SECURITY NOW!

Transcript of Episode #294

Listener Feedback #114

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-294.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-294-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 294, recorded March 30, 2011: Your questions, Steve's answers, #114.

It's time for Security Now!, the show that helps you stay safe online with the man, the myth, the legend, Mr. GRC.com, Steve Gibson. Good morning, Steve.

Steve Gibson: And that never gets old.

Leo: Yeah, well, it's true, I mean, I have to say, if you're going to do a security show, there are lots of security experts, but there are very few with the breadth and depth that you have. So this show is more than just how to lock your browser. This is how stuff works, how crypto works. And so I like somebody like you who really has a broad-brush understanding of this.

Steve: Well, and it comes from my passion. I just, I really, really am interested in this stuff.

Leo: Yes. Well, we share your interest, so that's why we're glad you're here. Today is a Q&A day; yes?

Steve: Yes, Q&A. We've got 10 questions and a couple, some of them are sort of short things; so as I was running through things, there were some little tasty tidbits that I just couldn't resist throwing in. We've got a couple of bonuses at the end. And not an overabundance of security news this week. No updates have happened. There was, I just

- I don't know why I feel compelled to mention when RealPlayer has problems. We last did about a month ago, they had a security fix in early February. Now there's another one, a heap buffer overflow. I don't have any real sense, either, for how many people are still using RealPlayer. But I think there is some penetration, for example, in the corporate world. And somewhere I tried to go, like C-SPAN or something, they still make you use Real...

Leo: Oh, I hate that, when you go to a site, and you have to use RealPlayer to play back the video or audio?

Steve: Exactly. So anyway, on the Security Focus website I kind of got a kick out of this. Apparently the person who found the problem described it, saying: "RealPlayer is an ugly media player...." I don't know if he didn't like the UI, or if he just meant ugly from a hacker standpoint or from, like, an internal workings standpoint. But he says : "...an ugly media player..."

Leo: It's both, both.

Steve: Yeah, probably, "...developed by RealNetwork and used mainly for its browsers' plug-in supporting the proprietary file formats of its developer." And then under the "Bug" category on the Security Focus posting, he wrote: "Classical heap buffer overflow during the handling of the IVR files caused by the allocation of a certain amount of data (frame size) decided by the attacker." And you never want to have your allocations decided by the attacker.

Leo: By the attacker, that sounds bad. I don't know what it is...

Steve: Really not a good idea.

Leo: ...but it doesn't sound good, yeah.

Steve: We're only going to allocate a little bit, but we're going to write a lot and just see what we stomp over. And that of course is the way you overflow the heap. And he says: "...and the copying of another arbitrary amount on the same buffer." So, yes, that's about as bad as it could get. That's in the rvrender.dll. I checked. They have no updates as of the recording of this podcast. Hopefully they will get onto it. The nice thing about Real is that they're not trying to make any claims as to, well, we're only going to update quarterly, so hold onto your seats in the meantime. So they'll fix it when they can, although I think I also just, it flew by my eye on the news a couple days ago, that they've just lost their CEO.

Leo: Yeah, their CEO quit after a year. Rob Glaser, the founder of RealNetworks, quit a year and a half ago. Replaced him, that guy just quit.

Steve: Yeah.

Leo: Doesn't feel like a vital, growing...

Steve: Ongoing enterprise.

Leo: You know, they tried, last year they announced kind of a complete pivot on their business model. I don't even remember what it was. It just was - it was odd. And I think it's obviously not going so well.

Steve: And when I went to their site to see what they had to say about this, there's, like, all this other stuff going on. It's like, okay. There's, like, nine different things they're trying. Essentially, they were first, to their credit. Rob left Microsoft and founded Real. And they were out there early. Unfortunately, they really upset people who cared by over-commercializing their player. I mean, it's like spyware before spyware existed. It was really nasty. And so they got a bad reputation and really created an opportunity for other alternatives. So I just think their day is probably past.

Leo: Yeah, I think that's true.

Steve: Now, the big news this week I'm not going to address in today's podcast because it's going to be the entire topic for next week, because there's so much interesting detail about it. And that of course is the rogue SSL certificates that were issued by a reseller of Comodo. Comodo is one of the trusted certificate authorities in all of our browsers. And a collection of alarming sites, I had the list earlier this week, and I've got it in my notes. We'll go over it in detail next week. But, I mean, like, Yahoo! and Google and a few other very high-profile domains had SSL certificates issued maliciously.

Now, some rumors are, for example, that it was hackers in Iran, or even maybe acting on behalf of the state because, as our listeners know, essentially what a rogue SSL certificate allows you to do is impersonate that site. But other people have said, wait a minute, that's only part of the game because you've got to get the person to go there, like to the wrong server, in order for that server, the rogue server, to serve the rogue certificate. But if you're a country, and you control the borders of your traffic, then you don't need to spoof IPs; you don't need, like, a DNS attack or something. You can essentially put up a proxy, and no one within your confines would know that they weren't actually going to that correct site. And SSL would not function in terms of keeping privacy.

So, anyway, really interesting topic. I didn't want to ignore it, but I wanted to give everybody a heads up. We're going to plow into that. And we've never talked about revocation because the SSL certificates were quickly revoked. To their credit, Chrome immediately revved their browser, blacklisting the bad certificates.

Leo: Good.

Steve: Microsoft, yes, Microsoft immediately produced a Windows update.

Leo: That's where the automatic updates of Chrome have a huge advantage.

Steve: Really do.

Leo: Because it happens instantly, automatically, without your involvement. Who knows who updates Windows, and how often, you know?

Steve: Yeah. And in fact I immediately tweeted to my followers the link to Microsoft's page, where there was just a menu of OS versions. Each OS version had its own little DLL or EXE that you could download. And so Microsoft immediately pushed out a bunch of updates also to deal with this. And I did see something interesting saying Mozilla sort of ignored the whole thing, and after the fact now is unhappy that they weren't more forthcoming about it.

So anyway, we're going to go into this in detail because we've talked about this before. Remember my shock when I looked at the number of certificate authorities that our browsers now trust. Famously, we used to joke about the Hong Kong Post Office being among them. And so this is what happens when you have this kind of problem. So that's our topic for next week. We're going to cover it in detail.

And then just a little bit more on the RSA SecurID breach. Pretty much everyone's upset. And one quote that I really liked from the SANS Institute. Alan Paller, who's a friend and very well-connected director of research of SANS, wrote in their most recent newsletter, he said: "One of the largest defense contractors has stopped the use of RSA tokens by its senior staff."

Leo: Oh, that's how serious that one is.

Steve: Yes. "They replaced the tokens with another manufacturer's solution. I asked," says Alan, "I asked whether the move had been planned for a long time. The answer was, 'No. We did it because of the breach.'" So, I mean, as I said, and as I blogged when this immediately happened, it could only be one thing. The secrets that they were being entrusted with were the secret key to public serial number mapping database. And there's only one way the SecurID system could be weakened, and that's if that's what got out.

Leo: Well, that proves it.

Steve: And it sure looks like that's what got out, yeah. Also in the news, we've talked about of course Stuxnet, that - I mean, we did a whole podcast on it - famously was used to deliver the first rootkit to the SCADA system, which is an acronym standing for Supervisory Control and Data Acquisition, which are the process control technology which in this particular case of Stuxnet was running Iran's nuclear enrichment process. We talked about how it was some vulnerabilities in that software that allowed Stuxnet to do its work.

Well, what I found interesting was the news that 34 new exploitable vulnerabilities had been found in these SCADA systems, produced by a handful of different manufacturers. And this is a classic case of there are vulnerabilities everywhere. And all you have to do is look for them, and you find them. So these SCADA systems hadn't, until Stuxnet, focused people's attention on them, hadn't been really looked at closely. Now security researchers are going, oh, you know, Stuxnet found some problems. What other problem might there be? And, oh, what do you know, here's 34 in two weeks.

Leo: I bet that, you know, people don't treat this kind of stuff as as insecure as, say, a PC is. They just don't think of it that way.

Steve: Correct. Correct. And there is some awareness, for example, we're seeing that there's sort of an awareness that you can't have, you cannot have a Windows machine on the network. So these SCADA machines that use Windows as their front ends, like the way the workstation that you use to program the lower level process control hardware is Windows hosted, but everyone knows that's not safe. So those machines are kept off of the network. But as we learned with Stuxnet, it cleverly used USB drives because you still have to get files to and from those machines. So they just used a USB drive rather than a network and, bang, same effect.

So anyway, I got a lot of email from people saying, oh, no, no, what does this mean, 34 more problems. It's like, well, this is significant because these SCADA systems are what run our nuclear reactors and our dams and factories. Leo, when you were famously touring Ford's production lines, building cars, all of those robot arms are controlled by these things.

Leo: Ooh, imagine that getting - ooh.

Steve: Ooh, not good.

Leo: Yeah.

