also computers with names like "Johns Laptop," et cetera. Every time I tried to ping one of these devices, it was no longer attached to the network, which made it difficult to figure out their location and how they were getting onto our network. Not having any live rogue devices on the network made troubleshooting difficult. I won't go into the details of how I finally figured out the source of the problem. It turned out one of our office wireless access points had mysteriously become wide open.

Steve: Whoops.

Leo: Whoops. The WAP had been configured with WPA, and I had even used GRC's Ultra High Security Password Generator to create the key. But now the key was blank and the wireless access point was wide open. This WAP is located in a conference room that shares a common wall with the airport passenger screening area. How convenient for the passengers. It didn't take long to put two and two together and realize that people cued up for airport security screening were still attaching to our network. Because of the nature of the queuing area I don't think anyone was intentionally connecting or even realized that they had connected. It's true, I think an iPhone, if there's an unprotected WiFi access point, will just join it automatically.

Steve: Yeah, it's free WiFi while you're going through airport screening.

Leo: Yeah. Thanks, airport. They would go through the airport screening area and continue on with their life, not knowing they connected to our network. That would also explain why none of the devices were live when I tried to locate them. The problem with the WAP turned out to be that it had reset itself back to factory defaults. I didn't want to have to climb up in the ceiling to replace the WAP, so I quickly reconfigured it back to its formerly secure state. Upon restarting the WAP, it was back to default settings again. Whoops. Apparently this device, for some unknown reason, stopped holding any configuration that was given to it. It wasn't a high-end device. It wasn't low end, either. It was a business-class model WAP, Wireless Access Point. Needless to say I had to climb into the ceiling to replace it. I felt it a bit disconcerting that a business-class WAP would reset itself to factory defaults upon a failure, and that those defaults would be zero security, wide-open wireless operation.

Thanks for the great show. For obvious reasons I can't give you my real name and city. But I'm signing off with the name Calvin because of Calvin and Hobbes, my hero of mischief. Wow, that's interesting. I guess if CMOS could no longer hold memory, just out of age or something, it would have to default to the default settings.

Steve: Yeah, I guess my point is, or the reason I thought this was interesting, is that it is certainly the case that routers today are shipping with no security by default. However, this thing could ship with wireless off by default.

Leo: That would be much better, wouldn't it.

Steve: Yes. So that instead of wireless being on and all the services being on when you do a full reset, why not have the default state be wireless off so that in any situation like this where the router gets reset, it'll reset and shut down, rather than reset and open up.

Leo: Right.

Steve: So we could wish.

Leo: Yeah. I mean, you can't - any device is going to, at some point, or could at some point fail to hold its settings. I mean, that's just the nature of technology; right?

Steve: Right.

Leo: These chips sometimes just won't hold settings. So it's really what happens when it can't, what the failover is that's important. And I agree with you, it should have a much more secure failover. I understand why it wouldn't fail over to wireless on with a WPA password because you wouldn't know what the password is.

Steve: Correct.

Leo: Although I guess it could have, like, a standard one or something.

Steve: And you wouldn't want that, either, because then it's subject to a brute-force attack.

Leo: Right, yeah, because anybody could know that. Now, Steve, are you ready?

Steve: I'm ready.

Leo: It is time for our Horror Story and Fix of the Week. This is from Ruan Viljoen in Cape Town, South Africa. And he writes: Hi, Steve. In a previous episode you mentioned how important it is to make sure your router's default username and password is updated. Or changed, anyway. Luckily I had this in place but was shocked to find my router's admin interface was exposed to the Internet on my public IP, leaving it open to a brute-force attack.

Initially I thought maybe this was only allowable from, you know, accessible from my own machine on this IP. But asking a friend to login from his home proved successful. The most annoying part of all this is that my router has a setting to hid the admin interface from the Internet and only enable it on my local LAN, and this hiding was enabled. That's that, you know, "turn off WAN administration" which we recommend. Steve's recommended that many times. But apparently even when I did that, it didn't work too well.

In the end the workaround for this problem was setting up a NAT rule to forward all traffic on port 80 to a non-existing IP on my local LAN. This seemed to work. My interface is now only accessible to me. Regards from a rainy Cape Town, South Africa. Have you ever heard of this? Isn't that the WAN administration port? Isn't that what we're talking about here?

