Listener Feedback #89

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-242.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-242-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 242 for April 1st, 2010: Your questions, Steve's answers #89.

It's time for Security Now!, the show that covers everything you need to know about keeping yourself safe online. I hope my wife's listening today. [Laughter] Episode 242, a question-and-answer episode with Mr. Steve Gibson of GRC.com. Hi, Steve.

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

Leo: Starting a little late today because we had a crisis at the Laporte household, Casa Laporte. Jennifer got an email, a panicky email from her gardener, saying - he's actually building some raised beds for us, really nice guy. We met with him, and he sent us a bid via email, and so they're in email contact. And the email came and said - it was kind of puzzling because it was a little ungrammatical and strangely capitalized. And his - it was signed with his last name, not his first name. And it said that he was in England, and he'd been robbed at gunpoint, and he'd lost his passport and all his - his billfold and all his money, and could we please send him $3,279 to cover his hotel bill so he could come home.

Steve: Wow, that's a lot of money to ask for.

Leo: Yes, considering we barely know the guy.

Steve: Yeah.

Leo: But Jennifer, of course, said to me, "Well, this is about what we owe him for the raised beds, so I'm going to send him the money." I said, "Whoa. Have you learned nothing from me?" And so I'm going to make her listen to this show from now on. But...

Steve: Well, it's funny, too, because I just this morning, when I was running through the mailbag and sort of catching myself up on various newsletters talking about security things that have happened, I ran across exactly this report, that is, that this is what's going on, is that people are - bad guys, when they break into someone's email account, they rummage around in their inbox and outbox for any clues about where they're physically located. Then that gives them some context for emailing money requests to people that this person whose account they've broken into knows.

So, I mean, it's exactly what happened to Jennifer is now something that is going on, is becoming a widespread attack because it's social engineering. And of course we've talked about that often. So it's using some sort of break-in to get into the account, then social engineering in order to trick innocent bystanders who know the person whose account's been hacked into giving them some money. And they make it sound believable because by reading the history of email they can figure out who the people are, what's their relationship, where - like, create some context for themselves. So...

Leo: Yes, it was very credible, yeah.

Steve: Yeah.

Leo: Although still misspelled.

Steve: And unfortunately something like Gmail, where you get to, by design, you get to retain all of the communications that you've had, well, think about that, over the years how much accumulates. And if you were to get into someone's Gmail account, you know, if you spend enough time, you can pretty much assemble a person's life and really generate some context for creating believable social hacking.

Leo: Yeah. Well, I wasn't sure. I was trying to figure it out. His email came from his AT&T account. And I thought, either he's been hacked or, as you say, his email's been hacked. I think, you know, where most of this happens these days, we were just reading about the French hacker who said he hacked Twitter. And he said it's not really a hack. He guessed the secret questions. That seems to be the soft underbelly of security right now is those secret questions. My suggestion is to do what I do, which is lie. So it says what's the name of your first girlfriend, and I put the name of my first dog in there, something like that, you know. Because especially nowadays, you can find out a lot about people just scouring around online. All you need is to get those answers to those secret questions often, and they'll give you a new password.

Steve: Yeah.

Leo: All right. That's my little security update. Let's get to yours.

Steve: So it's April 1st, April Fool's Day. I'm not doing - I'm not pulling any April Fool's Day jokes.

Leo: Let's state that.

Steve: This is straight up Security Now!.

Leo: I hate April Fool's because you never know what to believe.

Steve: Yeah.

Leo: So there's nothing in this show from Sloof Lirpa or whatever. You know, Dvorak always does the column that quotes a press agent named Slirpa Loof or something like that. No. Nothing - anything you hear here is real; right?

Steve: Just look elsewhere for your April Fool's nonsense.

Leo: We do have some great questions and answers. And before we get started, let me just quickly welcome Citrix back to the show.

Steve: Yay.

Leo: Steve Gibson, we have, I'm sure, a few things to talk about in the security news.

Steve: Yup, there's some news in the security world. And I just couldn't stop reading my in-bag, my mailbag this morning. I just - I kept reading them, and it's like, oh, we've got to have that one. And oh, we've got to - so we ended up with 12. So we're back...

Leo: That's fine.

Steve: We're back to a dozen. But some of them are quick and just notes and comments and things. So, but lots of really good stuff.

Let's see. People may have noticed by the time they're hearing this that there was an out-of-cycle patch from Microsoft. We discussed several weeks ago whether there might be, and I was guessing back then, it's like, oh, this is so bad, I don't know if Microsoft can wait until the second Tuesday of April. And sure enough they chose not to. This was the iepeers.dll problem, which was a zero-day flaw which affected IE6 and IE7, but not

IE8. So it turns out that it was being extremely heavily used on the Internet, and Microsoft decided, nah, we can't responsibly wait until, well, it would be another two weeks from now till April 13th. So they pushed out what is essentially their cumulative update for IE, which covers all of from IE 5.1 through IE8. So they fixed another nine vulnerabilities while they were at it. So that happened on the 30th was when that became available. So people may notice their little Windows Update yellow shield in the toolbar and think, wait a minute, what's going on? Well, that's the story.

So I'm glad Microsoft did this. They really had no choice because this thing was - this was a typical, what we're seeing now, so-called "drive-by web vulnerability" where just getting someone to bring up a web page would allow malicious code to be run in your machine. So once again, that's been fixed.

Also, when I turned on my Mac, which I do once a week for the show because that's where I run Skype, I got news of an update. And it's like, oh, sure enough. Well, the fun thing was, iTunes was being brought up to v9.1.

Leo: For the iPad.

Steve: Specifically, yes, specifically to synch with my forthcoming iPad, which currently seems to be stuck in Louisville. I was saying to you before we began recording that it left three - or it bounced through a couple cities in China, then briefly seemed to be in Louisville for customs clearance, then went up to Anchorage, Alaska, spent the night there, then came back to Louisville, which is where it currently is. So...

Leo: I remember this happening with my 3GS, as well. That's pretty funny.

Steve: Yeah. So, and you're tracking yours, as well. So, and I was thinking briefly that, oh, maybe if it's nearby, I'll be able to get it sooner. But I guess no. They're, like, all set up to deliver on Saturday.

Leo: Yeah. In fact, I talked to somebody whose friend is kind of a high-end delivery guy for UPS, I can't remember the town. And he has lined up 100 Saturday deliveries of something. [Laughter] So, you know, I think it's pretty, you know, they do this all the time. If you look at your tracking, it will say "exception" or something like that. And "held." And then it'll be...

Steve: Right.

Leo: But, you know, it's funny because people get all freaked out thinking, oh, no, this is something bad has happened, because maybe you saw there was a news story saying a company had sued the - asked the ITC to hold the iPad back. That's not what's going on. This is normal. Apple says to the UPS folks, hold this for Saturday delivery.

Steve: Well, and it's good, too, that they're not - that they're ahead of the game in terms of delivery. Because how upset would we be, Leo, if it didn't actually come on

Saturday?

Leo: Yeah, no, exactly.

Steve: We're like - it's like, wait a minute. I would have done store pickup if I didn't think I was really going to get it on Saturday, so.