Steve: Yeah, I remember when I was at the - this was back in the '70s at the AI lab at Stanford. They had a robot arm behind Plexiglas shields, and there was like a rope around it with limit switches. And I remember the first time I saw this, it's like, what's that about? And they said, well, do you know what happens when there's a bug in our software? I mean, this thing was hydraulically powered, and apparent- and I heard stories about it just literally pounding its own table into the ground when there was a bug in the software.

Leo: Oh, boy.

Steve: So anyway, so it will end up having been a good thing, in the same sense that Firesheep has been a really good thing for HTTPS and for vendors getting themselves, taking SSL security more significantly. Stuxnet, which was tightly targeted at the Iranian nuclear enrichment, we now know without a doubt, it had the beneficial effect of turning attention to the security of these SCADA systems, which you can imagine attackers, maybe they're getting a little bored these days. It's like, well, let's open the floodgates on the Hoover Dam because they're there.

Leo: Be kind of cool, yeah.

Steve: Yeah, well, you know, what a hack that would be. Oh, anyway, so.

Leo: You'd get a lot of attention for that. I mean, never mind, bad idea.

Steve: Bad idea. But anyway, we are - the problem is, these systems have not had the kind of security scrutiny that Windows has because no one's been looking at them. And when you do, what do you know, 34 exploitable vulnerabilities. And then in perhaps my favorite little "whoops" of the week, Oracle's MySQL.com site, MySQL site, was breached through a SQL attack.

Leo: Oh, please.

Steve: There was a great little posting that I'll read on the H Security site. It says: "MySQL allegedly hacked - via SQL injection. On a security mailing list over the weekend, an unknown party published details about the structure and content of databases on the website of database vendor MySQL." Which, you know, is not public. None of that information is meant to be public.

"The information was apparently accessible via a security hole on the MySQL.com website. The hacker says the vulnerability is a blind SQL injection problem. This is a worst-case scenario for a web server because the flaw allows access to the entire database behind a public-facing website. SQL injections are possible when SQL commands can be embedded in user input so that Web servers pass them on to the backend database. Blind SQL injection means that the result of the database operation is not displayed; in other words, the attacker has to work blindly.

"In such cases, hackers therefore often ask the database yes/no questions and link one of the answers to a time-consuming operation. Depending upon how long it takes the resulting page to appear, they can then tell what the response to the query was." So, I mean, it's classic, beautiful hacking.

"Among other things, the data made public includes password hashes for database access, and some of the plain text passwords behind them have already popped up on the Internet. Oracle, the database vendor that acquired MySQL when it bought Sun Microsystems in 2010, has yet to comment on the matter." So anyway, even the database vendors are vulnerable to database injection.

Leo: Well, if there's a MySQL problem, of course who's going to be running MySQL? I'd say the MySQL website. First place I'd go.

Steve: Exactly. Now, I did want to mention in miscellanea that I got a number of, I don't know what to call it, feedback for lack - I won't characterize it anything other than that, to my reference to "toy operating systems" last week when I talked about...

Leo: How dare you call my operating system, whatever it might be, a toy?

Steve: Exactly. And people said, like, well, and you're using XP. And it's like, well, yes. That's true. Because that's what everybody else is using. I would love to be using UNIX, but then I'd be all...

Leo: When Steve retires, he'll be OpenBSD all the way.

Steve: Precisely.

Leo: Or whatever. Is it NetBSD? I can never remember which one is the one you...

Steve: It's Free is the one I'm...

Leo: FreeBSD.

Steve: FreeBSD. We're being subjected to emergency, out-of-cycle updates pushed on us constantly. We update monthly from blindly accepting what Microsoft gives us. If we visit a bad website, we could be taken over. Mysterious things happen all the time on our systems, and we just sort of shrug and reboot them. I mean, my icons all turn into something different, and I go, okay, fine, it's time to reboot because I haven't for a week or two. And just ask anybody who does PC support. They never see the same thing twice. Users bring computers, well, I can't get on the Internet. Well, I can't print anymore. Well, Notepad doesn't work anymore. Well, IE won't open. I mean, it's one thing or another.

Leo: Oh, believe me, this is what I hear on the radio show nonstop.

Steve: These are toys. I mean, it's just - this is not, I mean, and the fact that we're used to it doesn't make it right. This is, I mean, the systems that I have that are running GRC haven't been rebooted in four years. I mean, it took a long time to get them that stable. It was really hard to do. But, I mean, they are rock-solid actual operating systems that are not like this, where it's like, oh, I downloaded some patches, may require reboot. When has it not required a reboot? May? Ugh. No, I mean, it's just, it is full employment guarantee for anybody involved with these things, anyone doing PC support. As you mentioned, you on the radio show, Leo, I mean, it's just - it's endless.

Leo: It actually makes me nuts because I feel like people, quite rightly, normal users have been sold this idea that they can use technology easily, safely, reliably, and change their lives. And then unfortunately what the reality comes down that they have to become security experts, they have to become geeks, they have to become enthusiasts or rely upon somebody else.

Steve: And learn not to click links. You know, Mom sent me some very well-meaning birthday cards...

Leo: Oh, I hate that.

Steve: You know, it's like...

Leo: She gave your address to everybody.

Steve: I know. So my email address is out there. And I didn't open them. She said, "Honey, didn't you get those?" I said, "Mom, we've had this talk before. I will not open those."

Leo: I know. Well, and...

Steve: "I don't know what they are." And she said, "Well, what do you mean?" I said, "Well, Mom, their site could have been compromised. People's sites are being compromised all the time."

Leo: That's a good point. It doesn't have to be a malicious vendor. They could just be hacked.

Steve: Well, like Oracle was. And who was it, oh, McAfee, it turns out their McAfee site is riddled with - it was just - this was in the news this week - riddled with security problems.

Leo: Oh, that inspires confidence. Geez. But that's the thing that - and by the way, this is why Apple sells the iPad in droves and will sell more and more and more, is because people are really frustrated and puzzled and baffled, and they don't know what to do. These complex operating systems are just too hackable.

Steve: Yeah, actually, Leo, I've got to tell you, I have opened some sketchy things on an iPad because it's a safe little contained environment.

Leo: Well, we hope. I mean, I'm sure there's exploits there, too. But...

Steve: Well, I've done other good, other safe things, too. But, yes. But, I mean, it's...

Leo: It's not nearly the complex system that a full operating system is.

Steve: No. I mean, and so in Microsoft, in defense of the toymaker, I will say that these things do everything. I mean, anything you could ask for.

Leo: Right. And that's part of the problem. A full general purpose computer is inherently complex and requires a complex priesthood to maintain.

Steve: And the highest level expert there is has no idea what most of the files are on these systems. Huge teams all submit their blobs. And then the only way Microsoft can know that it kind of might work is when they put it out and have it tested extensively. And when they ship it, it has tens of thousands of known problems at release time because, oh, well, we called Windows it 2000; and, shoot, it's November.

Leo: Well, and they can't help it. I mean, there is no perfect OS, so there's never a point where you have a bug-free OS to ship. You'd never ship.

Steve: Well, and decisions have been made, like, oh, we need more performance, so we're going to move the graphics system, which used to be out in user space, down into the kernel. Well, we know what happened with that, you know, bad idea.

Leo: So the thing to do is make what the iPad essentially is, which is a system that keeps users from doing anything. You can't put files on an iPad. You can't, you know, the dumber the system...

Steve: And what do we hear? We hear complaints from people that the iPad doesn't have a real file system.

Leo: Well, that's why.

Steve: It's like, yeah, I mean, you can't have it all. So did RSA learn a lesson? Oh, my god. Can you imagine they're going to change their architecture? Absolutely. Some people wrote saying how could RSA, I mean, we sort of hold them up as, like, this ideal of, well, they invented public key security. How can they make a mistake like this? It's like, they're using Windows. It's a toy. It's junk. Yes, we're all using it. I'm using it. I don't like it. But...

Leo: There it is.

Steve: It's where everybody is.

Leo: Right.

Steve: Yeah, I would love to be, oh, my god, do I pine for the days of a textual interface and commands. Yes. But I'm not useful to anybody if that's what I'm doing over in the corner somewhere. So, okay. That'll teach you, that'll teach you for asking me about toy operating systems.

Leo: Well, no, this is - look. I don't know why, but people treat this like team sports, like rah, rah, my team's the best. Go team, go team. And it isn't a team sport. These are just tools. And it's silly to say this hammer is so much better than any other hammer. If the head comes flying off and pokes you in the eye, it's a toy.

Steve: It hurts, yeah.

Leo: Period. Doesn't matter if you love your hammer. It doesn't love you. It's just a tool.

Steve: Okay. So I did want to mention something very cool, which is Amazon's announcement of a virtual machine-based Android test-drive system.

Leo: I'm very interested in this, yeah.

Steve: Oh. It actually, when you go to Amazon's site - Amazon of course released their AppStore. I notice they're spelling it as one word. Maybe the...

Leo: Which Apple does, as well. That's why there's a lawsuit.

Steve: Oh, okay. I didn't realize Apple was - because I had seen it as two words for some reason.

