Listener Feedback #81

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-226.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-226-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 226 for December 10, 2009: Listener Feedback #81.

It's time for Security Now!, the show that covers your privacy and security online with the guru of privacy and security, our very own Steve Gibson. Steve, it's great to see you once again, from GRC.com.

Steve Gibson: Glad to be with you, Leo. We've got a Q&A episode, our 81st one, with some security news, a little bit of errata. I have an interesting SpinRite story from the future. This has been sent back from the future. So I thought that was, you know, a fun thing to share. And we've got our Q&A.

Leo: I love that idea. What do you want to start with, errata or news? News, I guess, huh?

Steve: News, yeah. This is just the podcast following the standard second Tuesday of the month. So Microsoft has, on cue, released a batch of updates. There were 11 things that they fixed. None of them are particularly notable, so I'm not going to go into any great detail. The good news is that they did fix, as we were projecting and hoping they would, that bad zero-day vulnerability in Internet Explorer, which we discussed at length, it was either last week or the week before. And I remember saying at the time I hope that they would have time to fix this because it was being actively exploited on the 'Net. There was plenty of documentation about how to do it, and people were getting hurt by it. So that was fixed. So I just wanted to mention that we had passed through another second Tuesday of the month, and to encourage people to keep themselves up to date, as always.

Leo: Do they put out, like you can look up Patch Tuesday and what was patched for this Patch Tuesday?

Steve: Yes. They have a page essentially for December '09. All of them had, except one, actually, there was an ATL COMM vulnerability that wasn't high exploitability. Because remember they now associate each of these with an exploitability index, which is, you know, yes, there's a problem. And Microsoft rates how likely they think it is to actually be exploited. And it's like, okay, well, fine. So these were all definitely things you want to get patch because Microsoft was saying, yeah, there's probably going to be exploits created from these.

Leo: There's quite a few. But not a huge one like last month.

Steve: Yes, not a record-breaking one. So that's good. There's an interesting trend that has just recently surfaced which is really good, which is voting systems are beginning to swing open, to open source rather than closed.

Leo: Yay.

Steve: Yes. That's just such good news. There's an Open Source Digital Voting Foundation, the OSDV, that has an eight-year timeline, or like a roadmap, during which they're going to produce a comprehensive, publicly owned, open source, complete electronic voting system from registration all the way through election management and vote tallying. They've got a good team that are putting this thing together. They've released - the event was that they released sort of a preliminary blob of code to say, you know, here's a sample of what we're going to be doing. And then what was really interesting was that just five days after that, one of the most notoriously problematic closed source companies, that is, Sequoia, that's had all kinds of problems with its voting systems, they announced that they were going to go open source, and that by...

Leo: Wow. That's fantastic.

Steve: Yes. Which is really good news.

Leo: Now, why is open source - you should maybe say briefly why that's a good thing.

Steve: Well, for something like this, I don't think - I'm not - I don't necessarily believe that having something open source instantly means that it's going to be safer. But open source which is actively scrutinized is arguably dramatically safer.

Leo: At least you know what's going on.

Steve: And that's the key. So the fact that something is open source, if it's open and no one ever looks at it, well, it doesn't help you any. But if, in being open, it allows, and experts do take advantage of the fact that it's open, then you're in good shape. Now, Sequoia, for example, they threatened to sue [Ed] Felten and his friends at Princeton if, in response to a court order where Princeton was asked to analyze these machines, if they did so, then Sequoia said we're going to sue you. So, I mean, you could argue...

Leo: Oh. Oh. That's exactly the opposite of open.

Steve: Yeah.

Leo: That's like, don't touch our stuff.

Steve: You could argue that, like, they're like the poster child of the wrong way to do this.

Leo: Right. Hiding it.

Steve: Saying that everything is proprietary, and it's all closed, and just trust us. Yet when the results of their machinery have been looked at closely, there have been discrepancies found. And they've said, oh, it must have been a static discharge.

Leo: [Laughing] I'm sorry.

Steve: No, I'm not kidding.

Leo: I can't - I'm sorry.

Steve: You know, like vote tallies didn't tally. Oh, well, it's an operator error or a static discharge. And it's like, okay, well, how are we supposed to trust these people? So, I mean...

Leo: I think you're supposed to wear wrist bracelets when you vote.

Steve: So it's really, really good that, first of all, that there is this Open Source Digital Voting Foundation. The idea will be that they'll produce an open source system. Because it exists, and many people care, lots of smart people will study the source and say, hey, as far as I can tell, they've done, like, all my hot buttons have been, like, taken care of here. Now, it's certainly the case that something can still be missed. But it's much better to have many eyeballs looking at it than not. So Sequoia doing this demonstrates another step forward. And in the case of OSDV, this Open Source Digital Voting Foundation, they're going to freely license the result of this project to machine makers and others who have some application for it.

And I'm sure the license will include some things, some constraints on, look, we're giving this to you for you to use, but you can't just go screwing around with it. You've got to use it as is. And if you make changes, then there'll have to be some sort of review process, blah blah blah. But the idea being that the value added will no longer be this intellectual property which is so prone to mistakes. Instead, the value added - and there's still things that people, you know, that companies can do to add value - will be in the packaging and the production and the deployment and all the bells and whistles which will allow them to have product differentiation. It just won't be that there will be any value, that is, any commercial value in secret intellectual property. In fact, you could argue, as more companies take this approach, those that are trying to maintain closed systems will then...

Leo: Will have less value.

Steve: They'll end up having a hard time convincing anyone to buy their stuff.

Leo: Well, let's hope so, anyway. Yeah.

Steve: So, but really, really a good news.

Leo: Yeah, yeah, yeah.

Steve: Now, on the bad news front...

Leo: Uh-oh.

Steve: For our listeners in the U.K., and we know we have many, ZDNet UK reported the news that the major ISP Virgin Media is about - has announced formally that they are about to employ deep packet inspection to anonymously scan their customers' data, everything going to and from their customers, without their consent. They're...

Leo: Well, at least they're telling them that.

Steve: Well, yeah. Well, they're telling the world. The world's not happy, as you can imagine. What they're saying is that they're wanting to assess anonymously how much illegal copyrighted filesharing is transiting their system. So they're using deep packet inspection to look at the data transactions to their customers. The top level is they check to see whether the protocol is any of the known notorious filesharing protocols. And if so, then they will go deeper into the packets and look to see whether that flow is apparently copyrighted data.