Leo: You know what's fascinating is this whole drop-ship from China thing. If you order a cable from Apple, you really don't even buy it from Apple. A third-party makes it, delivers it, and ships it. And Apple never even sees it. And I think that this is kind of the very interesting kind of just-in-time way that we work nowadays. So it's not shipped from Apple. It's not shipped from an Apple store. It's shipped from the factory in Shenzhen, China.

Steve: Yup, that's exactly where mine originated.

Leo: Yeah, yeah.

Steve: So also OS X got a big update. I mean, the iTunes update was 100+ meg, like I think it was 101MB, for synching with the iPad and also to support the new iBooks store, both of those features. And OS X has now moved to 10.6.3...

Leo: This was a big update.

Steve: Yes. 436MB. And as this thing was downloading, I was thinking, where would we all be if 436MB wasn't just something we could casually do? It's like, oh, fine, yeah, update now, you know. I've got an...

Leo: That's half a gig. It's like a whole new operating system.

Steve: It's huge.

Leo: It is the largest, I'm told now, the most security patches Apple has ever shipped, I mean, by, like, two, order of two. I mean, it's amazing.

Steve: Yeah. Yeah. Well, and they didn't patch little things. They said, oh, just give them a whole new one.

Leo: Right. Easier to do that.

Steve: Yeah, exactly. I also did want to mention, speaking of people getting their email

accounts hacked, and specifically Google being a typical target, as of a couple days ago Google has added a new feature to Gmail which our users and our listeners may want to look out for. If you log into your Gmail box and notice a red bar, sort of a banner running across the top of your inbox, that's a new feature where Google will alert you to what it considers might be suspicious activity on your account. From the Google blog talking about this, they said now - I'm quoting. "Now, if it looks like something unusual is going on with your account, we'll alert you by posting a warning message saying, 'Warning. We believe your account was last accessed from ... along' - well, and they fill that in - 'along with the geographic region that we can best associate with the access.'" Clicking through that banner, and there's like a link as part of it, will deliver a log of your prior logon dates, times, and IP addresses.

So, and apparently, elsewhere I was reading that essentially their logic is, if you log in from one country and then a few hours later log in from another, where it's unlikely that you've actually made the journey in that period of time, they'll say, okay, hold on a second, this - and maybe, I mean, and I imagine that's a relatively lax period of time. Basically, if you appear to be country-hopping, they'll just say, are you really? Or is this something bad? So that's a nice feature. I'm glad that they've added that. And I think it's the kind of thing, I was thinking, well, how many users are going to understand how to, like, what this log means of their prior logons? Well, certainly our listeners will.

Leo: Oh, yeah.

Steve: And getting a list of IP addresses would be very cool. So I think that'll be a nice feature.

Leo: And you can log that other machine out, which I think is really - is nice.

Steve: Uh-huh.

Leo: You can say, I don't know who that is, but get them off my...

Steve: Well, and then you go - you're immediately going to want to change your username and passwords and so forth.

Leo: Right, right.

Steve: Making sure that there's nothing evil in your machine that might be watching you do that.

Leo: I think this is so great. I mean, this is just brilliant. I mean, I'm so glad they're doing this.

Steve: Yes. It's being proactive, which I think is really good. And there was an interesting study by an outfit we've talked about a couple times, an outfit called Beyond

Trust. They did a study to look at the - sort of to retrospectively look at what admin rights would have done for Windows 7 since it had been created in the past. They determined that of the 190 vulnerabilities published by Microsoft last year, in 2009, restricting administrator rights for users, and so if users were doing what we should, which we all sort of know we should, but it's a pain so some of us don't, you know, running as a normal rights user and only using admin account rights when you're installing software and so forth, all vulnerabilities in Microsoft Office would have been avoided.

Leo: Whoa.

Steve: All vulnerabilities in IE8 would have been avoided. 94 percent of all vulnerabilities in all other versions of IE would have been prevented.

Leo: That's kind of amazing.

Steve: I know. And 64 percent of all other Windows vulnerabilities. So would have been bypassed, would have not been a problem. So I'm thinking, okay, it's annoying to do that. But boy, what a benefit. So I would say, especially to people who for whatever reason have a history of getting themselves infected...

Leo: Like Jennifer and my mom.

Steve: Yeah, exactly. I mean, frankly, we've spoken, you and I, Leo, we're very careful, knock on wood. I mean, I just - it's funny because somebody, in fact, in one of our Q&As today, they made a comment. They wanted to give me a link. And they said, Steve, I know how you're reluctant to click on things in email. And I said, no, not reluctant.

Leo: I don't.

Steve: No force on Earth could make me click on a link in email. So "reluctant" doesn't begin to characterize it.

Leo: Not merely reluctant. It's uncooperative.

Steve: I just won't. I mean, I can't think of a good reason ever to do that. So...

Leo: Let me ask you this, though. Because it was my understanding, we've kind of gone back and forth on this, that in current versions of OS X and Windows 7, that even if you're an administrative user, you still have to kind of explicitly say I want to do this. But you don't have to enter the password, but you still have to say, yes, I know what I'm doing here. Right?

Steve: You have to sort of - you have to do the user account control.

Leo: So you're not really - you don't have full administrative privileges just kind of out of the box, which means no virus would, either. Even if you're logged in as an administrator.

Steve: Yeah...

Leo: And that's what puzzles me. I know in older versions of Windows that's true.

Steve: Yeah. And I think I'm going to probably follow this down because I'm curious. I mean, I'd like to give our listeners a solid understanding of what this means because...

Leo: Yeah, because I had been saying all along, be a limited user. Do not be a full user. You'll be safer. Yes, it's a pain, you have to - but then it was my understanding that the new, like starting with Vista, I think, and OS X...

Steve: Well, and remember, because the way Vista worked was, when you logged in, you were given a pair of accounts. There was actually a dual login. And so you were running with restricted rights normally. And then when you said - when you did the UAC...

Leo: It would elevate you.

Steve: ...elevation, it would actually switch over to an admin set of credentials that allowed you to proceed with that operation. So, you're right, I need to look more closely at their report and understand why that isn't enough. Because they're saying that isn't enough, that you need to actually be a limited user who doesn't have - presumably who doesn't have the option of, like, installing device drivers and installing stuff. But you'd think, okay, well, does that mean that the whole UAC dialogue is being ineffective? Or maybe they're just assuming people click and say yes all the time.

Leo: That's probably, I mean, yes. If you escalate, of course, or elevate, then of course you're going to have a problem. And it's probably true. People just go yeah, yeah, yeah, whatever. I - yeah. Do it.

Steve: Well, I did have an interesting news flash, not surprisingly about SpinRite v6. It's been approved for use by the U.S. Army.

Leo: Congratulations. What does that mean?

Steve: Yes. I don't know. John Galliano, looks like, I think that's how I would say his name. He said, "Steve, thank you for your wonderful product, SpinRite. I've used your

product for many years now and am such a believer in SpinRite that I recently submitted the product for approval Army-wide by IT Specialists," which is a group I guess within the Army because he capitalizes it. He says, "It passed a tough evaluation with ease. I look forward to purchasing four copies for my unit's use." So he'd be getting a site license by purchasing four copies. He says, "Thanks to you and Leo Laporte for your five wonderful years of Security Now!. Your netcast is by far, hands-down, the best one out there. Congratulations on the award."