Leo: Oh, no, it is two words on the Apple site, you're right. But I don't think that makes any difference.

Steve: Good luck with that, Amazon. So anyway, this is very cool. They have that EC2, the Elastic Cloud computing technology.

Leo: So cool.

Steve: And so Amazon is, I mean, they're doing many neat things. They also just announced a couple days ago a music in the cloud system. It's limited to the U.S., whereas their cloud drive technology for storing stuff is global. But the music-based system, at least for now, is only U.S. based.

Leo: That's just because of licenses, you know.

Steve: Yes.

Leo: You've got to get every record company in every country and, oh.

Steve: But, so, for example, users can upload 5GB of music, which actually is a pretty nice little collection. And then it's available on Android players or PCs and Macs and Linux machines. So you're able to just, like, stream music from Amazon's cloud. Well, they've gone one step further. They actually have created a virtual Android OS. And, I mean, it must be that they're going to be producing a tablet. It's just...

Leo: There's no doubt about that.

Steve: There's just no doubt about it any longer. And arguably they have the chance to be a real mover in the industry.

Leo: I think we talked about this yesterday on MacBreak Weekly. And I don't think Google minds. I think Google says, go for it, we'll help you. This is good. They don't want to be the marketplace. They want to be Google.

Steve: Right. So one of the things that has annoyed me with the iPad is there is no trial software. I've got all kinds of crap that I've purchased for a buck or two or three, and it's only the low cost...

Leo: 99 cents, yeah, okay, so if it's a piece of crap...

Steve: It's like, yeah, okay, fine.

Leo: I guess I'm out a buck, yeah.

Steve: But there's so much junk. It's like, oh, how do I get rid of this thing? I mean, it's like, okay, well, there went a dollar, there went two, there went three. So it is annoying that Apple doesn't do this. Well, so what Amazon has done...

Leo: And by the way, Android always has. You've always been able to - they had a refund process. They've shortened the length of time. Used to have a day to try something. If you didn't like it, and you deleted it, it would automatically give you your money back. Now they've cut down to 15 hours, which is why I'm glad

Amazon's doing what they're doing. This is really a good idea.

Steve: So they literally launch an Android VM instance using their elastic cloud computing technology. And their servers run the app for you and then download the display dynamically to your web browser.

Leo: Brilliant. I love this.

Steve: Oh, so you can click...

Leo: It's probably just EC2; right?

Steve: Yeah, they're using EC2. And so you can click things, you can play with the app on your web browser, not installing any software, I think it's like 30 minutes because I saw in their sample it said "29 minutes remaining" in the lower right-hand corner.

Leo: That makes sense. Yeah, that makes sense.

Steve: So you get, like, 30 minutes just to poke around and, I mean, actually use it virtually, not even download, not buy it, not commit, not trial. Just there it is running. But if you want it, then you click the little famous Amazon orange "yeah, I need this" button, and you can buy the Android app. So this is very cool stuff they're doing. I just wanted to bring it to our listeners' attention.

Leo: Yeah. This is, well...

Steve: What?

Leo: I sit on MacBreak Weekly, and people get mad at me because I say, look, it's finally - like Andy Ihnatko's finally saying, you know, this Android's not so bad. And it's like, I've been trying to tell you this for [frustrated sounds]. There are so many great features in Android phones. And I think people, you know, just because Apple was first with iOS there's a little bit of a prejudice towards iOS.

Steve: A blindness, yeah.

Leo: Now, I admit tablets we've got a way to go, but - "we." I don't want to say "we." Again, that's that team mentality, isn't it. My team has a way to - they've got a way to go. But I think for phones this is a pretty amazing system. And I'm very interested to see how Amazon enters this. They could change everything.

Steve: Yeah, yeah. They're big.

Leo: They know how to market. They know how to do this stuff. They're smart. EC2 is amazing. S3 is amazing. These guys do more than just sell books.

Steve: Yes, they really, really have broadened their reach. Speaking of which, American Express has launched Serve.

Leo: This I'm also really interested in.

Steve: Yes, a very interesting-looking PayPal competitor. We've often talked about there's no company more in desperate need of competition than PayPal. And American Express has come along and done that. So I just wanted to put that on our listeners' radar that there is something from American Express. I read a comprehensive review, and it sort of seemed like six of one, half a dozen of the other. Some things PayPal charges for, some things American Express doesn't. Some things American Express does that PayPal doesn't. And different things, they work a little bit differently. But essentially it looks like American Express is very interested in getting into this game in a serious way. So...

Leo: It's about time PayPal had some competition. They're just so, really so bad. And I use it because there isn't a lot of choice. If there were something better - Google payments is pretty good. But Amazon has a system. But I think American Express is a great financial services company.

Steve: And many people have said, hey, Steve, I trust you and all, and so I gave you my credit card information when I had to buy a copy of SpinRite. But why couldn't I use PayPal? And it's like, well, I use PayPal as an eBay customer, buying old computers and things, and I've had no problems with them. But we had a perfect case in point, those little PDP-8 models that you see running behind me while we're doing this podcast. The guy that produced the kits - remember when we were organizing a big group purchase to prepurchase a bunch of kits.

Well, a whole bunch of people sent him their money. And after a whole bunch of it accumulated, PayPal shut it down and then demanded all kinds of ridiculous paperwork, saying, well, you can't take money for a product you haven't delivered. You have to deliver the product. And he tried to explain to them that everyone knew that this was prepayment to get enough to see if we had enough orders to proceed, and if not all their money would be refunded, blah blah blah. I mean, it was a huge nightmare. And the industry has horror stories about vendors that have had massive problems with PayPal. And so there's just no way I'm going to subject myself to a third party where you can't get actually anybody responsible on the phone.

Leo: Well, we use, you know, that's how we take donations just because it's the simplest, the easiest, Drupal, the web...

Steve: And for that it makes so much sense.

Leo: And the web, everybody uses it, you can use a credit card. Drupal supports it with a plug-in that makes it very easy. I do this all by myself, that's how, you know, in the earliest days I had to figure out how to do this. But I think it's time, in the next generation, for us to look at alternatives. And I just knock on wood that we haven't had a frozen account or, you know, we've had no problems so far.

Steve: Yes. And American Express is a name everyone has heard of.

Leo: Oh, yeah, everybody would trust that.

Steve: Yeah. So I think that's - it really makes a nice step forward. I hope they just don't screw things up or have any real bad breaches and so forth.

I did get a nice note I wanted to share briefly with our listeners. Christian Alexandrov, who's in Sofia City, Bulgaria.

Leo: Yeah, baby.

Steve: As you can tell from what I'm about to read, English is not his first language. But I salute him because his is much better than my Bulgarian. So he says, "Hello, Steve. SpinRite saved my St. Valentine Day." He says, "A friend of mine is a restaurant owner who uses very old Compaq Presario M2000 laptop, Intel Centrino mobile CPU, a 1600, 1GB of RAM, so forth. The owner called me to go there on emergency call because his laptop just died in his hands while browsing for some recipes for the restaurant's chef for the St. Valentine Day menu. I went there as fast as possible to see the corpse." Meaning the laptop, of course.

Leo: Yes, yes.

Steve: "He assumed motherboard died, but quick tour around BIOS settings showed that this assumption was wrong. I suspected the hard drive on such old computer. I took the laptop home and started to mess around with files settings. My phone rang, and he said, 'Look, I have important files on that drive.' 'Do you have backup?' was my first question. He said [LEO: No.] no."

Leo: It's universal. Nyet.

Steve: Nyet. "Then he says he needs these files at all cost. So I told him I will do best to help him. He promised me that if I pull this stunt through, I will have the entire St. Valentine evening free, unlimited amount food and drinks for the whole evening for free, and music of my choice for me and my girlfriend."

Leo: Good way to make friends.

Steve: "So I booted this messed-up laptop from my SpinRite boot" - with three o's, that threw me for a minute - "booot CD, and I chose to run at Level 4. Once I saw that SpinRite took matters in its own hands, I went to the restaurant to set up a nice surprise, a gift and flowers for my beloved girl, and a nice Valentine cake. It took SpinRite 17 hours and 30 minutes to process the whole drive. At the end SpinRite says this drive has long years of faithful service ahead."

Leo: Really? Is that a message in SpinRite?

Steve: No, but it does, the SMART system does show you how the drive's doing.

Leo: You have long life, my friend.

Steve: He said, "And now the computer booted, and all of the drive's files were saved."

Leo: I love this.

Steve: "I was surprised as much as I could be because of the old model and age and obvious abuse of the laptop. So I updated everything, ran various tools, I backed up the files, I fixed the partitions and so on, updated Windows system protection such as antivirus, and set up" - oh, so he really spiffed the thing up - "XP SP3, firewall, and I connected the laptop to my router so I could update the OS. While I am waiting all updates to come and install, I decided to share this story with Security Now! listeners."

Leo: That's great.