Now, they're saying that all of this is done anonymously, that the equipment that's been installed and they're getting ready to turn on, it strips the IP address of the customer out of the packet. They're not attempting and intending at this point to do anything more

than just get some sense for how much of this is going on. So to me this feels like the beginning of something worse. But we'll have to see. And, you know, apparently their public acknowledgement of this is not the sort of thing that they think is really going to be great PR for them; but they must have felt that it was worth doing it and that they certainly could not do it secretly because it would come out, as these things always do, and then they would look really bad for having done it in secret. So anyway, a little bit troubling, but...

Leo: I'm glad that they at least had the sense to publish it. But you're right, I mean, that's not - it's better than nothing. Hey, by the way, I notice you're wearing the hacker shirt. I don't know, I have a NO cup now. So...

Steve: So it just says N-O, period?

Leo: Yeah, look. See? Can you see it? That's right, it just says N-O, period. It's from the same people, ThinkGeek. Actually a couple of guys from the Argonne National Labs in Illinois came by, Tom and Steve, and they brought me this NO mug. Obviously Security Now! listeners. Thank you, Tom and Steve. Now Steve and I both say NO.

Steve: No.

Leo: No. No.

Steve: No. I ran across an interesting page that showed - this is in our errata topic - that showed the current demographic breakdown of web clients on the 'Net by operating system. So not the traditional IE versus Firefox, but what percentage of Windows XP is on the 'Net? And what I found interesting was that today XP has 84 percent...

Leo: What?

Steve: I'm sorry, no, sorry, 64 percent of the OS. Vista is at 23. Mac is at 5.12; Windows 7 at 3.77; Linux at 1 percent; Windows 2000, still out there, 0.62 percent. And the iPhone is 0.54 percent, with miscellaneous others at 1 percent. So summing up the various Windows - XP, Vista, Windows 7 and Windows 2000 - Windows, any Windows, is at 91.26 percent, with Mac at 5, and then Linux at 1.

Leo: Wow.

Steve: So still very skewed toward Windows. And but those numbers are certainly - Windows numbers are falling. Mac is rising. Linux is rising. But they certainly have a ways to go.

Leo: There's some problems, as you can imagine, with the particular methodology and how the browsers identify themselves. But I think in general that's the correct proportion.

Steve: Yeah.

Leo: Yeah.

Steve: And an interesting report that was sent back from the future by Jake and Phillip, who need to remain anonymous, they explain, because they're with a time correction team. The subject of the email that caught my eye was "SpinRite Saves the Future." And they write, "Dear Steve. My team and I would like to express our heartfelt appreciation for SpinRite, your fine, lifesaving product. We've all become tremendous fans of SpinRite 12." Of course I'm only at...

Leo: 12? Wait a minute. You're up to 6.

Steve: Yeah, I'm at SpinRite 6. So, and given...

Leo: Oh, these people are calling from Alduran, okay. I understand.

Steve: Well, essentially yes. Given the fact that I release major version updates very infrequently...

Leo: 12 is going to be...

Steve: 12 is out there a ways, yeah. So they continue, "Your software saved our lives. Here's what happened. My team was sent on a mission to prevent some unfortunate results of the bad science presented in the movie '2012.'"

Leo: Oh, boy [laughing].

Steve: "While traveling too close to the sun, an unexpected solar flare" - and I was thinking, okay, are there any expected solar flares? But, you know, I guess if you're a time traveler...

Leo: You know, yeah, sure.

Steve: Yeah, exactly. So one caught them by surprise. "An unexpected solar flare hit our craft, resulting in a near complete loss of data from every system onboard. This caused our reentry into the earth's atmosphere to be very far off course. At this time I would like

to apologize to the people of Utah. I cannot imagine the fright our reentry must have given everyone there. Please accept our sincere apology. Anyway, once we landed, if you may call it that, we set about restoring our data. We popped in SpinRite v12, and in a mere three days' time all of the data from our craft was back, exactly as it had been prior to the above-mentioned unpleasantness." Now, this does give me pause, Leo, to think that maybe spinning magnetic hard drives are not as short-lived as I was concerned.

Leo: They might survive.

Steve: Yeah. Apparently...

Leo: Or...

Steve: ...SSDs didn't take over the future.

Leo: You'll invent some way to save SSDs.

Steve: Ah, but he doesn't specify what kind of technology SpinRite v12 has recovered. So he says, "You really saved our pork product (bacon, as they say in your time). Steve, you really are a magician. And although we really shouldn't tell you this, CryptoLink v3 is going to rock the world."

Leo: I love it.

Steve: "Please keep up your good work. Sincerely, Time Correction Team XVI."

Leo: I love it. Somebody reads a little too much science fiction.

Steve: They have to read a lot to keep up with me, so.

Leo: I'm reading the new Jerry - not new, the new recording of Jerry Pournelle's "Mote in God's Eye," which Audible just released.

Steve: Oh, one of my favorite, all-time favorite books.

Leo: I love the genre, first contact genre. You know what, I hadn't - I have never read this one before, which is funny.

Steve: What, you've never read "The Mote"?

Leo: No. Isn't that weird? No.

Steve: Oh, Leo, it's got a surprise. It's such a good surprise.

Leo: Well, I love Larry Niven, so...

Steve: Yes. And when Niven and Pournelle get together, it's great. That's the only problem with that book is that you don't know something which you will never forget once you learn it.

Leo: Oh, I love it.

Steve: And it makes it a little more difficult to reread it. And I'm a big book re-reader. So...

Leo: Oh, well, I'm lucky, then. I've never read it. So I'm, like, I'm in heaven here.

Steve: Go slow. Don't read it overnight because then you'll be like, aw, it's over.

Leo: Well, that's nice about Audible. No, that's what's nice about Audible. You really kind of can relish it. But you know what, Jerry told me when he was on TWiT a couple of weeks ago that the way they work together is Jerry is the plotter. He said, you know, I'm better at plotting than Larry is; and Larry's better at writing than I am. So Jerry does the plotting, and Niven does the writing, for the most part.