Leo: Yay.

Steve: So that's very cool. SpinRite formally - and he sent me a PDF, which I opened very carefully because it was an attachment to email, but I knew where it came from in this case. And it says, under "Factors," it says "Recommendation: Approve." And it said, "Background: Gibson Research Corporation, SpinRite, GRC SpinRite 6.0, is a software program for scanning magnetic data storage devices such as" - this is like an official Army, like, document that I'm reading - "such as hard disks, recovering data and refreshing their surfaces. SpinRite tests the data surfaces of read/write magnetic disks including IDE, SATA, USB, floppy, zip, and others, by analyzing their contents and will refresh magnetic disk surfaces to allow them to operate more reliably. SpinRite attempts to recover data from hard disks with damaged portions that may not be readable via the operating system or other utilities."

And then under "Facts" - that was "Background." Under "Facts" it says "SpinRite will be utilized on machines" - I don't know really what this means, but it says "not connected to the LandWarNet to aid in the troubleshooting, repair of hard drives, and recovery of data from failed hard drives. For machines connected to the LandWarNet, SpinRite will be utilized in a preventative maintenance mode only."

So of course that's good because you could run SpinRite on those drives to keep them from failing, which SpinRite really does a good job at. And then whatever the LandWarNet is, I guess they take the machine off of that if they want to run SpinRite in a post-failure, data recovery, bring the drive back to life mode. So anyway, that's very cool.

Leo: All right, Steve. I have, if you are ready, a dozen questions. We're going to power through these suckers.

Steve: Yay.

Leo: Are you ready?

Steve: I am.

Leo: Question #1 from Jon Hatfield, Indianapolis, Indiana. He says no, it's not fixed. I just listened to #241, last episode, and I was thrilled to hear you bringing up the mouse scroll wheel bug in Firefox, saying it was fixed in 3.6.2. Well, it's been bothering me several weeks since I upgraded to 3.6. Sadly, I have to report that the

problem is not in fact fixed, at least for me. I tried turning off KatMouse, which is that great program you recommended. And tada!, the scroll wheel works. So it's a problem with KatMouse. Turns it back on, breaks it again.

He says: Not having the scroll wheel has caused me no end of frustration. But for the interim, until this bug is fixed, I'll be able to scroll by turning off KatMouse. I searched Google for it, and until listening to last week I had no fix for this problem and was prepared to revert back to an older version of Firefox. So thanks, as always, for the great information. SpinRite 6 owner. I've used it eight to 10 times to recover aging TiVo hard drives. Oh, that's a good use for SpinRite.

Steve: I do it often, too.

Leo: Yeah. Also I've been a listener since the second or third episode. Keep up the good work.

Steve: Well, I just wanted to report this to our listeners, since I had believed that 3.6.2 fixed it. And I have to say, Leo, when you had the experience of that MX Anywhere Logitech Mouse with the zero friction....

Leo: Oh, I love it.

Steve: ...scroll wheel. Oh. And I would revert to Firefox 3.5 rather than give that up. I mean, it's sort of a pain to turn KatMouse off and on, like you'd have to turn it off apparently in order to get scrolling because apparently 3.6.2 will do that for you, although you'd probably have to - the cool thing about KatMouse, just to remind people, is that it sends scroll messages to the window your cursor is over, which is different than the window that is "activated," as Microsoft calls it, the topmost window, the one that's kind of lit up with the title bar emphasized, the idea being that it allows you just to scroll anything, you know, any window that the mouse is hovering over.

So it's just, you know, scrolling in web pages is certainly important. When you've given the focus to Firefox, any version of Firefox, spinning the wheel will quickly scroll the web page. But it's nice to have KatMouse because it does that universally. But apparently something in the way Firefox is working is conflicting with KatMouse such that Firefox doesn't see KatMouse's scroll messages the way it normally sees the wheel - scroll messages without KatMouse. So I did want to let people know that apparently, though it works for me - that's the other thing that's strange. I'm wondering if there may be some difference in add-ons which is causing a problem, if one of the add-ons maybe that Jon has is responsible for this problem.

So I would say to him that, you know, it definitely is working for me on several different laptops. It's working for Greg, my tech support guy. Both of us briefly had this experience of it not working, and now it is again. So it could be that there's an add-on conflict. I mean, I'm trying to think what's the difference between my version of Firefox 3.6.2 and Jon's. And certainly the collection of add-ons that we've chosen to run could be different between those two. So maybe that's it. Anyway, if I didn't have it, if it didn't work like that, I'd be back at 3.5. I'd just kind of camp there for a while and wait for 3.6 to get it fixed, so.

Leo: You have to think it's something that KatMouse is doing that maybe is nonstandard, as opposed to being a Firefox issue. But I don't know.

Steve: Well, except it worked under 3.5.

Leo: Right.

Steve: So...

Leo: That's why - it's why it's so difficult to debug software in an environment where you have multitasking and multiple processes going on.

Steve: Oh, and Leo, it's why GRC's newsgroups, with the listeners, I mean, with the audience that we have there, when I was doing the DNS Benchmark...

Leo: So handy.

Steve: ...I was able to do a version and say, okay, gang, kill it, pound on it, jump on it. And many of the guys, for example, were Linux users who were using Wine, which I wasn't living in. And they said, oh, well, that kind of - this went sideways there. It's like, okay, I'll go fix that. So, I mean, it's just incredibly valuable. But it's no longer the case that, if it works for you, it'll work for everyone.

Leo: Right.

Steve: As a developer, you really do need a large audience to give you the feedback.

Leo: And that's why Microsoft does these big betas; right?

Steve: Yes.

Leo: Question #2 from Trevor Awalt, who wrote to GRC's tech support email about something he noticed. Trevor writes: I'm using Wireshark on the - that's the old Ether, what was it called? It's a packet sniffer.

Steve: Yes.

Leo: On the PC, Dell XPS 9000, da da da da, i7, while doing a DNS Benchmark test in order to understand exactly what you were doing. He wanted to sniff your

packets.

Steve: Yup, he was.

Leo: I was just wondering if you'd noticed that in all of your queries the IP header checksum equals zero. Is that on purpose? Even though this is the case, the DNS servers seem to respond okay. Oh, this is a good - this is interesting. Well, is that intentional? What happened?

Steve: I thought this would - may be something that other of our listeners had seen. And it's a cool and interesting feature. I'm just using for the DNS Benchmark - not doing any fancy raw packet stuff. I'm just using the regular UDP technology, the UDP stack in Windows, and sending out packets. So in this case, although for example on the GRC server, where I'm doing all kinds of fancy things, I'm building the packets myself and sending them out through a raw interface, so I am doing things like setting IP header checksums and all that. In this case, running on a regular Windows client, I'm not doing that.

So the stack is sending packets down to the NIC, the Network Interface Card, with their IP headers left zero. The reason it's doing that is the NIC has said, we have hardware IP checksums. You don't need to do it. When you think about it, a checksum on a packet is a relatively expensive thing to do because it requires that you essentially scan the entire packet and sum up all of the 16-bit words which occur and apply the standard IP checksumming algorithm. So to do that takes time.