Steve: "I brought the laptop to its owner, and he tested it. He was happy to see all his files intact and the laptop working fine. Thank you, Steve, for this great piece of software; and thank you Steve and Leo for this upstanding podcast. Best wishes to both TWiT.tv and GRC.com from a happy SpinRite user."

Leo: I love that.

Steve: So thank you, Christian, for that great, great story.

Leo: That is just great. And I'm glad you didn't fix the, I mean, his English is excellent. But we could hear his voice coming through, which I love, yeah. I love that. Christian, thank you for listening to the show, too. That's wonderful.

Steve: Yes.

Leo: All right. We've got questions, 10 good ones, plus a couple of freebies we're going to throw in at no cost to you. Now it's time on Security Now! to answer questions to Steverino. By the way, people ask me, how do I ask a question? You go to GRC.com/feedback, fill out a form, Steve will look at it. You don't answer them individually, I know, but you couldn't.

Steve: Yeah, we got - I checked the mailbag, and there were more than 300 from last...

Leo: You'd spend the rest of your life.

Steve: ...from two weeks ago. So...

Leo: But you take representative samples.

Steve: Yup, I do. I sort of see, I sense the wind. In one case, I think #8 here, we've actually got two questions in one because they were two different people asking almost the same question, but with a little bit of a twist. So I sort of try to combine them and find something representative and try to do what I can.

Leo: Well, here you go. This is Question 1 from Patrick Pater, London, England. He says drive encryption is killing him: I'm a long-time listener of Security Now!, Steve. I enjoy it as a good source of information and amusement. I hope he's not laughing at us. Being a software developer for many years, I put an effort into keeping my data secure. The machine is a T9400 running SuSE Linux, using until recently his 200GB 7200 rpm full-disk encryption hard drive.

A couple of weeks ago I switched to an SSD drive. Wanting to keep my data still secure, I performed full partition encryption on the drive using openSUSE's encrypted root file system how-to. However, the amount of CPU power needed to decrypt and encrypt data on the fly was through the roof. Don't get me wrong, thanks to you and Leo know a thing or two about how encryption works and of course that it comes with a price. But can you advise a reasonably usable crypto that won't cost an arm and a leg? I got this SSD for speed, and I'm not getting it.

The drive stats for non-cached read timings, full disk encryption, the old style, around 50 MB/s. That was on the standard drive. On an SSD unencrypted, 220MB/s. But now with encryption 70MB/s, so that's a lot slower. Thanks for a great show and SpinRite. B.S. - P.S., not B.S., P.S.: Thanks to you, my private project SpaceBench.com now accepts Bitcoin. That's great. So that's interesting. And, well, what do you think?

Steve: Well, okay. When I was playing with TrueCrypt I was unable to measure a decrease in speed. And I did, I mean, I remember talking about it extensively on the podcast we did about TrueCrypt, and I was very impressed. It seemed to me that on the machine that I was using, which wasn't particularly muscular, that the overhead of encrypting and decrypting was fitting underneath the speed of the drive so that, while the drive was reading data, the AES-based encryption was as fast as the drive was, so that we weren't seeing a substantial overhead from that process.

Now, he went from unencrypted 220MB/s to an encrypted partition at 70, so it's about a three-to-one difference, like it's running a third as fast. His SSD is still going faster than his old mechanical drive was; but if he weren't encrypting, the SSD would be going more than four times faster than the mechanical drive that was running at 50MB/s as opposed to 220. So my feeling is that it may just be that the encryption technology that he's using is, for whatever reason, not as tightly optimized as what TrueCrypt has done.

I know, because I looked at TrueCrypt very closely, that they've got a ton of code that is in assembler. All of the speed-critical stuff, all the crypto has been hand-coded and hand-tuned in assembler so that specifically to reduce the overhead as far as possible. If, for example, the encrypted root file system technology he's using had stayed in C, it would be secure, but easily a fourth the speed of it being written by hand in assembler. So it might just be that it has not been optimized. The thing that I wanted to...

Leo: I think it's TrueCrypt. I'm looking at the how-to.

Steve: Really.

Leo: Well, this is an interesting question. I guess you can choose from different systems. Maybe he's not using TrueCrypt. Yeah. TrueCrypt, though, is one of the choices that they talk about in this article that he's mentioning.

Steve: Oh, okay. Because he says SBD. Don't know what that says, SBD encrypted root file system.

Leo: Yeah, I don't know what that is.

Steve: Well, and does TrueCrypt do whole-drive encryption? Maybe that's not available over on that platform.

Leo: I think it does, yeah.

Steve: Okay. In that case, one thing you could do, Patrick, if it's feasible for you, and you're not using TrueCrypt, is try switching to TrueCrypt, where at least on a PC platform it's really fast. And more generally what I wanted to suggest is, I don't think we're there quite yet, but...

Leo: Oh, yeah, wait a minute, yes, he's using cryptsetup instead of TrueCrypt. The how-to describes cryptsetup. So he's using a simpler, less sophisticated system.

Steve: Okay.

Leo: There's three choices: cryptsetup, loop-AES, and TrueCrypt. So he should just change to TrueCrypt.

Steve: Great, yes, perfect. And I did want to say that we're not quite there yet, but I don't think we're far away from all hard drives having on-the-fly AES encryption in their hardware. So it would not be something that is enabled by default. It's not something you would be able to add after the fact. You'd have to set it up and establish it before you loaded an OS or anything. But the idea is, and we've talked about this at various points along the way, the idea is that everything written would pass through the encryption; everything read would pass through it to be decrypted; and, at boot time, the drive would be given the key which it would have internally that allows it to do the encryption/decryption.

The beauty of that, whether it's on a physical hard drive or on an SSD, is it solves everyone's concern about these drives being difficult to erase, that sectors have been spared out that are no longer accessible that might have a piece of important data on it, or the SSD's drive leveling might move some data somewhere else that it hasn't erased, that forensic analysis could get. But if everything is encrypted from the beginning, then when you remove that key from the drive, the entire thing is filled with noise that is no good to anyone.

So, again, we see this in some laptops and in some drives. It's not universally available. It's something that really has to happen. And the other problem is, since it's not something you can add incrementally, the drive, if you're getting it from a manufacturer, it has to have been set up that way at the time that it was manufactured. And then you've got the problem of the manufacturer's technically having the password for the drive. So, I mean, there are some logistical problems with implementing it. But for people who are really concerned, once the hardware is there, we'll at least have the ability not to leave data behind when we decommission hard drives or solid state drives.

Leo: Kill that slack space.

Steve: Yup.

Leo: Moving right along to - actually now I've opened - I blew it. I opened up that Linux article, and now I don't see the questions anymore. Let me go back, back out, back to our wiki. Here we go, Question 2, an anonymous listener wonders, old Internet Explorers, will IPv6 kill them? Listening to 292, you're talking about Microsoft's attempts to kill IE6. I saw a job description today that included website testing with - ready, wait for it - IE5. But are these old versions of Internet Explorer IPv6-ready? Were they designed to be protocol agnostic enough? What about old Netscape browsers or old game consoles like the Xbox and PS2? What happens with them and IPv6?

Steve: Really good question because in many systems, for example, like an Xbox, you'll see configuration data that has the dotted quad IP address. It's 192.168.0.1, or it's DHCP that knows nothing about IPv6. It knows how to get a dotted quad IPv4 IP. So the question is, when IPv6 is being delivered from our curbs, curbside, what happens to all of this equipment that we've got that predates it? And that's just one more example of why this is a challenge and why people are going to be going kicking and screaming to IPv6. I believe what we're going to see is this will be something that befalls our NAT routers.

Leo: Yeah. There's something called "tunneling."

Steve: Exactly. There are all, I mean, it's a confused mess. And when we finally get to our How the 'Net Works, we'll certainly be spending a lot of time about the whole IPv6 to IPv4 transition. And I'm sure we'll be talking about it a lot this summer and in the fall as this becomes more and more important.

But what's really funny is that this is exactly what all the IPv6 proponents didn't want. The original concept of the Internet was every device has its own IP address. And we were supposed to have plenty because, after all, we had four billion, 4.3 billion in a 32-bit address space. But chunks of that space got allocated for other things. And turns out we need more than that many, so we have to go to a larger bit size for the address. So we're going from 32 to 128 bits, giving us really a lot. I mean, 340 with an amazing number of zeroes after it is 2^128 power different IP addresses.

So the problem is that we still are carrying the legacy of IPv4 which I would argue in our lifetimes will never go away. There will be all kinds of systems that stay on IPv4. So what does our NAT then do? Well, what it's been doing for us up until now is converting a single public IP address into a personal network of IP addresses. What it will next-generation do is convert IPv6 down to IPv4. And there's no reason it can't. It's simple to have hardware translation that works in the same nature as port translation and IP address translation works, that right now NAT routers are not translating the format of the packets, they're translating the content. But they can certainly translate the format so that you would have a NAT router with an IPv6 public IP that would behind it still be running, and I'll bet they do, an IPv4 192.168, and nothing within our home networks would know the difference.