Steve: And fills in all of the plot specifics.

Leo: Right.

Steve: Interesting.

Leo: And so you can credit Jerry Pournelle with the twist.

Steve: Yeah, good point. Very good point.

Leo: Oh, now I'm excited. Oh, now I'm very excited. I can't, I cannot wait. Anyway...

Steve: Wait till you learn the secret.

Leo: No, don't, no, okay, don't spoil it.

Steve: No, no, I'm not saying anything.

Leo: But one of the things I really like about it, I was a big fan, still am a big fan of the Patrick O'Brian 19th-century seafaring novels. And what's funny is the future, in the future, and this takes place I think in the year 3000, the Navy, the Spacers are like the Navy. It's exactly the same kind of thing. They have stewards who bring coffee, I mean, it's just like they're at sea. And obviously there was an intentional parallel done by Larry and Jerry. And I think it just really, it works so well. It's really, really great. So anyway, I just - I don't know why I mentioned that, but I'm reading that right now.

Hey, we're going to get to our questions. We've got some great ones for you, including at the very end, of course, we save the good stuff, the Brilliant Disneyland Authentication Solution of the Week. I've been hearing from a lot of Disneyland folks about this system, by the way.

Steve: Yep, I have, too. There was a surprising number of Disney notes in the last mailbag, so...

Leo: Yeah, lot of Disney folks listen to us. All right, Steve, are you ready for a question or two?

Steve: Ready, yeah.

Leo: Ready, Eddie. Question one from Chris in Las Vegas, Nevada. He's thinking about ARP. Steve, Windows throws an error when it receives an ARP response for the same - okay. Here we go. Get ready. Buckle in. Windows throws an error when it receives an ARP response from an IP address it's trying to use itself, saying another device has the same IP on the LAN. We've all seen this. If you use static IP addresses, for instance, it'll say, well, there's another device on the LAN with the same IP address. So wouldn't it be trivial to have the stack throw an error if it received multiple responses for the same IP address from different MAC addresses? We're trying to avoid ARP spoofing here. It could also just be a small program running that watches for such anomalies and notifies the user. Shouldn't, you know, it should always be, if it's one IP address, the same MAC address. The only real downside I can see is in cases of sites using something like link aggregation or something, or bonding. In that case you might get a false positive. What do you think? That's an interesting idea.

Steve: Well, it's a great idea. And I think I mentioned a couple weeks ago that one of the things I was going to toss into CryptoLink, because it's so easy to do, exactly as Chris says, is just watch the LAN traffic for anything suspicious. And so, for example, another example of something suspicious would be if an IP-to-MAC address mapping appears to change. Now, that would happen if you deliberately manually changed the IP address on some machine on your network. But that's normally not happening. So but it would be an

indication of someone coming in and beginning to spoof ARP traffic and mess up the IP-to-MAC address mapping.

So Chris is completely right. It would be a - it's a trivial thing to do, a simple little program. You know, it's not, for example, in Windows, mostly because people wouldn't know what to do with it. The idea of an IP address collision had to be in Windows. And as you say, Leo, we've all seen this. It's in Windows and Mac and Linux and, you know, UNIX, all the OSes, where they detect more than - they detect some other device that is responding to a MAC address query for the same IP that they have. And it's like, wait a minute. And again, it's all these OSes detect it and alert the user because you cannot have, just by definition, two devices with the same IP address on the same LAN. That would just cause confusion.

Technically, electrically, it's possible. But we've decided, well, we're not going to - we're going to disallow that because who's supposed to be the recipient of the traffic? So in typical sort of Microsoft approach, how would you present a warning to the user saying, oh, we believe that ARP spoofing may be occurring on your network? It's like, okay, well, you're never going to see a note like that from Microsoft. So it makes sense for it to be an add-on utility or something that an expert user would know how to interpret. And another example would be if this utility were to remember the MAC address of the gateway persistently. That is, like, make a little entry in the registry and then notify you if at any time in the future the MAC address for the gateway appears to change because that's classic man-in-the-middle ARP spoofing where somebody else spoofs the gateway ARP response in order to get themselves knitted in the middle. Well, I mean, I'd love to know if without me doing anything the MAC address for my gateway changes because there's absolutely no reason it ever should. Or if I get the notice after just having reconfigured my network, I go, oh, yeah, of course.

Leo: Right, right.

Steve: I just made a change. I'm expecting that. But so Chris is absolutely right. We will see that in CryptoLink. Maybe I'll spin out a little freebie that does that just while I'm at it because it would be simple to do and makes a lot of sense.

Leo: And some routers, I'm being told by people in our chatroom, do this and that kind of thing, and they warn about that kind of thing. So it's, yeah, that's...

Steve: I've never seen that.

Leo: Moss Wahlberg [sp] is saying Cisco and HP switches have built-in ARP spoofing protection. I don't know if they use that technique for it.

Steve: Okay, yeah. That would be a different approach where they would be resistant, for example. One of the games that people have played historically is it used to be that, in the old trusting days of the Internet, a switch or router or anything actually building an ARP table that maps IPs to MAC addresses, they would simply accept as the truth any ARP response that they saw on the wire. ARP traffic is broadcasted, and network interface cards see all the traffic, even if they don't accept it all in the case that they're on, for example, on a hub, as we used to use in the old days. And so it's possible for a

third party on the network to see other devices getting themselves registered on the 'Net using ARP and just say, oh, I might as well add that information to my own local ARP table. In case I ever need to talk to any of those guys, I already know their MAC address. So I don't have to go ask them, go through the whole ARP protocol broadcast and response to get that. In other words, they used to just accept all the traffic on the network and store it. Well, that's absolutely wide open for exploitation because it means that spoofing is trivial.

Leo: Right.

Steve: All you do is you just send out malicious ARP packets, and everybody on the network will accept them as gospel. And so one of the things - so there are many things you can do. For example, you would never accept an ARP reply unless you were expecting one. That is, only when you had a pending request out and were expecting a reply would you take it. And in any kind of a race condition you could do things, like if you got two different replies you could say I think I'm going to stay with who I believe from the previous response rather than some newcomer that's different. So you could certainly see plenty of strategies for putting filters up and preventing this kind of stuff from being just so wide open.

