SECURITY NOW!

Transcript of Episode #271

Listener Feedback #103

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-271.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-271-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 271, recorded October 19, 2010: Your questions, Steve's answers, #103.

It's time for Security Now!, the show that covers your security, your privacy online, protecting you from the bad guys that inhabit the Internet. Here he is, the star, our security guru, Mr. Steve Gibson of GRC.com. Good morning, Steve.

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

Leo: Good to see you. We've got a Q&A episode today, I think.

Steve: We do, #103. And no updates, but lots of news. And some great questions, lots of follow-up, actually, from things that have been on our listeners' minds sort of communally in the last couple weeks. So we'll address those and have a nice conversation.

Leo: You can always ask a question of Steve. People want to know sometimes, why don't you take questions from the chatroom and stuff? And some of our other shows do. But I'll tell you, I'll speak for Steve because I know why - because Steve likes to prepare his answer. He likes to make sure he's got it right. He's an engineer, and he doesn't like to do what I do, and what some of our other hosts do, which is answer off the cuff.

Steve: Well...

Leo: But you were doing it before the show today, which I was surprised.

Steve: Well, I mean, I can. But there are questions, like we have several today, where I had to go do some research for it. And so in order to provide a useful, detailed answer - which I love to do because, I mean, I'm learning, too, or I'm finding out things. I learned about what Logitech is doing in detail for the encryption of their keyboards, which I just wouldn't be able to answer on the fly; but I'm going to explain exactly how it works because now I know everything about it. So...

Leo: Right. Well, I think this, of all the shows we do, it's the most technical show. And so, rightly so, you want to give technically complete and accurate answers. And sometimes that does take a little prep.

Steve: Well, yeah. And, look, someone could have said, well, what about LastPass? And in fact I put off a LastPass episode until I could lay out a huge amount of time. I have invested more in learning LastPass than I've done for a long time for the podcast. But I was able, as a consequence, to really deliver a thorough review of exactly how it works, what the scripts do, blah blah blah. I mean, so there's a ton of time I'm spending behind the scenes that, as you say, I hope it shows in the content.

Leo: Absolutely. Very valuable. So you said there's lots of news.

Steve: Lots of news. After a couple weeks of rock 'em sock 'em updates, the industry seems to have gotten that out of its system for now. So nothing happened over on the update side. Nothing at all of any particular note.

However, Microsoft, the senior program manager, Holly Stewart, made a posting on Microsoft's security blog saying - I think the title was, "Have you checked the Java?" What they found in looking at the numbers - and we'll be talking about their numbers here a little bit later in news because their big half-yearly security intelligence report is now out for the first six months of 2010. In looking at the numbers, they discovered a somewhat surprising leap in the amount of exploits and attacks against Java.

Now, not JavaScript, which of course is my favorite whipping-boy on this podcast, forever. But the Sun/now-Oracle Java, which is a very nice late-model advanced language, which has a runtime engine which needs to be installed in a machine in order for it to operate - it doesn't produce native code, like not Intel instructions, but rather the Java language compiles to its own byte code, which is then interpreted by this interpreter. And of course, as with anything really complicated, and convoluted to some degree, there are problems which surface over time with the details of the code. Paraphrasing a little bit from SANS Security Newsletter about this, SANS wrote:

"Many of these vulnerabilities are created by flaws in the low-level implementation of the Java Runtime Environment [the so-called JRE]. Although Java is intended to be type safe" - meaning that it's intended to sort of protect you from these sorts of things, I mean, and some care was given to that - "low-level code sometimes writes user-defined strings [into] buffers, giving an attacker the opportunity to overwrite return addresses and execute [their own] code. Vulnerabilities like these allow Java applets, which start without user interaction when a target navigates to a malicious site, to execute ... the permissions of the Java process running them. Normally applets run with restricted privileges."

So the point is that this is - it's a variation on the same problem we have with JavaScripting, but the details are different. You go to a site which is using Java as opposed to JavaScript. It is still giving you an applet, a so-called Java applet, which then runs under the supervision of this runtime environment. The concept is that that encapsulation, created by the runtime environment, would give you protection. And it certainly gives you a lot of protection, but there's little mistakes in it.