So a new feature of many of the latest NIC hardware is that the NIC chips will do that on the fly. That is, it's impossible to send out a bad IP checksum. And there's no reason you would ever want to because, I mean, it would die at the first router that it came to. Anything that checked that for integrity, that's what it would look for in order to see that - if there was a transmission error. So there's no even tricky, hacky, fun way to, like, there's no win in deliberately messing up the checksums in TCP/IP packets. So you can't send out a wrong one.

Well, what's interesting is that Wireshark, where Wireshark sticks its little shim to sniff is right in between the stack and the network interface card. So it's seeing the packets go by with no checksum set. Essentially, the device driver has given Windows permission not to bother, just do not bother with that. We'll take care of it. So what's cool is that the hardware, with zero overhead, does that for the software as the packet is leaving it on its way out the wire.

Leo: Hmm, interesting.

Steve: So that's the answer, yeah.

Leo: Wireshark is kind of fun. You can see what's - you actually are looking at the traffic as it's going out, so you see all sorts of interesting stuff there.

Steve: And we have a not-so-fun one about that coming up here.

Leo: Oh, all right.

Steve: Yeah.

Leo: Curtis Clark in Sayreville, New Jersey with Question #4. He wonders about IP network addressing. He says: Steve and Leo, I have a question regarding the difference in IP addresses for my home networking devices. Recently I purchased a new wireless router for my home. The old router uses that 192.168.1.X IP address distribution. The new one uses 10.0.0.X. I use a NAS as a local backup. And before you ask, Leo, I use Carbonite for offsite backup - a good combination, actually. And I manually gave the NAS a fixed IP address of 192.168.1.20 so that I could always get to its web portal using the same destination IP address.

Of course when I switched from the old router using the 192 scheme to the new router using the 10-dot scheme, I noticed I could no longer access the NAS at its IP address. So I switched back to the old 192-dot router and changed the NAS's fixed IP address to 10.0.0.20, then switched back to the new router. Everything worked. But that made me think, why couldn't I still access the NAS at its original fixed IP of 192.168.1.20, since it was right there sitting on my network? And since I couldn't access it, couldn't this somehow be used for some kind of, I don't know, access security? Steve?

Steve: It's a great question. So he basically changed his network from - because as he evolved his router, he went to a new router, he changed it from a 192.168 network to a 10-dot network. And so he's asking - , but the NAS was still set with that fixed address originally, 192.168.1.20. It's, like, there. So why can't he still get to it, because it's right there on his network?

Leo: Right.

Steve: The answer is kind of cool, and it explains how this aspect of networking and masking and submasking works. The idea is that, when you have a network, a local area network, whether it's 192.168.1.X or 10.X, essentially there is the network address, which is those numbers, and then there's the subnet mask. What the subnet mask does is it specifies which IP addresses are on that local network. And any that are not are assumed to be somewhere else. They're not on the local network. They're elsewhere.

And so what happens is, when - remember that we're always talking about Ethernet networks here. So the actual way packets are addressed is with MAC addresses, which are the actual physical addresses of the interface cards on the Ethernet. The IP addresses are just sort of a - they're a convenient way for us mapping these IP addresses to the MAC addresses. But it's actually the MAC addresses that is the actual way packets are sent from point to point.

So what happens is, when he was at his computer, which was now in a 10-dot network, where anything beginning with 10 was regarded as on the local area network, and he tried to connect to 192.168.1.20, the routing system in his local computer's network

said, does this address begin with 10? If it begins with 10, it's on the LAN. If it doesn't, it's not. And when it saw that it didn't begin with 10 - and literally, the part of the subnet mask which has ones in it did not match the numbers of his network. That was the logic used. And so it said, okay, this is not on the LAN. Send it to the gateway. And so even though the IP address was physically a device on his network, he'd sort of moved his network out from under it.

And so by definition, if it's not local, it's remote. And if it's remote, you send the packet to the gateway, and now it's the gateway's problem. It's sort of like you've discharged your responsibility. It's now the gateway's problem to send it on to wherever it goes. So that's the end of the mystery. And as for could this be used as access security, well, not really because that device is there on the network. It is at that IP address. And if you made a change, for example, to your routing table in the computer, where you said this particular IP is local, then that would override this decision, and you could still access it, even at a funky IP. So it's there. It's ready to receive traffic. But it's just at the moment it's sort of been softly excommunicated, but not really hard excommunicated. You could get to it if you wanted to.

Leo: All right. Now it's time for some comedy relief. An anonymous listener, subject line "Sunbathing au natural." Steve, I finally got back to listen to your Vitamin D episode. By the way, some 'flu has been going around, Steve, and I doubled down on my vitamin D. I was worried initially about overdosing. This is not the letter, this is me talking. And I just read that just sunbathing for 15 minutes is like, whatever, is 10,000 units or something.

Steve: I know, yeah.

Leo: So I'm taking, like, 2,500 units. Which is probably not - I don't even know if it's therapeutic. But I haven't gotten sick.

Steve: Well, I've avoided - I'm getting constant...

Leo: I know, you're not making a prescription. You're not a doctor.

Steve: No, no. I'm going to say I have avoided talking about this all the time. But there is - it is really becoming an issue in the news. There was an article last week that talked about where they've actually discovered at the molecular level how T cells, which are immune system cells, put out a little VDR, that I talked about in the podcast, a Vitamin D Receptor, and require Vitamin D in order for the T cells' immune function to activate. And without it, it doesn't. And so they're beginning to understand increasingly how important Vitamin D is to things like immune system function.

Leo: Interesting, interesting.

Steve: And there's been, like, studies that have showed that - there was a study with school kids where their incidence of catching the 'flu, this was between '08 and '09, was nearly cut in half by Vitamin D versus a placebo. So it was a double-blind, placebo-

controlled study that said, I mean, that really demonstrated that kids didn't have enough Vitamin D. And when they were given some they got, like, the incidence of them coming down with the 'flu was cut nearly in half.

Leo: Wow.

Steve: And interestingly, asthma nearly by one sixth, that is, one-sixth the instances of asthma...

Leo: Holy cow.

Steve: ...versus not.

Leo: Holy cow.

Steve: So, yeah, I know. I just...

Leo: Well, purely anecdotally, I just haven't been sick since I started taking more Vitamin D. It's been great.

Steve: This is a security podcast. I want to keep us on that. But...

Leo: Well, and this has nothing to do with that except that he was listening to the fact that you were sunbathing in the nude.

Steve: Ah, okay.

Leo: As a test to see whether you could get enough Vitamin D the natural way.

Steve: Right.

Leo: He says: I had a friend who used to slew the NSA satellites around in some secret basement facility. And I asked him if it was really possible to read your license plate from outer space with them. He laughed out loud and told me, "Number eight font." He said you could look over someone's shoulder and tell what he was reading in a newspaper. They could read down to a font size of eight points. He said, "This is 15 years ago."

Steve: Wow.

Leo: So being aware of the surveillance laws, I asked, "Do you guys turn this off when the satellites pass over the U.S.?" He said no. In fact, he said, they knew the location of most of the nudist camps in the country. Sunbathing au natural has never been the same since. Just a word of warning.