Leo: Right. Question 2, Peter Jaros from Brooklyn, New York. He has a new approach to defeating whole disk encryption and other in-memory-key schemes. We talked a little bit about that. Never unplug the machine. Steal the computer without ever turning off the power or letting machine go to sleep. How would you do that? He actually gives us a link to WiebeTech.com. And I guess it's - I'm guessing it's some sort of battery backup. Yeah, it says transport a live computer without shutting it down. No other product performs this patent-pending feat. It's a hotplug device, obviously just a battery, big old battery you plug the computer into and then take it with you. And by the way, it says right here, "How to circumvent whole disk encryption."

Steve: Okay. So it actually is more clever than that.

Leo: Oh, really.

Steve: It's very cool.

Leo: WiebeTech, if you want to see this, dot com.

Steve: Okay. So the computer's plugged in. Okay, well, so you can't ever power it down. Yet it's receiving power now. So this clever thing is able to run in parallel with existing power.

Leo: Oh, it would have to be, yeah. So this would be for, like, law enforcement. They come into your house.

Steve: Precisely.

Leo: They think something's going on in your computer. It's running, and you logged in, so whole disk encryption is now - everything's unlocked. But they obviously can't reboot or they'll never get into it. So somehow they have to keep it exactly powered up and take it back to the station.

Steve: They also need to keep the screensaver from activating.

Leo: Oh, boy.

Steve: Or the machine going into standby. So they have a little USB dongle called the Mouse [Jiggler]. And it says it just generates little mouse move messages.

Leo: I love it.

Steve: So they plug this thing into a USB port, and the mouse starts jiggling around on the screen. Now, the reason that it caught my eye is that I was asked, oh, a couple years ago to be part of an advisory panel for an FBI effort to build a lab on the West Coast. They wanted to do a big forensics lab, and they wanted it to have all the stuff it needed. And in some of the meetings that I attended they were explaining, here are the problems that we have. And one of the problems that, I mean, they really do have is they get a warrant for some company's hardware that - computers that they believe there's bad stuff on. And if the people, if they've turned the computers off, and there's active encryption on the system, they can't get back in. And so this is like, this is really a problem that they have. So this gadget, not only does it have the little USB mouse wiggler, but it's like a UPS. But it's one where the power comes out of the AC outlet. So they give two examples. One is where they say, well, many computers are plugged into an outlet strip.

Leo: Right.

Steve: So you plug this backup power supply, with a male plug, you plug it into the power strip along with the computer.

Leo: So this is kind of a feature of power strip. It's all, I guess it's in serial, and you can just apply power to any plug socket.

Steve: Sure. All the power strip connectors are just in parallel. So you plug it into the power strip.

Leo: Parallel, okay.

Steve: You plug it into the power strip. Then you unplug the power strip from the wall.

Leo: Right, because it's now getting power.

Steve: It is now, exactly. So the power's feeding into one connector of the power strip...

Leo: That's clever.

Steve: ...and out to the computer. Or, if the computer's plugged directly into the wall, and on their site they show a little picture of this, if there's anything else plugged, you know, all wall outlets have, like, two plugs. So you unplug the lamp or whatever is plugged in there with it. You plug their box into the other dual outlet, then unscrew it, pull it out, and snip the wires.

Leo: Wow.

Steve: So now you've got their backup unit running, just routed through this little two-outlet plug back to the computer.

Leo: They call this their "outlet seizure" method.

Steve: [Laughter] And I just think it's very clever. They've got the mouse wiggler to keep the machine alive. And so...

Leo: You should have to have a license to buy this stuff. I mean, really.

Steve: Yeah, well, I mean, it's diabolical. And it would prevent you from - basically they don't know, if the computer shuts down, that they're going to lose all access to it. But they do know that it's alive and running right now.

Leo: Yeah, why take a chance? I can see this stuff now, so let's snag it.

Steve: Yup. I wouldn't be at all surprised if there's a large order from the FBI coming their way.

Leo: Oh, yeah.

Steve: I do know that the FBI, from our conversations, I mean, this is a problem that they've got.

Leo: That they have to solve.

Steve: And this would solve it.

Leo: Yeah.

Steve: I just thought it was very clever. I knew our listeners would get a kick out of it.

Leo: Oh, I love it. WiebeTech. Yeah, WiebeTech. They have videos demonstrating the whole thing on the site. I was just looking at them. Pretty cool. Pretty cool.

Steve: Yeah, it actually works.

Leo: Let's move on. Question #3 from Tom Aafloen, from Karlstad, Sweden. He has a password manager for my mom. Actually it wasn't my mom that had the problem, but okay. We'll use it.

Steve: A generic mom.

Leo: Any - or me. Certainly me.

Steve: Certainly my mom.

Leo: Hi, Steve. Leo mentioned a couple of Security Now! episodes ago he didn't think his mom would use any of the password managers out there. But there is one that is just as simple as Notepad - all right, I think anybody could figure that out - but secure. The application is called LockNote. It's made by Steganos. It's a text editor/notepad and encrypted text document in one. Wow. It's a portable application, no need for installation. You can run it right off a USB stick. It's only 312KB in size. And since you only store text in it, it's not going to grow that much even with tons of passwords in it. It is open source - it's on SourceForge - for the paranoid. You can get it from Steganos.com. It says you cannot have multiple documents in one instance of LockNote, but you can easily copy the application and have multiple versions with different passwords if you want. A simple application like this probably can run in multiple instances on Windows.

Just thought I'd pass this along. I've used this in combination with SuperGenPass - which I've recommended - for a long time now. I even have a LockNote version for gift ideas to my friends. So it doesn't have to just be passwords. You can lock up anything in here. You have mentioned on the show that when someone passes away it can be hard to end that person's accounts on all the sites he or she may have been registered on. Well, an envelope with your LockNote password and the location of the file solves that. Put that in a security safe deposit box or something. He says,

I'm in no way affiliated with the makers of LockNote, just a fan. Love the podcast. You should make it twice a week. Tom in Sweden. What do you think? Have you looked at it?

Steve: I have. And the reason I posted this was I'm impressed.

Leo: It's a good idea.