Well, our friend Brian Krebs, who did the security column for the Washington Post for so long, has been following this. And he noted recently that Java exploits, exactly what Microsoft's blog posting is talking about, now exceed Adobe-related exploits...

Leo: Wow.

Steve: ...as an attacker's preferred method of breaking into PCs. And Microsoft said that they had gone from hundreds of thousands per quarter, that is, in terms of exploits against vulnerabilities, to millions. And we're talking, when you look at the exact numbers, more than six million. So a real ramp-up.

Leo: That's not individual exploits. That's attacked PCs.

Steve: Correct. Absolutely, yeah.

Leo: Six million exploits would scare the hell out of me.

Steve: Yeah, well, we'd just unplug our machines at that point.

Leo: Yeah, no kidding.

Steve: They'd be Swiss cheese. And Brian believes, Brian Krebs believes he understands what the difference is. What's happened is that Java has gotten onto the radar of those who make the exploit kits. And so Java exploits have been moved into the exploit packs, which makes them, like, turnkey easy for malware authors to use.

Leo: But here's the thing that baffles me. Java was always pitched as secure because it has sandboxing. And we had malicious applets, but they never could do very much. Are these real exploits?

Steve: Yes.

Leo: Like root exploits?

Steve: Yes, yes. And that's the point is that it was pitched as secure. As I said, this runtime environment provides some containment. But if there's mistakes, then you lose containment. And as we know, mistakes happen. So there are some ways that it is possible for a user-provided string to be loaded into an unmanaged buffer, which can cause a buffer overrun. And we know that once that happens, all bets are off. So the problem is, there are mistakes. Now, remember...

Leo: Mistakes in the JVM.

Steve: Yes, yes.

Leo: Okay.

Steve: Yes. There are mistakes in the containment. And last week Oracle, what was it, 29 security fixes in Java when they went to version 6, update number 21 or, no, 22 I think we're at now. So here's the bottom line is you can look at, in your Add/Remove Programs, for Windows at least, Java will be there if it's installed. It will tell you what version it is. You want to make sure you're at update 22. The question is, do you need it? I don't have it installed on my main workstation here that I'm sitting in front of, that I use day and night for everything.

Leo: Yeah. There are very few things nowadays that use Java. Used to be much more omnipresent.

Steve: Yes. And so the danger is that it's sort of sitting there, really not being necessary, yet still representing an attack vector for people's machines. If you don't know that you need it, I would just say remove it. You can use Add/Remove Programs in Windows and just click on Remove, and it's gone. And this ramping-up exploit vector is just eliminated from your system.

Now, in fairness, the attacks that are being made currently, that is, the known vulnerabilities that are being exploited, have all been patched. So patching - well, as of last week. So Oracle is trying to stay current and keep these things patched. The bad guys are leveraging unpatched versions of Java to get into people's systems for drive-by exploits. And we'll be talking about drive-bys here in a few minutes, extensively. So it is the case that, if you know you need it, you can increase its rate of checking for updates. By default, it only looks for updates once a month, on the 14th of the month. You can change that to weekly or daily, if you like. So there is a Java Updater which is configurable. And Brian Krebs suggests, if you do need it, then there's really no - there's very little overhead with it checking more often. And I would say that makes sense. Just have it check more often.

Leo: So, okay, good. So it does auto update.

Steve: Yes.

Leo: And it's part of Windows Update.

Steve: Well, and Brian's also - oh, no. Java is independent from Windows.

Leo: There isn't a Java Update in Windows Update?

Steve: No. Microsoft sort of washed their hands of that. And there was a big battle, remember, back in the early days, when Microsoft had their own?

Leo: Oh, that's right, that's right, that's right.

Steve: And Sun said, no, no, no. We're unhappy with you.

Leo: So you have to make sure the Java Updater itself does the job.