Leo: A lot of the, if you get, you know, Hurricane Electric right now will give you an IPv6 setup. In fact, Randal Schwartz is boasting he's got like a Class C IPv6 network, or Class B, because it's - why not? There's so many addresses, go ahead.

Steve: I don't think they allocate on smaller than a certain, I mean, a large chunk. You get, like, 65,000 IPs. Like, okay, that ought to hold me for a while.

Leo: So if you go to TunnelBroker.net, you can go - this is free. Hurricane Electric is one of the big, they're like Level 3, they're one of the big backbone companies, big Internet service providers for Internet service providers. And what you can do is, for free, get your own IPv6 by tunneling over existing IPv4. And it's, you know, actually Randal did it because he just wants to kind of test it and play with it and learn about it. And so it's kind of interesting. So TunnelBroker.net, and you get your free IPv6 tunnel. And everything will continue to work. Your hardware doesn't stop working. It's just it's seeing IPv4 over a tunnel. And actually the IPv6 is going over an IPv4 tunnel. So it's crazy.

Steve: And I've asked my Level 3 guys about IPv6, and they're ready to give me a block any time I need it. I've asked my T1 providers, Cogent, and the hardware that terminates my T1s is not currently provisioned for handling IPv6. But the neat thing is one of the engineers is one of my old friends from the Verio days, and he is going to be lobbying for the importance of switching over because I'd like to have IPv6 natively flowing in here so I can do a bunch of experiments and prototype technology that I'll need ultimately to move over to GRC.

Leo: Yup. I'm sure that's what Randal's doing. It's also got great bragging rights. "Oh, yeah, I'm running IPv6. All through the house." Good question. I think that in fact there are a lot of people, I've talked to a number of people, including Dane Jasper, who is our local Internet service provider here, Sonic.net. They provide the big pipe that we use to stream and everything. And he says, you know, he's not convinced it'll happen at all, that they'll just - there'll be these hybrid solutions. There'll be ISP tunneling and so forth.

Steve: Yes.

Leo: ISP NAT, they call it, so that you get IPv4, but they do IPv6, things like that.

Steve: Well, for example, there are, when I was talking - I did a conference call with the Level 3 guys. And I had a technical sales guy on the phone who said, oh, yeah, large corporations are switching to IPv6. They're using it internally.

Leo: Internally; right.

Steve: Exactly. But externally they're still running over the IPv4 backbone, and they're contacting IPv4 websites. And like I'm sure GRC will always be on 4.79.142.203, which is my www.GRC.com's IP address. They're not going to take those away from me. I want additional ones because it would be very cool to be able to do native IPv6 and check people's ports.

Leo: Oh, yeah, for ShieldsUP! and things like that you need to do that, yeah.

Steve: Exactly.

Leo: Michael Noone in Circleville, Ohio has an update on Facebook and HTTPS. Remember, Facebook went HTTPS.

Steve: Kinda.

Leo: But then it turns itself off at the drop of a hat. A long-time listener, first-time commenter. I'm not sure if you covered this. I was on Facebook today, received the following message when I attempted to access an app: "Switch to regular connection (http)? Sorry! We can't display this content while you're viewing Facebook over a secure connection (https). Would you like to temporarily switch to a regular connection (http) to use this app? You will have a secure connection" - oh, this is a change.

Steve: Uh-huh.

Leo: "You will have a secure connection upon your next login." Looks like they are trying to fix - so we mentioned a few weeks ago that once you turned it off, it just stayed off. Like you turn it off for an app so you can use an app because a lot, most apps don't do it. And so you're using Farmville or whatever, it turns off, and then just stays off. So this apparently will turn it back on.

Steve: Yes.

Leo: Looks like they're trying to fix the issue about having to shut off the secure connection completely. I did need to log out of Facebook, which people don't typically do. But when I logged back in, it was back to HTTPS. Thanks for a great podcast.

Steve: So that's great news. I wanted to update our listeners that that was fixed because a number of people wrote to me and said, eh, not so much, Steve, and then verified that http setting was disabled if you acknowledged that little dialogue box. It unset it, essentially, in your configuration and left it that way. Now, as you say, it's a little bit of a problem that you have to log off in order to have it back. On the other hand, what they're protecting people against is logging on in an insecure WiFi hotspot.

So the good news is that this really does look like, if you were to log on freshly, it will preserve your security. Of course, you still have the danger of applications forcing your whole session into HTTP. That they need to fix because you ought to be able to use Farmville over HTTP but maintain the security of HTTPS everywhere else.

Leo: So you're saying it's a weakness in their implementation.

Steve: Yeah. And it may be, I mean, Facebook has so much money, they're hiring people right and left, and I imagine they can get this fixed. The good news is it really does, this really seems to be on their radar. And I'm glad they're moving forward. So that's just good news.

Leo: Yeah. Question 4, Rommel in San Diego wonders about the LastPass virtual keyboard. Hi, Steve. I'm wondering how secure it is to use the LastPass virtual keyboard when I login to LastPass? Let's say I have to use a computer that I'm not familiar with. I don't have my onetime passwords. My phone is dead. Is using the virtual keyboard safe? LastPass says keyloggers can't detect what is entered using that keyboard. That's the whole reason they have it. What do you think?

Steve: Well, okay. So basically he's painted himself into a corner where he's using a computer that he doesn't control, and he doesn't have one-time passwords which LastPass provides as sort of an escape hatch for this purpose, and his phone is dead so he can't use telephone authentication. So he's backed up against the wall with their virtual keyboard. Well, so one thing I have to say is, well, what choice do you have? It's the only other way at this point to log in.

Leo: Well, you could not log in, I guess.

Steve: Yeah. And it is the case that they did not implement this virtual onscreen keyboard through the keyboard interface specifically so that keystroke loggers could not detect it. So all that's happening is that there's JavaScript there which is capturing mousedown events in coordinates and translating that into keystrokes. So that's about as secure as you can be given the situation you're in. The problem, of course, is that LastPass is still logging you into websites. And if the browser remembered your username and password that's being logged in, then those are sticky. So you definitely want to make sure you use a browser that offers private browsing so that you can create a session that will not leave breadcrumbs behind.

And then, yes, I think you can use LastPass's virtual keyboard with as much confidence as possible. I mean, again, if something malicious were in the computer designed specifically to intercept the virtual keyboard, it could because all software is software. But the chances of that are vanishingly remote. So I would say, as long as you, you know, you definitely want to use, always use a browser that offers a sandboxed private browsing option when you're logging into sites on machines you don't control so that it's not going to leave traces behind. And then LastPass is the way to log in.

Leo: Question 5, Joseph in Los Angeles has a VoIP hacking follow-up question: Steve, I'm addicted to your podcast. That's good. It's like free continuing education, but this is one class I really look forward to attending. Anyway, on to my question: I listened with great interest to your most recent Q&A #113, our last one. One of the questions had to do with being able to decrypt about half of a VoIP call. If you didn't hear this hack, it was a very clever hack using VBR compression.

My business has a PBX switch that allows us to connect a traditional office phone, multiple phone lines and the ability to intercom other employees and so forth, over the Internet. Instead of a traditional phone cable, we plug in an Ethernet cable. Actually that's the kind of system we're going to put into the new studios, using Asterisk, hosted Asterisk. We've had this since 2004 when I literally begged my phone vendor to sell me the equipment so I could have employees work at home and answer our phones. We were the first customer in Southern California to install this equipment.

The system has been incredibly reliable for seven years. I couldn't be happier - until I listened to the podcast today. At the time, the vendor thought I was crazy for worrying about people hacking our phone switch. I was really worried about a bad guy somehow connecting to our PBX over the Internet to make phone calls. I was insistent that the PBX only be accessible over a local 192.168 IP. Here's my question. Are the VoIP calls through a VPN tunnel able to be monitored using this technique? I've always assumed that our calls are private when on the VPN, but fully hackable over copper. Do I have anything to worry about or change? I'm very curious whether you and Leo gave me an A or an F for the way I set up access to the PBX. P.S.: I'd like to vote to make the podcasts even longer. You never waste our time trying to educate us. Interesting question.

Steve: Okay. Really interesting question. First of all, I salute, I definitely give him an A.

Leo: Yes.

Steve: For Joseph in Los Angeles for going to the extent that you have. I've also, when I did build this building that we were talking about earlier, had a phone system installed, and I remember, and I'm sure you do, too, Leo, there were a bunch of scams going on with people breaking into PBX systems and getting outside lines that then they would make transatlantic phone calls from. I mean, like, and this is in the day, back in the day when, you know, long distance was really expensive, so that you thought twice before you even dialed out of your own area code. And many corporate systems ended up clamping down by, like, disabling the ability to use an area code in order to prevent this kind of problem.

So just to refresh, the hack which he's talking about which has concerned him is that what was discovered was that variable bitrate encoding changes the size of the samples of digitized voice as a function of what's being digitized because some things can be compressed more than others. And an analysis showed that just by looking at the size of the data packets, about half of a variable bitrate conversation could be determined blindly, just, I mean, which is just really cool, speaker independent, I mean, just amazing cool hack.