Steve: Yeah, Big Brother may be watching, but he probably doesn't want to see what he does.

Leo: [Laughing] I don't - yeah.

Steve: Exactly.

Leo: Exactly. I wouldn't worry about it.

Steve: Yeah. The nudist camps that I've been aware of anecdotally, never been to one, but they don't look like places where one gets very excited about going there.

Leo: No, no, no, no, no.

Steve: No.

Leo: Here's Question #5. Peter - bleah...

Steve: Yeah.

Leo: ..."Brjesson" in Sweden says - he wants to talk about "disposal mail." Steve and Leo, thanks for Security Now! and the information you give us. It helps to be safer on the Internet. Love the show. And for Leo's sake, if you decide to share this, yada yada yada. [Laughter] Which is kind of what I always say. Et cetera. You know, Rush Limbaugh, that's why he created the Dittoheads, you know, it's just, like, just say "ditto," okay, because - mega dittos. Because people just kept saying the same thing over and over. So just say "ditto" from now on.

Anyway, I was thinking about how annoying it is to have to supply an email when you just want to get past a point for getting to the next step in the process, whatever it is you want to do on the 'Net. I discovered Disposeamail.com. As I know you don't like to click on links in emails, just Google it.

Steve: Huh.

Leo: See?

Steve: Yeah, I won't click.

Leo: Yeah. [Singing] I won't click. Don't ask me. He says: I think it's a really nice solution for just getting past these steps. Furthermore, if you want to get a unique disposable email address, you can just use the GRC password generator, which is awesome. The only thing I'm missing for the Disposeamail solution is HTTPS. Thought it might be fun for you to know that I follow the TNOESG rule, that is, "Trust No One Except Steve Gibson." Keep the invaluable work up that you and Leo do. Regards, Peter in Sweden. Oh, that's a neat thing, Disposeamail.

Steve: Okay, now, this is really sort of odd, but interesting. So, yes, Disposeamail.com. Now, what it is is, okay, I am intrigued by it, but I'm a little frightened by it, too. It is just a galactic email recipient that you don't even have to tell it ahead of time, you don't create an account, you don't log on, you don't identify yourself, nothing. All you do is, if you are at some random download site or account creation nonsense - I hate that. I mean, when I built GRC's eCommerce system I said I am not going to ask people who want to buy SpinRite to "First you must create an account with GRC." It's like, the things that drive me nuts, I'm not going to ask my own customers to do. That's just bogus.

But I'm sure we're always, I mean, I know I'm always having to give an email address for something where I'm never going to go back there. I'm afraid that they're going to send me an email loop confirmation because they're trying to harvest email addresses from people, even though I don't want them to do that. So it's like, okay. So wherever you happen to be at one of these sites, you just make something up. I mean, on the spur of the moment. It could just be "test." It could be "himom," anything, @disposeamail.com. So that site sends email confirmation, follow-up, click-through loop, whatever it is, it sends it to Disposeamail.com. Disposeamail.com accepts anything from anywhere. It doesn't care.

And I think, my god, how do they handle spam? Because I've looked at - I've done packet sniffing of my own, GRC's SMTP servers which transact email. And I see servers hook up to GRC and try Adam at GRC.com, Alex at GRC.com, Annette at GRC.com, and right, I mean, right down through every possible first name there is. And in fact I created a temporary email address that I realized after, in order to purchase the iPad, doing exactly this same thing, what we're talking about, and I got spam on it because it wasn't bizarre enough.

So this wacky Disposeamail must just be accepting all the spam that's ever been sent to it. Or they must - maybe they do some good RBL stuff, blacklisting SMTP sources so they're not getting too much. So the point is, if you go to - so you go to Disposeamail and put in, like, "test." All you get is a simple little form that says, "What email address would you like to check on stuff from?" And so you put in "himom" or whatever. And if they've ever received any email addressed to himom at disposeamail.com, including everyone else's...

Leo: Yeah, so it'd probably be a good idea not to use something obvious.

Steve: Correct. And I did. I mean, well...

Leo: I just used "spam," and look at all the...

Steve: Now try "test." "Test" I think has, like, a nice little set of maybe about 12 things.

Leo: Yeah, yeah.

Steve: And so...

Leo: So it doesn't even check to see if it's you or anything. You're just looking for what did you get with that email address lately.

Steve: Yes. And so certainly you would want to use...

Leo: There is a lot of spam here, by the way. In fact, it's almost all spam.

Steve: I'm not surprised. I mean, it would have to be. It's collecting it from anything. But if you were to put in 729_37A9CB, there's probably not going to be many of those. You can make it up on the fly. And then you just go over and put the same thing into it, and it'll give you your mail that was sent. So with an understanding that it's strange, that it's not private at all, that anybody who puts in the same email address that you put in will see whatever you were sent - and that's the problem is you wouldn't - if you were doing something where a bank was sending you confirming credentials or something, or click this link to access your account, and you used "doggybreath" or something, anybody else who put that in would see the mail that was sent. And I don't know if there's a way to delete it. I didn't notice to see. I guess probably not, otherwise people would be deleting each other's email. So...

Leo: That's why I guess he's suggesting you use Perfect Paper Passwords.

Steve: Yes, use a bizarre, absolutely unique string.

Leo: Or the password generator; right.

Steve: Yeah. And I would also say don't do it for something sensitive. Do it for things that are just annoying, but don't really - you wouldn't mind it if somebody else saw it because potentially someone else could. There's no security here. But for what it is, it's wacky, but it's kind of useful.

Leo: I would bet that spammers have - or somebody, hackers have written scripts that scan through this stuff and are looking for bank passwords and things. So in fact I would say this is a very dangerous thing to do for something that you'd want

to keep secure.

Steve: Yes. Although, again, we don't know - I don't know how long an email address it could accept. But if you use one of GRC's perfect passwords, I mean, there you've got...

Leo: Pretty unlikely.

Steve: You've got a gazillion bits' worth of randomness. I mean, that's what I'm offering at GRC for that reason. So, but again, without your ability to delete it, it's going to be there forever. So you don't want - and you're sending it to somebody else, not to you. So it is a concern. But I could see myself, for clearly nonsensitive things, saying, ah, this is easy. This is better than having to create random temporary email accounts.

Leo: Chatroom tells me there are a number of other services. This is another one does exactly the same thing: Mailinator.

Steve: Cool.

Leo: And there's quite a few of them. So if you think about it, it'd be an easy script to write, really.

Steve: Yes. It's a no-brainer.

Leo: It's a no-brainer.

Steve: But I'm not writing one.

Leo: No.

Steve: It just seems like a bad...

Leo: You don't want the responsibility.

Steve: I'm not having it on GRC, no.

Leo: By the way, the chatroom has also sent me an article from CNN a couple of days back. Bob Greene, a CNN contributor, writing a story in CNN about getting exactly the same email that my wife Jennifer got this morning, from a friend of his who is a famous sportswriter. And it's the same - so apparently this is really going

around right now.

Steve: Yeah, exactly. So tell Jenn that, if nothing else, she's in good company.

Leo: Panic not. Well, she didn't get hacked. It was somebody else. But she's in good company falling for it, probably.

Steve: Yes.