Steve: Yes. And Brian noted something that I had, too, which unfortunately we always note with a lot of these updaters. Sometimes it just sort of doesn't. There is a new one around, and for whatever reason it just didn't get the message somehow. So if you want to make sure, you can look in Add/Remove Programs, make sure you're at 22 - version 6, update 22. If not, then manually update. You can go to Oracle's Sun site and update to update 22, which you definitely want to do, especially with this thing becoming as prevalent as it has.

Now, I was just talking about mistakes in containment. Adobe Reader, the next version, apparently Reader 10 - I'm seeing it referred to as Reader X. I won't call it "Reader X," as I was calling it "OS X" in the case of...

Leo: I wish they'd just call it 10.

Steve: Yeah.

Leo: C'mon, we're not Romans, for crying out loud.

Steve: Well, because it's 9 right now. It's not VIII. So...

Leo: It's just fancy stupidity.

Steve: Or I guess it would be IX, wouldn't it, yeah.

Leo: It's just ambiguity. That's annoying.

Steve: Yeah. So the big news - drum roll, please. It's that Adobe's management have said that next month, coming in November, Reader will get sandboxing.

Leo: Yay.

Steve: And it'll be on by default. And they're saying, well, I mean, thank goodness. And they're saying initially only write calls will be sandboxed. Reads will come later. Now, I say, well, this is all good because more is better. But mark my words, here we are, middle of October. It won't matter.

Leo: Right. Why not? Why isn't that enough?

Steve: Well, it's better because it means that Adobe is focusing a lot of attention and resources on this. If they're talking about it happening next month, it's something they've been working on for quite a while because it's not an easy thing to do, to go in and retrofit containment where there hasn't been containment. The problem is, it won't be perfect. They'll make mistakes. Just as the Java Runtime Engine was designed from the beginning to be a contained environment, and it isn't. It's got mistakes in it, flaws in its containment, which are now being exploited like crazy.

So Adobe's got problems with the quality of their code. The policy that they're implementing of sandboxing is a good thing. It represents progress. It doesn't mean this is going to get solved. So with any luck we'll be talking about Adobe less often. Maybe the exploits will be less bad. But...

Leo: Less bad.

Steve: We couldn't be talking about them any more often than we are.

Leo: Adobe Acrobat - less insecure.

Steve: Less horrible than it used to be. Yeah, yeah. Well, and speaking of the first half of 2010, Microsoft's Security Intelligence Report is out with a bunch of interesting numbers which are always sort of fun to actually see because we always use superlatives here. It's nice to have some actual numbers.

Leo: The most secure in the history of this week.

Steve: Yeah, exactly. So Microsoft, with the combination of Microsoft Software Removal Tool, MSRT, and the Microsoft Security Essentials, MSE, which I'm now using on my various Windows machines...

Leo: Oh, interesting. Ah.

Steve: ...very happily. Yeah, I mean, it's my antimalware. I never was a third-party malware user.

Leo: You've never, yeah, we've never used antiviruses; right? I mean, it wasn't merely third party. You just didn't use them.

Steve: Didn't use them at all. But now that it's sort of there with Windows, and Microsoft's going to do it, it's like, okay, fine. I'm happy to have it. And it's what I'm recommending to other people, so I figure I should be using what I'm recommending, much as I'm using LastPass, for example. So between those two tools, Microsoft has data from 450 million PCs that are running those things worldwide.

Leo: Wow.

Steve: During the first half of 2010, nearly 1.9 million PCs were infected, some multiple times. In fact, many multiple times. Of all of the machines out there, the U.S. is number one in infections.

Leo: Really. Huh.

Steve: Their tools did 2.16 million bot cleanings, which is 5.2 per thousand runs of the MSRT. So the Microsoft Software Removal Tool, which we've talked about, in fact last week I was even saying to people, just go to the Start Menu and just run it. Type "MRT," no "S,", "MRT." That pops it up, and you can just sort of do a manual deep scan of your system. Microsoft runs it monthly after it updates itself with each month of security updates. For every thousand runs of that MSRT, they find and remove 5.2. I don't know how you can have 0.2. I guess it's like...