Now, the good news is he's over a VPN. It's not clear, though, whether the packets will be varying in size after they're VPN encapsulated or not. And all other network traffic is sharing that same VPN connection, which would tend to mask the VoIP packets within the VPN tunnel. So, and if this system is, what, seven years old, it might not be using a variable bitrate codec. The older Asterisk systems were using fixed bitrate codecs, not variable. So if it's a fixed bitrate codec there's nothing to worry about because that's leaking no information in this really clever hack. Or, if there's other network traffic happening at the same time, web browsing or anything else, it sounds like he's got everything tunneled through a VPN, that would mix in with the VoIP traffic, and there's no way then that anyone on the outside - because the VoIP is going to be encrypted. So it's just going to look like completely opaque blobs of data that no one would have any way of dissecting further. So in general I think he's probably safe, partly because of the age of the system he's using that's probably using a fixed bitrate voice and not variable.

Leo: Well, also because it's a VPN, I mean, anything outside of his building is safe because it's inside an encrypted tunnel.

Steve: Except that, if the VPN, for example, if he's using UDP, the VPN might be just encapsulating the UDP packet.

Leo: Oh. I should mention that, because I always assume VPN's encrypted, it doesn't have to be an encrypted tunnel; right?

Steve: Doesn't have to be, but I think it probably is encrypted. But remember, that was the cool thing. That's why the hack that we talked about two weeks ago you could read, you could determine 50 percent of the conversation from encrypted VoIP.

Leo: Oh, right. But it sends tunnel. So that wouldn't affect the tunnel, or would it?

Steve: The idea would be that the packet length would be varying.

Leo: Oh, it would. So it would affect the tunnel.

Steve: Yeah, yeah.

Leo: The VPN doesn't pad?

Steve: The VPN pads, but it still varies.

Leo: Interesting.

Steve: So the VPN would have a fixed amount of padding, but the individual packets would still change in size depending upon their payload, which is encapsulated inside the VPN packet.

Leo: Wow.

Steve: Yeah. I mean, so it's possible that with a variable bitrate codec on a VoIP which is encrypted and then encapsulated in a VPN tunnel, that you could still figure out what was going on inside.

Leo: We should probably say that, although this method's published, it is nontrivial.

Steve: Oh, you're right. Good point.

Leo: It's not something some hacker has a...

Steve: You can't download it anywhere right now.

Leo: Because you need, I think you'd need a massive database of sound samples and things to compare it to. I'm sure it's just not a simple thing to do.

Steve: Yes. I mean, this was a very cool research project at a university that showed a proof of concept. Now, we know that proof of concepts do tend to mature over time. So...

Leo: Yeah, somebody could do a rainbow table sort of a thing with voice samples, I guess. But it's not - I don't think it's widespread.

Steve: It's not something you have to worry about.

Leo: And what are you really saying over the phone call anyway, c'mon. Question 6, JT in Wintergreen, Virginia - mmm, that's fresh - wonders about MSSE versus MRT: Long-time Security Now! listener, Steve, licensed SpinRite user. I switched my home office and home computers to Microsoft Security Essentials - that's the MSSE - which I keep current. And I run an automatic full scan with Security Essentials every night. It only flags malware once every couple of months or so.

Steve: Okay.

Leo: He says that so offhandedly. No big deal. Also, immediately after Patch Tuesday I run the latest MRT in full mode, thorough, that's what you want to say, thorough scan, which it doesn't do automatically. Once I do that, do I have any further use for that month's MRT? Isn't the once or twice daily update to MSSE definitions making Security Essentials more current, therefore more complete? That's a good question. Microsoft does not explain this at all.

Steve: They really don't. And in poking around, I see a huge amount of confusion about this, so I wanted to try to provide a little bit of clarification. Remember that we heard last week someone who told us that he ran the MRT, which is the Malicious Software Removal Tool, in full mode, and it found an installed rootkit which nothing else had found. That is why Microsoft created the MRT. And maybe it's the consequence of the history of the way Microsoft got into this that explains why it's unclear. So I wanted to share what Microsoft says about their MRT, the Malicious Software Removal Tool.

They said: The tool removes malicious software from an already infected computer. Antivirus products block malicious software from running on a computer. It is significantly more desirable to block malicious software from running on a computer than to remove it after infection. The MRT removes only specific prevalent malicious software. Specific prevalent malicious software is a small subset of all the malicious software that exists today. And, finally, the MRT focuses on the detection and removal of active malicious software. Active malicious software is malicious software that is currently running on the computer. The tool cannot remove malicious software that is not running. However, an antivirus product can perform this task."

So the two, MRT and MSSE, the Microsoft Security Essentials, are very different. And

MRT came about because Microsoft was having problems updating Windows with their monthly Second Tuesday of the Month patch on systems that had rootkits installed. Remember that was causing problems, causing all kinds of crashes and things because Microsoft would change some core components whose internal offset addresses changed. And when the system rebooted, the rootkit would try to reinstall itself, hooking those physical locations which in the new update had moved, and it would destabilize the system, I mean, it would crash. And so people were blaming the update for wrecking their system, and that's what was so screwy because we reported this, like a few people are having problems. Well, yeah. Those few people had rootkits that they were unaware of.

So Microsoft stepped up and said, okay, the only solution for this is for us to do a pre-update check for anything that has its hooks currently into the system. So that's the difference. The Malicious Software Removal Tool, which only looks at things in RAM actively hooked in, versus Security Essentials, which is much more like a traditional AV. Bottom line is, directly answering JT's question, is there a benefit to running MRT more than doing a full scan immediately after it has been updated, I would say, well, given that MSSE is finding malware every couple of months on his system, I would say yeah.

Leo: That's not good.

Steve: It is absolutely the case that MRT can find things that Security Essentials may not, although MRT predates Security Essentials. It came first, as we remember, Security Essentials came later. So my sense is there's probably some overlap. But believing in maybe using both a belt and suspenders, run MRT. It won't schedule itself automatically the way Security Essentials will. But you could set up, using Task Scheduler, a task probably to run it. I would bet there's some command line switches. This is something I haven't looked at because normally you have to click a few buttons to get it to do a full scan. Knowing Microsoft, you can probably use Task Scheduler to run a full scan. And it takes a while. So it's the kind of thing you'd want to automate and do at night. So I would say, yeah, probably worth doing. Not fanatically; but, you know, why not. You're running MSSE every night, so MRT and MSSE are not doing the same thing. Probably worthwhile to use both.

Leo: You can, I presume, use Microsoft Scheduler to run this automatically, I would guess.

Steve: Right.

Leo: I don't know what the command line would be to do a thorough scan, because otherwise you have to click a button.

Steve: Oh, I just did it. I typed in - I opened up a DOS box and just typed MRT /?, and it popped up a little usage with /q for quiet, /n for detect only, /f for forced full scan, and /f:y for same as above but automatically clear infected files. So you can definitely run it from the command line, meaning that you can give it a command line through Task Scheduler and have it automatically run at night, doing a full scan.

Leo: Perfect. Moving right along to Question 7, Jonathon Bly in Sioux Falls, South Dakota. He's peeved with his bank: Steve, I've been listening to Security Now! since around 2006 - that's pretty good because I think we started in 2006, maybe a little earlier, 2005 - but I've recently been working through each and every episode to bring myself up to date. I also recently purchased your excellent SpinRite software. Haven't needed it yet, but I feel very comfortable knowing that, not only can it save my bacon - mmm, bacon, oh, sorry - when one of my disks start to fail, but also provides preventative maintenance.

With the standard introductory material out of the way - just boilerplate - I would now like to comment on my bank's ability, or inability, to allow the use of secure passwords for online access. The following is a letter I sent off to the bank through its contact link:

Dear Sirs, I have been trying to change my password to something more secure than the easily guessable combination of a dictionary word followed by some numbers to a secure password from GRC.com. I was completely dismayed at your ridiculous restriction of a password a maximum of 16 characters. Quite honestly, that should probably be the minimum. Fine. I'll obey the restriction. I dutifully cut down the secure password from 64 characters to 16. I copy-pasted the new password into the appropriate fields, I hit the submit button, I got an error. Maybe you don't allow copy-pasting of passwords, so I tried typing in the password. No go.

I tried typing in a new password that I made up off the top of my head, being a slight modification of my current password. That just went fine. I tried switching to Internet Explorer (ugh) and Firefox. Neither allowed me to use the password I'd like to use. Fix this. Good day, sir. As you can tell...

Steve: I'm sure glad the bank was glad to get that note. We'll get right on that.

Leo: Good day to you, sir. As you can tell, I was little miffed with the bank. I feel like duct-taping the software engineers to a chair in front of a computer and playing every episode of Security Now! for them. Maybe you'd prop their eyeballs open, as well. Now, if I did so, I would think they'd come up with a system a little more security friendly. I understand that having a small password would be preferable to the people who have no sense of security and just want to log in quickly. I, however, live on a shoestring budget, and I need my finances to be completely secure. Anyway, love the netcast and everything you and Leo do. Just wanted to know that your guys' hard work is very appreciated. All the best, Jonathon Bly, Sioux Falls, South Dakota.