Steve: I've got the source, and I'm going to take a look at it because they don't talk at all about what they're doing. And I want to make sure that what they're doing makes sense. But what this is, is just an EXE. When you download it, and if you go to Steganos.com - it took me a little while to find it. But on the left-hand column under "Free Stuff," there's, like, four free things. The other ones aren't very compelling; but this one was, called LockNote. You just download it, and that's it. There's no setup. There's no install. I mean, I like everything about this so far.

And what it is, is it's just like a Notepad app. In fact it looks exactly like the Windows Notepad. And what's cool is that you can cut and copy and paste, and it acts in every way like Notepad. Then you can assign a password to it. Now, as far as I could tell it makes no attempt to make sure you use a good password. I just put "nuts" in, and it loved it. So it's like, okay, well, that's not a super good password. I could have probably put "r" in, and it would have been happy.

But what's nice is that it binds the text and the password into itself, into the EXE. So you never have a separate text file. It's just this EXE. And as he says, I mean, I'm a little thinking, okay, 312K, that's huge. But that's just my bias because if it were in Assembler it'd be much smaller. But it's neat because you then, under the file menu, you can change the password. And the only way you can change the password is if you know the password because if you try to run it when there is a password, it just says what's the password? And so, I mean, it's very clean.

For me, as I mentioned before, I just got this one big list of URLs and usernames and passwords that I keep in my Palm Pilot. Well, I could easily just cut and copy and paste that into this, give it a really good, strong password because the vulnerability would be guessing the password, so you want to make sure that it's not guessable. And but it just - I love it because it is so clean and just so simple. There's nothing to learn. No UI. No fanciness. It's not trying to do more than just locking up a text file. And it and the password are in some fashion bundled to itself.

Now, again, these guys clearly know security. They've got a bunch of security stuff on their site. So I'm assuming they're doing everything correct with the password. That is, they're not including the password in the EXE. Instead, they're hashing the password or encrypting it or doing something. Anyway, I've got the source. Here's a perfect example. We were talking at the top of the show why open source can be useful. Frankly, if they told me on their site this is exactly what we're doing, yeah, I'd believe that because they've disclosed it, and they have no reason to lie to me. But they didn't tell me anything about what they're doing. So the good news is I can answer those questions by looking at the source.

Leo: You can validate it, yeah.

Steve: Yes. So I will - well, there's nothing to validate because they didn't say anything. But I want to know for myself what they're doing. And I will next week tell all of our listeners exactly what they're doing from my having looked at the source, and be able to say, okay, here's exactly what they're doing, and they did it all right. So anyway, it's very cool, and I wanted to tell our Windows users. Unfortunately there's no Mac version, although it's open source. Again, it's not a super-brilliant, hard-to-reproduce concept. But it's just done, and it's just - it's very nice. I like how clean it is. And it's a cool little gizmo.

Leo: Very, very neat. Question #4, a long one. Get ready. Stand back. Jim in California, in the Bay Area, has some real-world feedback about WOT - Web of Trust. We talked about that I think a couple episodes ago.

Steve: Yep, a browser add-on.

Leo: Steve, first of all, let me say I've been a fan of yours for many years. The security information that you post on GRC.com is invaluable. I've been a regular user of ShieldsUP! for years. I'm also a very happy owner of SpinRite, which is an essential tool for my computer work. It's fantastic.

Now, I recently discovered Security Now!. Wow. I had no idea you were on the air, and I'm thrilled. Now I'm listening nearly nonstop to previous and weekly podcasts and passing it on to my other geek friends.

This is a big thing for me is I don't understand how people could be in the tech industry and not know that TWiT exists, but they do. They are.

It's people like you and Leo that really make the world a better place as your help to others is priceless. Thank you. Spread the word. Let them know.

What I'm writing to you about is a point regarding Web of Trust. There's a bad shortcoming regarding WOT. I started using it and recommending it about a year or more ago. So he was ahead of us on this one. What I found was that undeserving sites were being blacklisted, that is approved, in WOT. These sites were listed as having malware, adult content, et cetera. Oh, I'm sorry, blacklisted means bad. They're bad, okay.

Steve: Right.

Leo: So that undeserving sites that are fine were listed as being not so fine. I knew nothing could be further from the truth. These sites were totally safe and helpful. On emailing WOT about this, I was informed that WOT does not moderate the ratings. How it works is, when a user finds what he or she believes to be a bad site, they simply tag it as bad, what category of problem occurred, and comments. Yeah. That's a problem in a lot of things - email blackholing with MAPS and ORBS and that

kind of thing. There's no appeal process. There needs to be some way of aggregating the information and kind of validating it.

Seems some users may think they got infected from a certain site, but due to the nature of clickjacking or maybe cross-site scripting it may not have been from that site at all, possibly not even during that session. We all know that. Users often don't know what happened or why.

Further, what some Internet "griefers" are doing is using it to launch political or social or other attacks on websites by using WOT to blacklist that site. Any user who uses WOT will see a warning page when they attempt to go to the actually benign site. This warning is a full page and will certainly scare off any new visitors. Better safe than sorry?

Consequently, as you might imagine, I've stopped using WOT and stopped advising its use to others as it forwards malicious users' efforts to deny service to legitimate websites. That's a shame. Web of Trust is a neat idea, but unfortunately it really needs trust. Or at least modifiers and verifiers, an expensive proposition. Perhaps WOT has corrected this problem in some way. It's been over a year since I conversed with them. As always, there are people in the world who use technology to harm rather than help. They need to follow the examples of Steve and Leo. That's a shame, but that's a very good point.

Steve: And it's not surprising. I mean, the concern was that their threshold for blacklisting a site would be very low. And you could argue that, if they don't have a huge user base, then they're not going to have an opportunity to receive a large consensus on a site being bad. In fact, it sounds to me like any user saying, oh, I got hurt by this site, suddenly makes it questionable. Now, it would be nice if they, like, published how many people agreed, or if there was...

Leo: That's what they need. They need, yeah, some aggregation or something, yeah.

Steve: Yeah. But he's right. As it is now, it sounds like they're - it's just unfortunately he's right that it would cost a huge amount of money for them to go around verifying everything. Which frankly, when we were discussing this, I was saying that I liked the idea that Google's bots were doing this because they've got no cross to bear. They're looking at all the code. They're able to be kept up-to-date with the latest exploits and see whether they see evidence of those exploits on the sites that the bots visit in their normal web visiting, as they spider around the web. So to me I think that does make more sense than this kind of an aggregation approach.