Leo: Well, there's a million runs, and so they got 52,000 or whatever.

Steve: ...0.3 kids or something. Yeah, 5.2 bot cleanings in the U.S.

Leo: That's not such a high rate. That's less than 1 percent.

Steve: Yeah, exactly. Yeah, it's, what, 0.52 percent. So 0.52 percent.

Leo: That's fairly low. One half of one percent, that's not so bad.

Steve: But Leo, I mean, you know, bots are not good.

Leo: Now, and by the way, this is just its kind of quick scan that it does. There is a more thorough scan that it doesn't do automatically.

Steve: Correct. So, yes, it's doing the quickie one, and it's during those quickie ones that it's finding these. Although our listeners, who are doing it deeply, they probably get some credit for doing that, too, although they're hopefully not finding bots on their machine.

So Brazil, whereas the U.S. machines experienced 2.16 million bot cleanings in the first half of 2010, Brazil is in the second place with 511,000. And also, interestingly, the same number of cleanings per thousand MSRTs, also exactly 5.2 cleanings of bots per thousand runs of the MSRT. Korea is in number four place, and it's distinctive because it's got substantially more bots per thousand runs. It's the highest of any region, 14.6 cleanings per thousand runs of the MSRT. And so Microsoft reports that, overall, the infection rate of machines they're seeing is 1.4 percent. So that is a high number. I mean, 1.4 percent, that's a lot of machines. 14 machines out of every thousand have stuff on them.

Now, looking at demographics a bit, in terms of drive-by-download pages - drive-by downloads of course mean that you visit a website, and it infects you. It does something to you, running JavaScript, typically, through whatever vector is available, JavaScript or Java, something executable, maybe an ActiveX control that gets downloaded. It could be anything. So what they're seeing is that in general on the 'Net, three out of every 10,000 pages is a drive-by download. So three out of every 10,000 pages.

Leo: Oh, that's a lot.

Steve: That's a lot when you consider all the good pages out there, yeah. Three out of every 10,000. And they're saying that out of every thousand search results pages that a search engine pulls up, two of those thousand search result pages will contain links to sites with drive-by downloads. So two out of every thousand searches results in a page containing malicious sites.

Leo: So it's worse if you're searching? I don't understand.

Steve: Oh, they're saying that three out of every 10,000 web pages...

Leo: In general.

Steve: ...in general will infect you. But in terms of search results, which is different...

Leo: Why would that turn up more bad things?

Steve: Which?

Leo: Search results. Why would searching...

Steve: Well, because they've got so many links on one page.

Leo: Oh, yeah, yeah, yeah, okay.

Steve: Yeah. So the thing that...

Leo: Okay.

Steve: Yeah, yeah.

Leo: I thought, is there some magic thing happening? Well, maybe they're targeting certain common searches. It actually may be, I mean, how many links are there? 15? They may be actually targeting common searches, which would raise the...

Steve: And that would make sense...

Leo: ...the hit rate, yeah.

Steve: ...that they would try to do that. Because of course that's the way people go to web pages now is they do a search, and they click on links. So not surprisingly, in terms of top-level domains, the .cn domain, the China domain, has the most infected sites by domain name. And get this, Leo - 5.8 percent.

Leo: One in 20. One in more - wow.

Steve: Yes.

Leo: Now, how do you get a .cn? Do you have to go through the Chinese registrar? You do.

Steve: Exactly. So their top...

Leo: So these are Chinese sites. These are not bad guys in Poland pretending to be Chinese.

Steve: Well, all we know is that their URLs end in .cn. So they are the Chinese registrar.

Leo: It's like, to get a .ca you have to verify that you're doing business in Canada or a Canadian. I would bet you the Chinese registrar is at least as restrictive as the Canadian registrar.

Steve: I would imagine that's the case.

Leo: And then so now you have to wonder, well, how many of these are rogue sites, and how many of them are government sites?

Steve: Well, and remember, we have talked in the past that China's not happy about the state of affairs, and that they've begun to make some noise about checking people's credentials more. It had traditionally been incredibly easy to just register whatever you wanted to .cn. And now they're saying, we want to see you. We want to see who you are and check your identity.