Steve: So any time you see a limit on a password length, that's a bad sign because what it implies is that they have allocated 16 characters to store your password in their database. The one good thing we heard about the hack of the Oracle MySQL database was that hashes were obtained as opposed to the password plaintext. Remember that a hash converts any amount of data into a fixed-size token. And so, if a site were hashing passwords, as everyone should in this day and age, then there would be no length on the password because they could take as long a password as you gave it, and they would hash it to the same token, which that's what they would store. And when they asked you for your password again, they would perform the same function and see if the two tokens matched, the one stored and the one they just made from what you gave them. So it's distressing that a bank is not doing so.

What this means is that, if at some point someone compromises their database, they'll get everyone's username and password and be able to log in as them. The beauty of using a hash is that, if a database is compromised, they get their usernames and the hash. But the whole point of a hash is you can't unhash it. You can't unscramble the egg. The hash is an information lossy process that loses information as it moves through the hash, but it creates something unique. And from that you cannot guess what the input was.

The only thing you can do is to use, as you mentioned earlier in the podcast, Leo, a rainbow table, is a table of known input and known hashes. So if it weren't a salted hash, which is the other thing that good security requires that you do, where you add something different to it, like you salt the hash by adding something to what the user provides so that the result is still different from what a rainbow table would provide, then you've got security. So all I can say to Jonathon is that I hope that over time we stop seeing this kind of limitation from websites where security really does matter.

Now, mitigating all of that, 16 characters, if you really choose a random chunk - I'm confused as to why he took 16 characters from what he got from the Perfect Passwords page at GRC and the bank wouldn't accept it, unless they also don't allow some special symbols.

Leo: I bet that's what it is. I'm sure that's what it is.

Steve: It might just be, like, A through Z, 0 through 9, and dash and underscore or something, which is further annoying because then it's really preventing you from creating a unique password. And then I'm wondering if it's case sensitive or not because the only thing you could really do then is play with the case, given that the password is case sensitive, come up with a non-alternating but odd changing case if you're not able to use special symbols. Do anything you can to make it something that is different from what someone would try brute-forcing. So anyway, it doesn't bode well for the security of that bank.

Leo: It's a little weird.

Steve: Yeah.

Leo: You know, this is good. If everybody wrote letters like this, maybe people would start to - look, these companies are going to respond to what their customers want. And all they're hearing is, it's too hard. It's too much typing.

Steve: Right. I lost my password. What was my password?

Leo: Yeah. So if they start hearing from people who say, you know, I want you to be more secure, maybe they will. So Question 8, as you said, two listeners with similar questions. Jason Stratman in St. Charles, Missouri, he wants to know about

Smartphones and Firesheep: Just started listening to Security Now! when Firesheep first sprang up, and I heard you talk about it again last week. I started wondering, if I'm using Facebook or let's say Twitter, the apps on my Smartphone on an open access point at a local bar, can Firesheep still acquire my login information? Do Smartphone apps use cookies like web browsers? It's funny because I had this same question that day, the Firesheep day, and I immediately tested it.

Jim Guistwite in New Jersey has some thoughts and concerns raised by Firesheep and mobile apps: I tried Firesheep a few months ago when you first mentioned it. I was startled, as many other listeners were. Many websites are switching to secure communications for browser-based HTML traffic, but are their APIs used by mobile applications also using HTTPS? Couldn't there be a similar session cookie issue as with the browser clients on the desktop? Makes me wonder how safe it is to use mobile applications on an open WiFi connection. Perhaps other listeners are similarly concerned - yes - and you should address this on an upcoming show. Thanks for the podcast.

P.S.: My 11-year-old son calls Steve "the bot guy." His iPod died on a car trip, maybe about a year ago, and he was forced to listen to what I was listening to. His first introduction to Security Now! was during a discussion of botnets. So, Steve, you're "the bot guy."

Steve: Okay. So here's what we know. We know that cell phone radio is encrypted. It may not be the best encryption in the world, but it is encrypted. So if your Smartphone is using its cellular connection, then you're relatively safe. You're at least safe, but in the local air between you and the cell tower or the terminus where it then goes over the Internet, at which point the cellular encryption is removed, and then the actual data in the connection would be moving over the Internet. If you're using a - and this must be what both of these guys, Jason and Jim, are talking about. You've got a Smartphone which also has WiFi capability and preferentially uses WiFi when it's available, much like, for an example, an iPhone or an iPad does. If it has WiFi, it would prefer to use that than cellular.

Then this is a great question. The question is, are these apps encrypting themselves for, not browser-based apps, but Smartphone apps that are bringing their own little world with them. And I don't know. The way to find out, if you are curious, and our listeners could, those who are curious and savvy, would be to use the app with your Smartphone and your WiFi at home...

Leo: I did.

Steve: ...while looking at the traffic.

Leo: And it was fine.

Steve: Neat. So all you see is just gibberish.

Leo: Yeah. They don't - they're not using the same techniques browsers use. They're using the...

Steve: Makes sense.

Leo: And if you think about it, they're using the API. They're not using browser cookies or that kind of thing, tokens.

Steve: Right. Or they might just be setting up, they might use an SSL connection, like within the app, just to have security from end to end, or some kind of encryption. So, or as you say, Leo, it might just be a completely dense binary protocol, which is their own API.

Leo: Yeah. Both Facebook and Twitter have an API for this kind of thing, and that's what they use.

Steve: Right.

Leo: So I think there's nothing to fear. I certainly played with it and wasn't able to get any Firesheep love. That was the first thing I did when I installed Firesheep. I said, let me see. What else?

Matt Vanderville, Woodstock, Illinois, wonders whether, after uninstalling Internet Explorer 9, his Windows 7 is less secure. Hmm. Love the show. Get to the point, I've previously chosen to remove IE8 through the Add/Remove Windows Component section. After investigating and trying out IE9, I chose to uninstall it, as well. Is my OS now less secure? In other words, will I be left with the old IE8 components that integrate with the OS, or am I left with the newer IE9 components? Oh, I get his question. That's a good question.

Steve: It is a great question. And I have no idea.

Leo: Microsoft doesn't say.

Steve: It was a great question. So, Matt, here's the problem. You really can't uninstall Internet Explorer. You can remove the icons for launching it, and you can remove the EXE. But it is the case that modules of IE are part of Windows. Now, when you install IE9, those are being updated. And that's probably a good thing. So I would imagine, when you uninstall it, it probably puts back the things that it removed. And so you're probably back to IE8.

Leo: But he uninstalled IE8. So what does he really have?

Steve: Exactly. And that's my point is you can't really uninstall IE8. You can remove the UI of Internet Explorer, but you're still, for example, going to have the browser, the browser helper, the browser DLL, the HTML rendering. For example, Outlook uses IE's browser renderer to display your email and for its preview window. And we know that when you - just previewing email can cause your machine, your toy Windows operating system, to be taken over.

So IE is still there. If you're using Windows, you've got Internet Explorer. It is deeply integrated into your Windows system. I don't know whether having IE9 and then removing it put back what was there before. I would guess it does, in which case you probably have IE8. That is, whatever IE came with Windows 7, which would be Internet Explorer 8. So, and also I'm surprised that you just uninstalled IE8. I mean, I don't use Internet Explorer any longer, except, for example, using Windows Update. I like to go to use Windows Update or Microsoft Update to sort of more carefully pick and choose what's going on with my updating of my software. And you can't do that with Firefox. It only runs in Internet Explorer. And also there are times when I'm downloading things from Microsoft that it wants to run me through all kinds of weird validation hoops if I use Firefox. I go, oh, that's right, I've got to do this from Internet Explorer.

So for me it's handy to have it around. I just don't use it every day. And I've never been an Outlook user, so I'm not risking being bitten there. So anyway, my sense is don't use Internet Explorer daily. Use anything else - Firefox, Chrome, Opera. But also know that Internet Explorer is still lurking in Windows. You just really can't get away from it. It's part of the OS.

Leo: So the only real question is, what does Microsoft do when you uninstall components? I mean, at some point IE9 will become the default, and it will be using IE9 components whether you install it or uninstall it.

Steve: Yeah. And so, for example, I'd rather have IE9 installed and not use it than have removed IE9 and maybe be falling back to IE8 because then you're getting the benefit of the security updates in the components you can't get rid of anyway.

Leo: So that's the real answer, is just install IE9 and keep it. Just don't use it. You don't have to use it.

Steve: Right.

Leo: And you're not really getting rid of it. So it's kind of a false sense of security anyway.

Steve: Exactly.

Leo: Question 10 from Jerod Lycett in Duncannon, Pennsylvania. Actually, I should be more specific: Duncannon, Pennsylvania, U.S., North America, Earth, Sol, Milky Way. He wanted to really narrow it down.