Leo: Question #6, Mark Fink in Baltimore, Maryland. Just listening to Security Now! 240, couple of episodes back, and the question about disabling the microphone. We were talking about how easy it is to disable a camera by taping it over, but the mic still works. And in fact it doesn't look like you can necessarily disable it very easily. He says: Sorry if I'm the millionth person to suggest this. On my Dell M4300 laptop you could disable it in the BIOS settings. Don't know how common an option this is, but I thought I'd mention it as one place people could look. Thanks for helping to make the world a little safer and more aware. My wife and the IT folks at work wish I'd never found your podcast. Mark Fink, Baltimore, Maryland. So, now, if I disable it in BIOS, does that mean software could turn it back on?

Steve: No. Well, okay. Maybe ultraspecialized software could turn it back on because it is the BIOS. You're using the keyboard in the BIOS and when you're in the setup mode to change the BIOS. But this is a very good idea. So if you're a person with a laptop who doesn't use your microphone, that is, the regular microphone on your laptop, you're not doing teleconferencing and Skype and so forth, or when you do you're not using the built-in microphone, but you're using a headset, for example, the reason I like this is that, in the BIOS, when you turn it off, it disappears to the OS. The OS believes that it's on a laptop with no microphone. That is, with no built-in microphone.

Leo: Aha.

Steve: It doesn't see it in any way. The hardware, it's removed from the hardware list, and it's just gone.

Leo: Oh, that's good.

Steve: So that's a great suggestion. I hadn't thought of it. I wanted to give Mark credit for that and thank him because - now, we don't know that all BIOSes are going to have this. But, you know, BIOSes often give you the option of turning, like, your serial ports on and off, how many of those do you want, do you want this enabled or not. If you have an option for microphone disabling, and you're not a user, by all means turn it off in the BIOS. It'll just disappear from your operating system, and the OS won't know that it exists at all. Great, great idea.

Leo: Question #7. Yeah. Patrick Boyle, Springfield, Missouri, has more forensics suggestions for us. Steve, I just heard last week's episode. Someone was wondering how to block an IP address. You mentioned your buddy Mark Thompson's FixedOrbit.com. Thank you for the tool. And boy, do I have some more related tools for you.

IP Neighbors, it's www.myipneighbors.com. You can enter an IP address or a domain name. It'll show you all the domains that are hosted at that IP address. Oh, that's interesting. Here's one for domaintools.com, used to be whois.sc, domaintools.com. You enter an IP address or a domain name, it shows you the ownership. And whois.net, same thing by IP address, tools.whois.net. So there's some other useful ways of figuring out what's going on on that network.

Steve: Yeah. And I thought that our listeners are the kind of people who would appreciate knowing about those other little tools, since we're all sleuths.

Leo: I put - there's a command line Java program called JWHOIS that I always put on all my Macs. You do it from the terminal, from the command line. But it's really good at scanning. The problem with finding out from IP address or domain name who owns it is you have to go through a lot of different registrars. And this does - this has a very complete list of registrars. But there are websites, like some of the ones he mentioned, that do a very good job, too.

Steve: Right.

Leo: Question #8. David W. Griffin in Atlanta, Georgia comments about programming in assembly language: I respect your abilities to program in assembly language, but much of the world's software these days is designed for large-scale software for which high-level solutions rather than low-level solutions are the right way to go. Developing large software projects with large staffs and then maintaining them for a decade is not a job for which you would select assembly language, not if you could help it, anyway. I'm not sure I agree with that.

Software engineering has made little progress toward reusable components, but at least high-level languages have some effect on achieving reliability. Nothing you have said contradicts this. You, after all, are doing small, well-focused applications with a single author. But I thought I'd make the point that much of the world's software today has other design considerations. I enjoy the podcast and your lectures on computer science.

Steve: And largely I completely agree. When I talk about my use of assembly language, I regard it as a personal preference. I'm not pushing it on people. I'm not suggesting that the world would be a better place if people programmed in assembly language. Well, maybe I am. But I completely recognize that high-level languages are here to stay; that they make much more sense for many applications. I mean, it's just - it's programmer productivity. I guess the metric that I've seen which is most compelling is that, no matter what level of language you're programming in, programmers generally produce the same number of lines per day. So if a high-level language line of code does much more than an assembly language line of code, and both programmers are going to be equally

productive when measured in lines of code, then it's clear that more functionality is being written per day by someone whose lines of code do more per line because they're using a high-level language.

So I have no problem with that. I'm sticking with what I love and like and know and I'm so comfortable with, assembly language. But by no means have I been intending to denigrate in any way the value of high-level languages. We wouldn't have nearly as much stuff if we didn't have high-level languages. I would argue maybe we'd have better stuff, but much less of it. So would that be a bad thing? I'm not so sure that would be a bad thing.

Leo: Yeah. I mean, I guess my thinking is, you can make assembly look just like a high-level language with macros, and probably make it very efficient.

Steve: Well, mine is very clean, and I write a lot of it in a day. So again, it might be a little bit like, you know, the guy who wrote in about Forth, who took exception to my saying, "I can't read that. How can anybody read that? Nobody can read that." And he said, "I can read that." It's like, okay. So it's what you know.

Leo: It really is.

Steve: Yup.

Leo: To each his own. It's like arguing which human language is the best. I mean...

Steve: Yeah.

Leo: They're all - they can all be equally expressive. But I think I like the metric, which is the more you can - assembly language does require more typing.

Steve: To get the same job done, you're absolutely doing more typing, yes.

Leo: Giovanni Darquea in Maryland wonders about the RFID YubiKey. This is the new one. Steve, I just wanted to let you know, Yubico is now making their famous YubiKey with an integrated RFID transmitter. I was wondering what you think the potential security implications could be now that anyone can just wirelessly get your YubiKey passwords. Or, if you do think it's safe enough to use, what scenarios do you envision yourself using the RFID YubiKey with. As always, love the show. Please keep recording it for many years to come. Looking forward to CryptoLink. C'mon, Steve, start coding.

Steve: I'm glad he reminded me. I did meet with Stina Ehrensvrd about a couple weeks ago. We had some coffee in the morning when she was down here after the annual RSA conference up in San Francisco. And to clarify, this new YubiKey is exactly like the previous YubiKeys, the new generation ones, the ones that have two different modes of

operating. Just to remind our listeners, that allows you to have both the original, preprogrammed with a secret key that nobody knows, but which will authenticate against Yubico's authentication servers. And you can also have, it's like a second channel. You can also touch it differently, and it will generate a whole second channel, where you can put a fixed password of your own. You can also make it a one-time password. They now support the standard oath-style authentication, which is the same thing which the VeriSign tokens and other things use. It's less resolution in terms of the digits it's producing, but it's an industry standard. So they've gone that way. So that's the non-RFID version of their current sort of second-generation YubiKey.

What they did was they have another version for a little more money, I think it's $35, which has all that and a static serial number RFID transponder. The idea was that, well, rather than, in this quest to minimize the so-called "necklace" of having to have all these separate authentication things, they said, well, we'll just put in an RFID transponder. So if something pings us, we'll respond with an RFID standard token which is fixed. It's not variable. It's always the same. It simply identifies that particular YubiKey out of the world of them, and out of the world of other RFID things. There is a registrar that you use, very much like you do with MAC addresses, so you don't have to worry about them having collisions.