Leo: It's also conceivable that more Chinese machines are hacked because, if you hack into a web - it's very frequent, at least it has been in my experience, that sites that have malware on them aren't always - the owner isn't always the guy putting the malware on there. They've found a security hole in the server, and then they put malware on all the sites. And it may be that's what's going on.

Steve: Well, and we know that, for example, Network Solutions has had huge problems with that recently, where there was a mistake, and because Network Solutions has a big web hosting service, a huge number of their sites were being infected with malware through some exploits that people used. So all of those would count as infected domains. So, yes. So 5.8 percent...

Leo: That's appalling. That's terrible.

Steve: ...of .cn domains have drive-by-download pages. Second and third place are tied: .ru, Russia; and .de, Germany.

Leo: Hmm, now that's a surprise.

Steve: Are both tied. Yeah, you wouldn't expect Germany to be up there so high. And they're both tied at 2.8 percent of their domains. But still, that's a big number, yeah. And interestingly, the U.K., the .uk top-level domain is in fourth place at 1.7 percent.

So, overall, when you stand back and look at the trends from '08, so where things were two years ago, the number of security breaches, that is, breaches reported by companies of people getting into their networks and stealing credit card information, stealing database data and so forth, that's - the good news is, that's been on a continual downward trend. And it's about half, frankly, of where it was two years ago. So there's really been progress made. We've got laws now that require this to be reported. So you'd almost expect to see some inflation of those numbers rather than deflation because we're being much more strict about requiring companies to acknowledge when information gets away from them.

But the good news is, I think it's probably because it has been - they have to report it, and the news agencies are covering breaches, that we are seeing that decrease. So people are tightening up their networks; they're being better about educating their users; they're training their own IT security people more thoroughly. So overall, for the last couple years, a downward trend. And so we're seeing about half the breaches that we were before.

And also vulnerability counts have been falling, since actually now in this case Microsoft's tracking back since the second half of '06, so over the last four years, in general we're seeing the counts coming down in terms of number of vulnerabilities per half-year, which is how Microsoft aggregates these, that is generally coming down over time. Not dramatically, but trending that way.

And the top threats - won't be a surprise to anybody listening to this podcast - are trojans and worms. The top of the trojans and worm threats are, interestingly, gaming password stealers. There's two in particular, a Win32/Taterf trojan and a Win32/Frethog, F-r-e-t-h-o-g, I guess it's Frethog. Those two are at the top. Those are the two most commonly detected malware families. And they focus on stealing gaming passwords and sending online gaming passwords back to their trojan and worm masters.

And the number one way that malware gets money from people, and this also we've talked about many times, is so-called "scareware." It's the stuff that pops up on your machine. Typically you visit some website with scripting enabled. It takes advantage of a scripting opportunity, or just using scripting on that site to pop up windows, which often is done with the script's permission, even with the browser's permission, to pop up a notice that says, oh, we've just detected malware on your machine. Go here, click this in order to get taken to a site, and we'll tell you how you can clean things up.

Doing that, of course, typically actually is the event that installs something bad on your machine. Up until that point, all you had was a scary notice. Then ransomware takes over and requires that you give them some money in order to do something. So anyway, that kind of scareware is the most common method that bad guys get money out of victims, is basically people say, I mean, they believe all that, and they enter their credit card information. And, you know, god help them.

Leo: It's a protection racket. Without any protection.

Steve: Exactly. And lastly, I mentioned a week or two ago that I had seen the blurb go by, but I hadn't been able to backtrack it afterwards, about the ongoing drama of the laptops-spying-on-students story. Remember I said that I was sure I'd seen that someone had decided that there was no criminal intent. And so the news is finally all in. What happened was that a settlement was reached over on the civil side because there's the federal suit and the federal felony stuff, and civil complaint side.