Leo: Alas, it's true.

Steve: Yup.

Leo: Matthew Justice in Austin, Texas - a good place for justice - wonders about

Google's DNS Server. Steve, just in case you did not see this - this actually happened since we talked last. This is brand new.

Steve: Yes.

Leo: Google is now doing its OpenDNS kind of a thing. It's a public DNS server, 8.8.8.8. He says you might want to run it through your new DNS benchmark tool. And when might we, the world, be able to play with this? Love your show. Thank you. Matthew. So you have a tester. When this BIND flaw was first publicized, you figured out a way to test; right?

Steve: Well, actually it's different from that.

Leo: Oh, okay.

Steve: It'll pop your eyes out of your head, Leo. But if you go to GRC.com/dns/benchmark.htm, you'll see just a screenshot of it. And I've - this is what I spent a large chunk of the year working on. It's gorgeous. And I just need to finish its documentation.

Leo: Well, let's see it. We want it.

Steve: We'll have it soon. So many people wrote about Google's new DNS service...

Leo: So this just tests the speed, not its security. That's right. We showed another program that tested the security.

Steve: The spoofability system is tied to this. And in fact I got onto this because I wanted to launch them both around the same time. So this is performance as opposed to security.

Leo: Wow. This is great.

Steve: Oh, it's phenomenal.

Leo: Look at this. Steve, wow.

Steve: It's a real piece of work.

Leo: Now, you can't download it yet. Or can you?

Steve: Oh, it's there.

Leo: Oh, good.

Steve: It's downloadable. Just click on it. And it's tiny.

Leo: 175K. I downloaded it faster than my mouse could click it, practically.

Steve: Yeah, and it's all Assembler. And it works. I'm glad that Google did this because I will - I'll add Google's servers to it. I've seen a couple postings from people who have used it already, and Google's benchmarking a little slower than OpenDNS. And this thing even tells you if, like, OpenDNS is in its default configuration, if it redirects mistakes.

Leo: Google does not do that.

Steve: And Google does not do that, right. So...

Leo: Yeah. Which surprised me because, if anybody would want to stick some advertising in there, I would have thought it would be Google.

Steve: And do you know, I have not - I've been so preoccupied trying to get ready to get this finished that I have not yet looked in depth at Google's DNS offering. Have you done a show on it yet?

Leo: Yeah, we talked about on This Week in Google, and I have certainly used it. And...

Steve: So what's Google's motivation?

Leo: Well, they don't disclose their motivation. They say, well, we just, you know, we want to improve the experience on the 'Net because the more you use - and actually this is probably true. The more you use the 'Net, the happier we are; right? And that makes sense. Now, the problem is there is OpenDNS already. And frankly, OpenDNS I think has some significantly better features, things like filtering and so forth. But the nice thing about Google, it's easy to remember. It's 8.8.8.8. And I can't remember the other one.

Steve: The other one is 8.8.4.4.

Leo: So very simple, very easy to remember. But, you know, I think it's good to have another one out there. I don't think there's anything - I can't see anything wrong with it.

Steve: Yeah, well, we'll know soon how its performance compares, and ultimately I think that's the way it will win, with a tool like this that makes it easy for you to see, from your location, what is the fastest server, which is really what you want to know. That's why no one can say, oh, OpenDNS is faster. Well, you might live next door to Google's DNS server, in which case it's going to be a lot faster.

Leo: Right, right. So I'm adding 8.8.8.8. And so how - I just would click to run it, or how would I...

Steve: Yeah.

Leo: Run benchmark. Okay. Oh, I have to right-click it? I'm not too bright when it comes to this. I see the red button. Now what do I do?

Steve: You can click on the big GRC "G" logo if you want. That'll start it up.

Leo: Oh, okay. Well, it's testing them all now. I see. Okay.

Steve: Yeah.

Leo: So, all right, cool. So, yeah, Google is sinking to the bottom at this point, so...

Steve: Yeah, and it may be that they have said, okay, we're launching this, and over time we've going to install more servers.

Leo: Yeah, they've got plenty of bandwidth; right?

Steve: Yeah. We can imagine, if they wanted to give OpenDNS a run for their money, they'd be able to.

Leo: You know, Verizon's is very fast, the four-dot.

Steve: Yes.

Leo: Huh. Yeah, Google's way down on the list. Not way, way, way down, but lower

than some of the other ones. Interesting. Interesting. So this continues to run...

Steve: Until it finishes. You'll see a little progress bar there at the top which is moving along.

Leo: I see, yeah. Oh, that's neat.

Steve: And it shows cached, uncached, and dotcom. Those three different bars are showing you different things. And then if any little red marks appear on the left, that's reliability problems because it's looking for any loss of reliability. I mean, there's a ton of technology here. It's what I - as I said, it's what I've been working on. I've talked about it a number of times.

Leo: That's neat.

Steve: And we'll do a show on benchmarking DNS as soon as I get all the documentation finished.

Leo: They're saying in the chatroom, uh, Leo, you might want to click the giant "Run Benchmark" button. I'm not that bright. Sorry. Let's move on. Question - so, yeah. I mean, I think this is a good choice. I use OpenDNS. Now, OpenDNS does do the thing that you may not like, and others may not like, which is if you do a bogus, a nonexistent search, it pops up a helpful page with some advertising on it that says, you know, did you mean this? It doesn't bother me...

Steve: In fact, other people are beginning to do it, too, other ISPs. Comcast, I believe, is doing that. You'll see that OpenDNS is shown in orange in the benchmark. I detect that for any DNS server. And so I alert people that this is what's going on. And on the summary page, once the benchmark is finished, I actually interpret everything that has happened and compare your DNS servers that you currently are using to everything we just learned about all the other alternatives and advise whether - I actually compute whether there's a statistically significant improvement that you could make by making some changes. So anyway...

Leo: Top four in my results are orange, and numbers two and three are OpenDNS, which is usually what I use. I like OpenDNS because I can say - I can use the filtering for my kids and stuff like that.

Steve: Well, and if you become a subscriber you can turn off the redirection. So it's not like...