Steve: Yeah, he didn't name a universe. I think someone else said universe number, you know, 39274, yeah.

Leo: We don't know what universe we're in. That's the problem. We do know we're in the Milky Way, though. He has the Chrome Security Tip of the Week. First of all, I want to give a small tip of not saying bad things about Java, as one of your sponsors, Citrix, uses Java. Hey, wait a minute. We don't say bad - first of all, if there's a security issue, we say it. What Steve says is, if you don't have a need for Java, don't install it because there's no reason to install something that you don't use, given that it might have potential security issues.

Steve: Precisely.

Leo: That's just good policy. You don't install a bunch of crap you don't use. Nobody should do that. However, you're right, Citrix does use Java. And I think, as I have looked, there has never been a security issue with Citrix.

Steve: And by bringing it along, they'll be keeping it current, also, instead of it just...

Leo: That's right. Yes, it actually does that, yeah. It's interesting, it installs fresh each time and makes sure you have the latest Java. That's probably why they do that. Here's a quick Chrome security tip: In about:flags - so you're in Chrome. You type in the URL bar about:flags. I'm doing it right now, just to see...

Steve: Which is just a cornucopia of things you should, like, think about before you click on them. All kinds of goodies.

Leo: There's a lot of flags. Boy, there's a ton of flags. So he says, in about:flags, one of the most important flags there is Click to Play. This adds a third option to the menu Content Settings, which you click the Wrench, then Options > Under the Hood > Content Settings > Plug-ins, and that menu item is Click to Play. Now, that means, when you go to a website, you can choose not only whether or not to use the plug-ins at all, but also which ones specifically you want to allow. So you can only play the YouTube clip, but not the ads or other possibly malicious content. Also, you need to expand the Location box, as I couldn't fit Alpha Quadrant into it. I guess Alpha Quadrant's a game.

Steve: So this is a great tip, and I did it because he's right. Your normal options under managing your plug-in content is an all-or-nothing. And if you go to about:flags, and then enable that Click to Play, and then restart the browser, when you go back into the Options > Under the Hood > Content Settings > Plug-ins, sure enough, what used to only have two options, now has three. And the one in the middle, I think it is, is Click to Play. So you'll bring up a page whose plug-ins are disabled, and then you can selectively click on them in order to allow that plug-in to run, which is a very nice little upgrade to Chrome.

Leo: I'm doing it right now. Tools and then - Tools...

Steve: And options.

Leo: Options, hmm.

Steve: Under the Hood is like the last thing down on the left.

Leo: I don't see it. I must have some strange setup.

Steve: Uh-oh. I'm in Windows, and we know that there are differences.

Leo: Oh, it's not in the Mac. Okay.

Steve: Okay. We know that there are differences between Windows...

Leo: Oh, rats. I can set the flag, but apparently I can't get to the menu item.

Steve: Yeah, the other thing I liked is that remember that Windows had the tabs on the side option, and I don't think that the Mac version does. Which is really weird. Why are there two different versions of Chrome?

Leo: Yeah, I mean, I'm sure the engine is the same, the WebKit engine is the same. It must be a - huh, interesting. Well, it's okay [sobbing]. I didn't need that. Let's see here. Going on...

Steve: Stay where you are, Leo. You're safer over there on the Mac anyway. I'm holding on for dear life over here on this toy operating...

Leo: There are plug-ins, and there were plug-ins for Firefox that would do that Click to Play thing for Flash and stuff like that. And that was - that is a very handy feature.

Steve: Well, and NoScript does.

Leo: Oh, right, of course. Are you ready for Bonus Question - wait a minute. Yeah, that was 10. So here's a couple of bonus questions, first from Matt Peterson. We were talking a couple weeks ago about your old InfoWorld column, the Tech Talk column. Although they are mostly of historical or nostalgic interest now, writes Matt, I thought that the other Security Now! listeners might be interested to know that all or most of the back issues of InfoWorld containing your column are archived on Google Books. I didn't know that. So all of your insights, from "Borland's Turbo Basic Language Encourages Fast, Easy, and Casual Use" column, December 1986, to "The Only Drawback to the SCSI Interface Is Its Pronunciation" from January 1989, all the up to your farewell column in 1993, are there to peruse. Ready for the short URL, kids: snipurl.com/sgtechtalk. Oh, dude. This is great. Look at this. Did you know that, Steve?

Steve: Yeah, yeah.

Leo: You knew it. You already knew that.

Steve: Yeah, all the columns are there.

Leo: Oh, that is really a wonderful thing to have. I think that's fantastic. So thank you for that tip. It's worth a trip, he says, down memory lane if you were a computer nut back in those days, as I was, or if you just want to see what Steve's mustache looked like back then.

Steve: It was a lot darker.

Leo: And Bonus Question 2, just had to mention this. Kevin in Ocala, Florida found Khan Academy. Steve and Leo, though you might want to check out this website: KhanAcademy.org. Many students use this to get help in math. It's a terrific training site and free of charge. I love the podcast and listen to many, but yours is my favorite. I'm going to have to point Henry.

Steve: Okay. Now, Leo, go to this page: KhanAcademy.org. And then scroll. Look at the scroll thumb, how small it got, and just look at the topics.

Leo: Holy moly.

Steve: It's just, it's unbelievable.

Leo: This is, okay, so Algebra I, Algebra, Algebra II, which Henry is in, Arithmetic, Banking and Money, Biology, Brain Teasers, Calculus, and these are all worked examples from various textbooks. So you can really learn. California Standards Test Algebra II, I can sit down with Henry and play with that. Chemistry, oh, he's in Chemistry right now, too. First year high school or college course, roughly. Cosmology, astronomy, credit crisis - I'm just in the C's. Developmental math, differential equations, finance. This is amazing.

Steve: It's just an incredible site.

Leo: So who are these Khan Academy peoples?

Steve: I have no idea. But it looks big and legitimate, and it's free, and just an incredible amount of content. So I wanted to point our listeners to it. I'm sure some people will find it very useful.

Leo: This is "A free world-class education for anyone anywhere. The Khan Academy is an organization on a mission ... a not-for-profit with the goal of changing education for the better by providing a free world-class education to anyone anywhere." Wow. Free of charge completely, in every area. This is so cool. It's just one guy? They're telling me it's a person, it's an individual who does this. 2100 videos, exercises, a knowledge map. I'm going to school. I'm going to school.

Steve: Yeah, I had a hard time pulling myself away from it. It's like, okay, wait, I've got to get this podcast produced here.

Leo: You know what I really love?

Steve: What?

Leo: Creative commons licensed. I think, whoever you are, Mr. Khan, I salute you. That's awesome. Hey, great tip. What a good way to end. I'm glad you...

Steve: Had a bonus.

Leo: ...threw that one in because that is fascinating. Wow. I never heard of this.

Steve: Hey, and we've got to thank Kevin in Ocala.

Leo: Thank you, Kevin.

Steve: Thank you, our listener. Our listeners bring it to us.

Leo: Thank you all for being here. We do this show every Wednesday about 11:00 a.m. Pacific, 2:00 p.m. Eastern time at live.twit.tv. You can tune in and watch, or just download the show. It's available at all sorts of places, of course on iTunes, the Zune Marketplace, anywhere podcasts are. Or you go to our website, TWiT.tv, that's where all the shows are. And each show has its own page. Usually it's an abbreviation of the initials, in this case TWiT.tv/sn for Security Now! And let's not forget - and by the way, there's a TED talk. This Khan guy, Salman Khan has a TED talk. So if you want to know more about this guy who does Khan Academy, that's awesome. I'm going to watch that TED talk. He says, "Let's use video to reinvent education." Yeah.

Steve: Makes so much sense.

Leo: Brilliant. Wow. I'm so glad there are people like this in the world. Steve has copies of the shows. I'm glad there are people like Steve in the world who also gives away a lot of free education. If you go to GRC.com, you'll find all of the audio of all 294 episodes, including 16KB versions for the bandwidth impaired or people with bandwidth caps. You'll also find the smallest version, which is a text transcription of it, which makes it really easy. All the show notes, too. That's GRC.com. That's where you'll find SpinRite - Steve's bread and butter, his program to maintain hard drives - and all his freebies that he gives away, including the Perfect Paper Passwords and more. GRC.com. Steve's on Twitter, too, let's not forget. He is @SGgrc.

Steve: And I think I'm either approaching or right around 18,000 followers. So I've been tweeting a lot about Fukushima and various things that happen. So I'm trying to create a useful stream for people who follow me. And so, thank you, thank you for...

Leo: Thank you for doing that. I really appreciate it. And, Steve, we'll see you next week.

Steve: We're going to talk about the Comodo theft of the SSL certificates, how it apparently happened, what people have, about certificate revocation, how that system works, which is something we've never covered before, and have lots of information about that.

Leo: Should be great.

Steve: Thanks, Leo.

Leo: Thank you, Steve. Thank you all for joining us on Security Now!.