So what happened was the federal authorities announced that they would not prosecute the administrators, and we're talking about the Lower Merion County Pennsylvania School District, which was caught sending out laptops with webcam spyware installed, ostensibly to allow the laptops to be recaptured or reclaimed if the students lost them. But what was found was that people within that school district were turning on the webcams of non-stolen, non-misplaced, not-lost laptops, and basically spying on the kids.

So lawsuits were filed by the parents of the kids that had been spied on. So the federal authorities, there's a Zane David Memeger, who's the United States Attorney for the Eastern District of Pennsylvania, said that they found no criminal intent in the alleged surveillance. So that moved, essentially, the feds off the table; but that still left the civil suit and the need for a civil settlement. Now, get this, Leo. The school district has agreed to pay a total of $610,000 to make this go away, to settle the civil side. Of the $610,000, the attorneys get $425,000 of that.

Leo: Geez. Well, that's normal, though.

Steve: I guess so. And the students get the remaining $185,000. So this would have been the plaintiff attorneys who were bringing the suit. I'm sure the parents went to some attorneys and said, hey, we really don't have any money to pay you whatever it's going to cost to go sue the district, so how do you want to arrange this? And the attorneys said, well, it looks like you're got a case. We'll take it on contingency, and take a percentage, a heavy percentage, looks like two thirds, of whatever it is we're able to get for you. And the parents at that point said fine, we accept that. And to defend itself from the plaintiffs, the school district's insurer, a company called Graphic Arts, has agreed to pay the defense attorneys $1.2 million.

Leo: I'm confused. I thought they - oh, the - who got the money then? I thought attorneys got money.

Steve: Oh, yeah. All the attorneys made out pretty well on this.

Leo: Yeah.

Steve: So the school district is insured against this. So they've got some sort of, I don't know...

Leo: No, that's normal, an umbrella insurance. I have insurance, if you sued me. I shouldn't have said that. But no, that's normal. You'd have...

Steve: We love you. No one's going to sue you.

Leo: You can have liability or, you know, you'd have definitive insurance. And any business would.

Steve: Exactly. So, I mean, I'm in a condo association. Our association has insurance because some homeowners went off the deep end a few years ago.

Leo: Right, it's normal.

Steve: And were pissed off.

Leo: You've got to have an umbrella liability policy. I'm sure even a school district would.

Steve: Yes, they do. And I would imagine their rates have gone up recently.

Leo: Oh, yeah.

Steve: So their insurer agreed to pay $1.2 million for the school's defense costs.

Leo: Oh, I get it. The defense cost more than the $425,000 they got from the settlement.

Steve: Yes, the whole extent...

Leo: It cost 1.625 million. Geez, Louise.

Steve: Yeah.

Leo: You know, though - okay, fine. This is nothing new. We've seen this before. It still bugs me a little bit that the court found there was no intent. Because, I mean, we didn't see the evidence. But the anecdotal evidence I heard sure sounded like there was intent. Some of the quotes from the IT people...

Steve: It sounds wrong. Yes. There were 400 photos taken of the one student...

Leo: That one boy, yeah.

Steve: Yeah, the one boy who was confronted by the school officials saying that he was popping pills, and it turned out it was Ike and Zike or...

Leo: Ike and Mike's, yeah, it was candy.

Steve: Ike and Mike.

Leo: And the thing is, the camera was supposed to be if the laptop was reported stolen. So it seems to me there's intent. If they're taking pictures of students, and they haul the student in, I think that's criminal intent. I'm sorry.

Steve: And not just one. Multiple students, also.

Leo: And then there was - now, and again, maybe this wasn't entered into evidence. But there was a transcript of comments on the web. One of the IT people said it's really fun watching the kids. So I'm - not criminal? I guess it's not criminal. It's offensive.

Steve: Yeah. Well, the good news is there's been enough money rolling around in this, and enough headlines and press, that - I mean, what we would want is this never to happen again, anywhere. And you have to imagine that any schools that are using, I mean, this was commercial software. So you can imagine that the Lower Merion County Peninsula School District...

Leo: They're not the only ones.

Steve: ...are not the only ones.

Leo: Oh, no.

Steve: Yes, not the only ones. So the good news is, I would imagine this will not happen again. There's no excuse to happen again.