Steve: Yes, that's exactly what it is. And I was horrified to hear that there are any routers out in the world, this guy has one, that apparently ignores the setting for "disable WAN access."

Leo: Oh, that's terrible news.

Steve: So I wanted to bring it to our listeners' attention. And the first thing I was thinking, well, have a friend attempt to logon to your IP, except it's kind of hard to know what your public IP is, and maybe you don't want to expose this problem to anyone. One thing you can do conveniently is use ShieldsUP! at GRC.com to scan your service ports. And port 80 is where the WAN port will be. And unless you know you're running a web server on port 80, in which case you've already got this external port mapped through to your web server, unless you know you're running a web server on port 80, it should either be closed or probably stealth. You should not see port 80 open. And if by any chance port 80 is open, and you're not running a web server, then it's your router that is, unfortunately, accepting connections on its web port from the public internet. And you definitely don't want that to be the case, especially if it's serving up your login page, which would then allow anybody to sit there and try to guess what your username and password was. And of course that makes it doubly bad if you have left them to their default settings.

Leo: Right, right. Wow, I'm shocked. You know, I guess it means that those of us who use wireless routers and have turned off WAN administration might want to test this to make sure that we've got it set up properly.

Steve: Well, yeah, that's my point is, in fact, I would ask our listeners...

Leo: I'm going to try it.

Steve: Yeah. If they haven't gone to ShieldsUP! and made sure that port 80 is closed...

Leo: So that's all you had to do was just go to ShieldsUP!.

Steve: Yeah, just use ShieldsUP!. It'll show you...

Leo: You don't have to try to login or anything.

Steve: No, you should not have port 80 open. This guy would have had port 80 open, which is how his friend was able to go to his IP and bring up his login page. ShieldsUP! would show you that port open. But I wanted to ask our listeners, if we have any other listeners who encounter this problem, please go to GRC.com/feedback and let me know and put something in the subject line so that I'll be sure to see it. Because I would love - this individual did not tell us what brand of router.

Leo: Yeah, we want to know.

Steve: And it's like, whoa, this is a serious problem.

Leo: I'm going to go there right now. I'm using a Linksys. But I'm pretty sure, I'm pretty sure I don't get my port 80s open there. I mean, I would have noticed that. I always use GRC's ShieldsUP!. GRC.com, that's the place to go, not only for ShieldsUP!. I'll actually run my - if you do common ports, port 80 will be in there; right?

Steve: Yeah.

Leo: Yeah, I'll run that right now, just check. And while I'm doing that - oh, whew, it's stealth, whew - I invite you to go to GRC.com not only to do that. Everybody do that and let us know if you find a router that doesn't comply. Make sure you have WAN administration turned off, though. And then you'll also go there to get show notes, 16KB versions of the show - Steve makes those available for people with limited bandwidth - and some transcriptions, too. Elaine does those, and that's a great way to follow along. GRC.com. And it's Steve's site.

And by the way, while you're there, get a copy of SpinRite. It's a great tool for maintaining - it's THE tool for maintaining your hard drives and often very useful in data recovery, too. SpinRite from GRC.com. Steve, it's been a great 12 questions. What are we going to do next week? Got something planned?

Steve: Well, yeah. We're going to do our last show talking about this problem with ISP spying nightmares. There's a neat guy who's been very active over in the U.K. who has really - I think I mentioned he sent you email, he sent email to my office, he posted it in our user group news server, he's on the inside of sort of the whole social, political, legal battle going on about Phorm. And I thought it would be fun to have him on as a special guest since he really knows from the front line what's happening. And I'm going to talk then also a little bit about NebuAd, just because it turns out it's bad, too, and it's another one of the really obnoxious companies that are inserting their technology into ISP facilities.

Leo: Right, right. Well, I look forward to that. That'll be Episode 153, and it'll be up on next Thursday, a week from today. If you want to watch live, we actually do these live on Tuesday, and you can watch it live at TWiTLive.tv. We do it at 11:00 a.m. Pacific time, that's 2:00 p.m. Eastern time or, let's see, 18:00 UTC. And so you can watch live, and chat in the chatroom, and I watch the chatroom sometimes and get some suggestions from there, too. And you can see Steve's smiling face, which is the whole reason to watch live. Look at that. Hey, thanks, Steve. We'll talk again next week on Security Now!.

Steve: Thanks, Leo. Talk to you then.