And so the concept was, if your corporation used RFID, like, door keys, you could register your YubiKey's RFID ID with your company's door security, in which case you wouldn't have to have a separate RFID dongle to get into the building. You'd just use your YubiKey, waving it, rather than using it in the normal USB mode which we all know the YubiKey uses. So it's just a cool little additional feature. Not much money. And they thought, well, why not toss it in? I mean, in no way, it doesn't interact with the YubiKey functionality. It's just a separate - it's like a third channel that says, this is my ID. Now, if you don't want that, don't use that YubiKey. If you do, if that would be useful to you, they've got that, too.

Leo: Way to go, Stina. They're amazing.

Steve: Yeah.

Leo: What a great company.

Steve: They're doing a great job.

Leo: Yeah. All right. Now we get into some special questions.

Steve: Our final three great things.

Leo: Three great things. Starting with The Great Warning of the Week. Subject: Yes, it matters, from Brian in Raleigh, North Carolina. Steve, in case anyone dismisses your continual warnings of ARP poisoning and man-in-the-middle attacks in public spaces as improbable, I'd like to pass along a report from a friend who says he witnessed someone using the Ettercap network sniffing tool in a local coffee shop

this morning. It does happen. It's well worth protecting yourself from it. Thanks for a very informative podcast.

Steve: Yeah, it's actually Ettercap.

Leo: Oh, Ettercap.

Steve: E-t-t-e-r-c-a-p. It's hosted over on SourceForge, and the people are proud of what they've created. It's ettercap.sourceforge.net. They're announcing that 0.7.3 is now released. And their short description of Ettercap, which was being used in this coffee shop this morning, reads, "Ettercap is a suite for man-in-the-middle attacks on LAN. It features sniffing of live connections, content filtering on the fly, and many other interesting tricks. It supports active and passive dissection of many protocols, even ciphered ones, and includes many features for network and host analysis."

So one of the many things it does, for example, is catch usernames and passwords in email logons and unsecured web logons, like, automatically for you. And I would be - I don't know that the person wasn't doing anything more advanced than that. But even that, remember that for the longest time Gmail logons were not secure unless you deliberately used HTTPS initially in order to connect up to Google. And then you dropped back out of security. And most, I would say today most standard SMTP and POP logons, where you log onto your server to get your mail, are still being sent over port 110 for POP, and it's not secure. So somebody sitting in a coffee shop running Ettercap may very well be harvesting logon, email logon credentials. I mean, for example, this is exactly how you start the exploit that got Jennifer, Leo.

Leo: Ah.

Steve: I mean, this is how you do it. This guy collects these logon credentials. Maybe he's selling them, or maybe he's using them himself. So that allows you to logon to somebody else's POP account and browse through their email, learn about them, and then send email asking for money from the people they know. I mean, this is how it starts. And this was happening in a coffee shop this morning.

Leo: Yeah, I mean, it happens all the time. Randal Schwartz used to do that on the cruise ships. He would say, "Is this your password?" He'd come to people. Because people were on the WiFi unencrypted. And he said, "You just sent your password in the clear." And I think, in a way, that's the worst thing...

Steve: Just making friends wherever he goes.

Leo: Randal. Oh, okay. Moving right along to now #11, which is our Great Recommendation of the Week from Steve Hiner, between a keyboard and a chair in Phoenix, Arizona. Subject: Loving the current podcast series. Steve, I'm really enjoying your current "build a computer" series. Thanks for putting it together. The

series has been the motivation I need to read a book I've owned for two or three years, Charles Petzold's book "Code" - this is a classic, by the way - "The Hidden Language of Computer Hardware and Software." There are huge parallels with your podcast series, of course. But it really helps to fill in some of the gaps since he has the room to expand on topics and use graphics to help explain things. I'm over 200 pages into the book, and he's finally gotten to the point of being able to talk about opcodes and machine language. 200 pages in. He takes it very slow and explains every little thing in detail. Anyone who is enjoying the "Let's Build a Computer" series and wants to go a bit deeper should consider picking up this book. I highly recommend it.

Steve: I highly recommend it, too. First of all, Charles Petzold is a tremendous technical writer. He is the guy who taught me Windows.

Leo: Oh, you're kidding.

Steve: It's Charles Petzold's classic book, "Programming Windows," which was my bible when I'm, you know, I'm coming from DOS, where I owned the whole machine, and all you had was a BIOS, and you could put characters on the screen and [indiscernible] the keyboard, and that was, for example, the environment in which I wrote SpinRite. And that's the environment in which everyone programmed. The original Lotus 1-2-3 was a DOS program that ran on the text screen. And so when I sort of thought, oh, looks like this darn Windows thing is going to happen after all, I kept waiting for it to die, but...

Leo: No.

Steve: ...it just didn't die. And I thought - and then for a while I would only fire up Windows in order to run Designer, Micrografx Designer, which was like a fantastic graphics drawing tool. But everything else was better still in DOS. And then Word kind of happened, and I thought, oh, I guess I'm going to have to learn this newfangled thing. And so it was Charles Petzold who came to the rescue. And, I mean, I remember scratching my head, what's going on here with the windows, I don't really get it. But he explained it to me. So, yes, "Code: The Hidden Language of Computer Hardware and Software," I really like Steve's recommendation. It's a great one. For anyone who's enjoying this series, Charles, as Steve says, takes it very slow, and you'll really understand this stuff.

Leo: He wrote for PC Magazine? I know I know that name.

Steve: Yeah, yeah. Oh, yeah. He wrote for PC Magazine for decades. I mean, forever, yeah.

Leo: Great guy.

Steve: He's top-notch.

Leo: Yeah. Question #12. Can we be - are we at the end?

Steve: We are.

Leo: Holy cow. Went fast today. Jack Daniel, with Astaro, in Wilmington, Massachusetts brings us The Brilliant Idea of the Week. Steve, I heard the question about blocking attacks by IP, and I had a few thoughts. First, given where I'm sitting, if you're running Astaro, you can easily "black hole" route by IPs or networks. It's also easy to add a route to your computer to misdirect traffic, for Windows something like: route ADD [problem IP] MASK [255.255.255.255] [non-existent local IP

address] -p will do the trick. Works for - I'll put that in the show notes because that's a command line. Works for networks, too. Don't forget the -p. It makes the route change persistent. Then a "route print" command will show the current routing table to confirm the changes. If you know how to speak router, you can do anything, can't you, Steve.

Steve: Well, I completely forgot about the routing table that all of us have in Windows. And so I loved Jack's suggestion. It's brilliant.

Leo: This is better than hosts, then, for blocking.

Steve: Well, hosts won't do it because hosts will only - our computer goes to the hosts file when it wants to do a DNS lookup, and we want to prevent it from doing a DNS lookup. So, for example, you would tell hosts to go to, I mean, you would put an entry in the hosts file for - say that you wanted to just block all access to DoubleClick.net. You'd put DoubleClick.net, tab, and then 127.0.0.1, which is by default the IP of your own machine. And so your computer cannot get the actual IP address of DoubleClick.net because it always asks the hosts file, that is to say it looks in the hosts file first to satisfy any request. And only if it's not there does it go on. But it doesn't look for IP addresses.