Leo: Right. And that's free.

Steve: Yeah.

Leo: It's not like you have to pay for anything.

Steve: Yeah.

Leo: I use the redirection because, first of all, I like it, and I don't want to - I want to support them.

Steve: Yes.

Leo: It's all for free. Question 6 comes from Lex Thomas in Research Triangle Park, beautiful North Carolina. He wonders about router DNS. This is a little different: I've been reading about Google's new Free DNS project. We just talked about that. A few years ago for a brief time I used OpenDNS, liked it a lot. But after an unfortunate and unrelated incident, I had to restore my PC, which caused me to lose my OpenDNS settings. I put mine in the router. I think that's what he's about to say.

After that I just never got around to putting OpenDNS back in. I just defaulted to using what the ISP sent down the pipe. I suppose I should have set up my router instead to point to OpenDNS, rather than doing it in Windows since I'd probably want every computer on the network to use this alternate DNS anyway. I haven't made up my mind about Google's DNS yet. But are there any advantages or disadvantages to using the DNS lookup in the router as opposed to the operating system? Thanks for a great show. Been a fan for years.

Yeah, I've been using it in - I use it in my router at home because that way my kids, you know, unless they're smart enough to bypass it, or motivated to bypass it, which apparently they are not at this point, any computer they use has the same filtering on it.

Steve: Well, we've learned some interesting things through - not only through the work on the DNS benchmark, "we" meaning myself and all the people in the GRC.dns newsgroup where we've actively been working on this, and on the spoofability tester before. What's interesting is that there's a growing list of routers that the spoofability test crashes. And as we know, crashes, well, exploits start out as crashes. And then people figure out exactly what it was and how that the router is crashing, and they turn them into remote code execution. And so there's the possibility that there are a surprising number of routers that you can give them a specially formed DNS response and take over the router. So we're a little concerned about that. So I discussed that on the spoofability system pages.

The other concern I have is that typical consumer routers are not very smart. You know, they're made to be very inexpensive so that they're profitable for the people making them. And doing DNS lookup correctly is sort of tricky. You want to remember what the fastest configured DNS server is, and you want to give it a chance to reply. But if it doesn't reply, then you want to ask it again. And if it still doesn't, then you want to ask all your secondary, tertiary, and so forth servers. And the fact is, this is the logic that UNIX and Mac and Windows uses. That is, when all these OSes are given multiple DNS

servers, they use them intelligently and in a way that overall maximizes performance.

The problem is that, if you remoted your DNS to the router, now it's sort of your proxy. And so your computers all just get one DNS address, meaning the router, and are at the mercy of the router doing the right thing. It's certainly possible for a smart router to be doing a good job with DNS resolution and be passing that back to the clients that are using it to provide that service. But the fact that we've seen flaky router operation, and in fact the DNS benchmark has revealed that some routers are much slower than going direct. That is, the router is actually a speed problem for that.

And so, for example, you give your - you're using the benchmark. You leave the router registered. And you'll end up finding that, for example, going directly to OpenDNS is faster than using your, like, often 192.168.0.1, for example, because typically your DNS will be the same as your gateway, which is the IP that the router has inside your network. So we've also seen, thanks to this benchmark, that using the router is slower than manually configuring DNS and just bypassing it completely. So your mileage may vary. Once the benchmark is finished and public, people will be able to see for themselves. Certainly Lex is right. Putting those settings, sort of making them global for your whole network, exactly as you have done at home, Leo, can make sense because then every system gets the benefit of making a single configuration change.

Leo: Right. And you can override it because, if you override the DNS numbers in any individual machine, it'll override it. And so...

Steve: Exactly. Instead of just saying "obtain DNS automatically," you just manually put those in.

Leo: And don't tell my kids that.

Steve: Exactly. Right.

Leo: Well, actually, what I do is I lock down the settings. Then they'd need an administrator password to change the network settings. So it's actually so much more effective, I think, than any filtering solution out there. It just seems like that's the no-brainer for any parent.

Steve: Yup. So switch to OpenDNS and then go to your OpenDNS configuration page and remove the kinds of sites that you don't want people...

Leo: Well, it has built-in that you can just say, I mean, it has a whole list, but it has pretty good filtering. You can say just keep us safe. But you have to create an account. It's free, though. That's the advantage of that.

Steve: Yeah.

Leo: Steve, are you ready for our Disney authentication questions of the week? Starting with Question 7, Daniel Ernst from West Bloomfield, Michigan, USofA. His Disney fingerprint story: I'm a week behind, just finished 224. Thought I'd mention my experience with fingerprints at Disney. My family went to the Disney parks in Florida last year and encountered the fingerprint scanners. I've been guarding my fingerprints for as long as I can remember, going back to an FBI tour in the '70s - that's neat, he wised up in the '70s - and not volunteering to have my fingerprints taken. I'm sure I would have balked at giving them up at Disney, had I been surprised by it. But being a Security Now! listener I was well prepared. I didn't even try the knuckle thing. I waved over a gatekeeper and explained I'm a privacy advocate. This is what people should do.

Steve: Yes.

Leo: Instead of trying to fake it, let them know. Because if enough people complain, they'll go, oh, I guess we can't use this system. I waved over a gatekeeper, explained I'm a privacy advocate - nice way to put it, I'm sure he did this nicely - and refuse to give up my family's fingerprints. This is interesting. The employee wasn't surprised, told us the alternative is to show photo ID each time we use our passes. We had our IDs out the next few days at the entry gates, and without a hiccup we were let in each time almost as quickly as those giving their fingers. So no need to fool them. Let them know you'll take the alternative. If enough people do, maybe they'll get the message. That's great. I love it.

Steve: Yeah. I thought that was a really good bit of news. I did - a bunch of people, as you apparently independently experienced, Leo, have been talking about this and Disney. And I saw, I found an article that talked about Disney's policy where they say that they are deliberately keeping this biometric data separate, that they're not recording a fingerprint at the resolution, that is, enough data points so that it could even be used for recognition. It could only be used as a go/no go sort of verification. So only a few aspects of the fingerprint are being maintained. And they flush them after the pass which is associated with it has been expired by more than a month or something like that.