And so one of our questioners, I guess it was week before last, he was asking, I've got some bad IP addresses. I know they're bad. I've stumbled on them before. They've bitten me before, whatever. I just want to prevent my computer from ever going there. How can I do that? And so I scratched my head and noted that, well, some software firewalls will allow you to block by IP address.

Jack comments, first of all, that the Astaro security gateway will offer that facility. And the advantage, of course, of doing it at the gateway is then you're blocking that evil, presumably evil or malicious IP for all machines within your network. So it keeps any traffic addressed to that IP from heading out past it. "Black hole" is the networking term for doing that. But in our computers is a routing table. And I referred to it indirectly earlier when I was talking about - it was that question about the guy's NAS that was on 192.168, and he switched to a 10-dot network and so forth.

If you were to open a command window in Windows, or in the Mac for that matter, I mean, this is something that has existed from the beginning of the Internet, in the first UNIX machines that were on the Internet. And all OSes - Linux, UNIX, Solaris, Windows,

you name it, if they're using IP technology, there's a routing table in your local machine. And that's where that decision is made that a packet is addressed to another machine on the local network or not on the local network, meaning route that out to the gateway. So that line that Jack provided is route ADD, then an IP that you want to match, then the word MASK, and then in this case it would be 255.255.255.255, meaning mask every bit. Every bit of the IP you're giving it is important.

If you wanted to block a whole network, that is, the IPs in the range of that bad IP, you might go 255.255.255.0, which would mean that the last byte would sort of be a wildcard byte. It would be like .* on the end, meaning any of those IPs. Then you give it a nonexistent local IP, which could be 127.0.0.1 or 192.168.100.100, whatever. And so essentially what that does is that tells your computer, this is sort of underneath a firewall, without needing a firewall of any kind, that tells your computer, as this packet is getting ready to be sent, it says check to see whether it matches, what it matches in the routing table.

The way the table works, the first match that occurs is the one that takes precedence. So the routing table is ordered so that the most specific matches are earliest, and the more general ones occur later. So that you always get the more specific match occurring before general ones. And that ends up just sort of working out in terms of routing table dynamics. And the idea would be that it's a simple way of efficiently and cleanly blocking specific IPs that are blocking your computer from sending them out to the gateway. Normally they would end up matching the last rule in the routing table, which is sort of, if nothing else happened, send it to the gateway. But in this case it would match that rule, and it would send it to a nonexistent IP, making it just disappear. So it would be impossible for your computer to contact that remote IP you're wanting to prevent.

And then what's cool is, from the command line, again, you can say "route print," I mean, you can do it right now, anyone listening could just open up a DOS box and say "route print," and it'll dump out your current routing table, showing you what the default routing table is. And he makes a point of that because, if you do the -p, it will end up making an entry in the registry which will reinstantiate that route every time your machine boots, which is what you would want if you wanted to keep these things blacklisted, essentially. But you'd have to remember that you had done that because it's a very powerful mechanism.

And, I mean, I could imagine scratching my head for days if someone brought me to a computer and said, "Steve, everything works except I can't go to Google. Nothing I do lets me go to Google." And we'd look in the hosts file, and there would be nothing there. And we'd look, and he wouldn't have a firewall, everything would be fine. And I would just, I mean, maybe I'd think to sniff traffic and go, oh, look what's happening, the packet's going to the twilight zone. And that might lead me back to the routing table. But, I mean, it's kind of a cool, very stealthy way to make some changes deep in Windows that most people don't even know about, or don't even think about. And it's all built in. It's just - it's in there.

Leo: It's in there. Wow, these were great questions, and some great tips.

Steve: I had to stop myself at 12, Leo. I just, you know, I thought, well, [indiscernible].

Leo: Well, we whizzed through them, so that's fine.

Steve: Yeah.

Leo: You can find more about Steve and all of his great software at GRC.com, the Gibson Research Corporation. That's where you'll find SpinRite, everybody's favorite hard drive maintenance and recovery utility, but also lots of freebies like Wizmo and ShieldsUP!, which is very famous for testing routers. You can also find 16KB versions of the show there, as well as the full quality versions, transcriptions, and show notes. It's all at GRC.com. If you'd like to ask a question for our next Q&A segment in a couple of episodes, you can go to GRC.com/feedback. And Steve, we will see you next week with - do you know what you're going to talk about yet, or is it going to be a surprise?

Steve: Well, I'm glad you asked. We were going to be talking about, we've been planned to talk about, the multiverse - multithreading, multitasking, multicore, multi everything. But we can't.

Leo: Why not?

Steve: Something has come up.

Leo: Oh, my.

Steve: And it's always the case that we will give precedence to things that are important that have come up. And many of our listeners were writing to me about this well after I had learned about it, and so rest assured I know all about it. I'm not going to do an "I told you so," but it turns out there's a problem with so many certificate authorities being trusted by our browsers.

Leo: Oh, boy.

Steve: There is evidence that some governments have been legally compelling trusted certificate authorities to issue bogus website certificates specifically to allow them to spy.

Leo: Oh, dear.

Steve: So we need to talk about how this is happening, the mechanisms, how we can detect it, and what to do about it. There's an 18-page academic paper that we'll link to next week. And as I'm reading through it, I mean, I could have written part of it because at one point it says - it's, like, bemoaning the huge number of authorities which are now trusted certificate authorities in our browsers. And remember I used to joke about the Hong Kong Post Office.

Leo: Yeah, Hong Kong Post Office, yeah.

Steve: Not meaning to pick on them. But, you know, it's like, why does my browser trust anything they do? And what's significant is that Google may have their certificates signed by VeriSign, but that doesn't prevent any other certificate authority from generating a bogus Google.com certificate for someone else. And that allows the interception of our SSL secured traffic. There is evidence that this is happening. So we're going to talk about that next week.

Leo: Terrible.

Steve: Yup.

Leo: Okay, well, Steve, that's...

Steve: Aren't you glad you asked?

Leo: Yeah. Wow. Well, no, this'll be an important episode. You've got to make sure you listen next week.

Steve: Yup, it's a classic Security Now! topic.

Leo: Don't miss a one.

Steve: And what's so cool is, all of our listeners who've been following along understand what I just said.

Leo: They're ready.

Steve: They're ready.

Leo: They're prepared. And the rest of you, you've got some listening to do. Just go back and listen to the previous 251 episodes, should be easy. 241 episodes, should be easy. Steve, we'll see you next week on Security Now!. Reminder, of course, you can get us in video now. Go to iTunes, search for Security Now!. Or just search for TWiT, and you'll find all the TWiT shows, including Security Now!, there. We have high- and low-quality H.264. Now low, but actually large and small is probably a better way to describe it, suitable for, depending on your device, your computer, your laptop, or your big-screen TV, or maybe your phone. We also have YouTube versions at YouTube.com/twit. Look in the Security Now! channel, and that's going to be that way from now on. Once a week we're adding more shows to the video lineup so you can get the video versions. Thanks, Steve. We'll see you next time.

Steve: Thanks, Leo.