So even independent of all this, it does sound like Disney at least was always conscious of these issues, which is really nice to hear. Of course that doesn't tell us anything about anybody else's fingerprint policies. So everything we've said about banks needing you to use your fingerprint in order to cash a check and so forth likely still applies. But at least in the case of Disney it sounds like they've been acting responsibly.

Leo: Yeah. And here we go with our Brilliant Disneyland Authentication Solution of the Week. And this comes from another Swede. You know, we have a lot of Swedish listeners. And just a tip of the hat. It's really great to have all these listeners all over the world. I love it. And Tom Aafloen from Karlstad, Sweden says: Hi, Steve. You and Leo sometimes talk about the problem with companies wanting to have your fingerprint. I think it's going to be harder and harder to resist this. By the way, if you are a Swedish citizen and you come to the U.S., you get fingerprinted. And you sometimes get iris-scanned, as well.

And with nagging kids behind you and a stubborn Disneyland employee in front of

you, the slight obvious knuckle solution might not always work. So why not dedicate a finger? Save your index fingers for personal use. Use your pinkies as a personal backup in case you injure your index fingers. Let's say use, I don't know what's left, your middle finger, for external companies [laughing]. I can't wait until I can hold up my middle finger, my palm facing me, at the Disneyland reader and pressing it down there. There's no correlation between the fingerprints on your different fingers; right? I mean, if they have my middle finger, it doesn't mean they can figure out what my index finger is. Love the show. Tom in Sweden. What a great - does that mean the same thing in Sweden as it means in the U.S.? I don't know. Apparently so.

Steve: Apparently it does. And I just - but I loved the idea. I don't know why, I mean, it's so simple. We've got 10.

Leo: Got 10.

Steve: And he's right, there's no correlation of fingerprints from one to the other. So it's not like your DNA, where they can say, oh, look, this is the father of somebody because they're able to see that it's a close match. And so by all means, use your middle finger for the bank that insists that they have a fingerprint. And you may need to conceal which finger you're using. But if you can get away with it, I think that makes a lot of sense. I just - I thought that was very simple and very clever, as some of the good ideas are.

Leo: My god, man, you're brilliant. Brilliant. Now, I've completed the benchmark here from the DNS benchmark. And the Google - I see Level 3 is very high up there. Google is fairly far down. Not at the bottom of the list, in the top 20. But by far OpenDNS is the fastest. I don't know what this 156.154.7...

Steve: You can click one of the tabs. The other tabs will identify by name and...

Leo: Ah. Neustar. Huh. I don't know who - N-e-u-s-t-a-r.

Steve: And they're pretty high on your list?

Leo: Number one on my list.

Steve: Oh, interesting.

Leo: Look at that, incredible response time. Look, their cache time is almost zero. Their purple bar.

Steve: Interesting. So they - it must be - see, that's one of the things that's so interesting about this is DNS performance is absolutely a function of where you are. So it

must be that if you're using your fancy Ethernet T1 or, no, super connection, that for whatever reason, wherever that terminates has got very short response time to that particular server.

Leo: Here's an interesting tidbit. The highest ranked DNS server that does not replace the 404 page is NTT. That's the Japanese telecom. No, I think it's NTT DoCoMo, isn't it? America Technical Operations. Then Speakeasy, Neustar again, then Level 3. Somebody's saying in the chatroom that Google uses Level 3, so their connectivity might be coming through Level 3. Then Sprint. Speakeasy is very big on there. The Planet. Time Warner. It's interesting. So Comcast, Verizon, and then Google way down on that list.

Steve: It's a cool little app, isn't it.

Leo: Boy, I love this. Steve. I wish more people knew about this. We've got to...

Steve: Oh, everyone'll know soon as I get the documentation finished.

Leo: Plug this more. Oh, wait a minute. I'm seeing Google. It's announcing itself. It is above some of those others as Level 3 Communications, not as Google, 8.8.8.8. So I wonder if they're just using Level 3's DNS server and branding it Google.

Steve: And click on the recommendations, is that what it is? No, conclusions.

Leo: Conclusions.

Steve: And it turns everything into English so that people who aren't super gurus can just sort of quickly scan through, and it highlights important things that it found.

Leo: It's interesting because we're using - it says there's only one DNS in here, and it's our local router's DNS.

Steve: So it knows that; right?

Leo: Yeah. But I think that that's because this is Skypesaurus, which DNS is not important to Skypesaurus, particularly. System name server is slower than three public alternatives. This is great. Look at this, Steve. You're brilliant.

Steve: Well, this is a big piece of work. But it was a labor...

Leo: I can't believe this. And this is free.

Steve: Yeah.

Leo: GRC.com/dns/benchmark. You can get it right now. It's a tiny download. You'll think you didn't really get it. When you click on it, it's like, wait a minute, I must have missed that. So it's, like, five copies because it's just - it was so fast. Steve writes everything in Assembler. This is what's so great about Steve. Look, if you go to GRC.com, buy SpinRite just to say thank you, Steve.

And then, by the way, it's a great thing to have. Everybody who has hard drives needs SpinRite. It's the world's best hard drive maintenance and recovery utility. But there's so much great free stuff there, like this benchmarker. And of course the show is there, including 16KB versions. Steve makes those himself. We stopped making them, so Steve said nope, gonna make 'em, gonna have 'em. Thank you, Steve. He also pays for transcriptions himself. He takes this stuff really seriously. So give him your support because he works very hard for us. GRC.com. Do you know what we're doing next week? Maybe we're answering that question about ARP spoofing and random data. I don't know.

Steve: We're definitely - I'm going to come clean and say that I got myself tangled up on the last Q&A, and I'll have a complete, thorough, clear answer.

Leo: Good. And all the security news and more, every week, with Steve, right here. You can watch us do the show live on Wednesdays. We do it at 2:00 p.m. Eastern, 11:00 a.m. Pacific, every Wednesday unless there's a schedule change. But you'll find the schedule in our calendar and the live video at live.twit.tv. And some really interesting changes coming to our websites soon that's going to make it easier for you to see what you want, including video of all our shows, and this one, as well. So people who have been wanting to see Steve's smiling face as he saves the world can do that. It's all at TWiT.tv, and live.TWiT.tv for the live streaming. Steve, we'll see you next week. Have a great week.

Steve: Thanks, Leo. You, too.