Leo: So just to make it clear, there was a civil lawsuit. That's where the settlement was. The feds declined to criminally prosecute because they couldn't find that evidence of criminal intent.

Steve: Correct.

Leo: Or, you know, it's very hard to prosecute government agencies. It's certainly hard to sue them. They may have decided that, even though there was some evidence, there wasn't sufficient evidence, something like that. That happens all the time.

Steve: Yeah.

Leo: Anyway, yeah, you're right.

Steve: Or maybe the evidence was tainted, I mean, who knows what was going on?

Leo: It's hearsay. You put it on the web, it's not real. Anyway, I think the good news is you're exactly right, this ain't gonna happen again. And, you know, my kid's school handed out laptops, MacBooks, with cameras on them. And you'd better believe that immediately the question was raised, well, is there any software on there that could monitor it?

Steve: Yeah, and the first thing you want to do...

Leo: And there isn't, by the way.

Steve: We've talked about this before. Laptops really need to start installing...

Leo: Shutters.

Steve: ...a physical shutter, a little slider. I noted that there's laws which require sufficiently high-powered lasers to have a mechanical shutter. Actually they require three things. If your laser is above a certain number of milliwatts in its brightness, it has to have a lock and key, that is, an electrical key. It has to have a mechanical shutter which physically blocks the aperture of the laser. And when you turn it on, there has to be a delay of several seconds between the time you press the "on" switch and the beam actually begins. So there's, like, three requirements for a sufficiently high-powered laser. I know because I own one. And I was curious about all of that rigmarole. And sure enough. So you can imagine that...

Leo: Just out of curiosity. You're not building a new...

Steve: No, no, no. No. No. No animals are going to be...

Leo: Which color is - did you get a green one or a...

Steve: Yeah, it's really very bright.

Leo: They're really cool, yeah. Yeah, Woz had a green one a couple of years ago...

Steve: I mean, this thing will pop balloons. So you want to be careful with it.

Leo: Ooh. Where do you shop for something like that?

Steve: I don't remember where now. But on the 'Net is my standard reply.

Leo: So it's legal, but you have to have these restrictions, like a gun lock.

Steve: It's legal, and certainly you need to use it responsibly. Because, I mean, if it'll pop a balloon, it'll burn your retina, too. So you don't want - this is not a toy to mess around with.

Leo: Geez. Holy cow.

Steve: Yeah. And I'm close to the Orange County Airport, too, so I can't even aim it out in the sky or anything.

Leo: You shouldn't, rightly so.

Steve: I'd have satellites zooming in on me, I'm sure.

Leo: Oh, yeah. Oh, yeah.

Steve: Yeah.

Leo: Did you get the 1W laser?

Steve: It's, yeah. It's pretty bright. Pretty good. So on that note...

Leo: Oh, man.

Steve: ...we have a nice SpinRite testimonial. Last time Greg was the subject of compliments, and I had something about Sue this time that I thought I would share. From a David Speigner, he spelled his name phonetically for me, it's S-p-e-i-g-n-e-r, Speigner. He wrote, and he said - actually he wrote to Sue saying thanks for your assistance in completing my SpinRite order. It's churning away and will not be ready for a while. Would you please forward this to Mr. Gibson? So he said, "Dear Mr. Gibson," and then he put (Steve). It's like, yes, David, we're on a first-name basis. It's quite fine. He says, "I appreciate all your great efforts on security and Windows and Internet vulnerabilities over the past years. I've used a lot of your freeware and tools, such as ShieldsUP!, OptOut, and many others. I just recently used Securable. Actually, Securable is our #1 freeware right now.

Leo: Really. What's that one do?

Steve: People are using it to see what capabilities their chips have for going to 64-bit Windows because it's just super secure and lightweight, and it shows you if your BIOS has virtualization locked on or off, whether you've got 32-bit or 64-bit, identifies your chip by name, like what type of chip it is. And, yeah, people are getting a lot of use. And the news of it is passed around the Internet. It's like, oh, just go get Securable. You don't have to install it, you just run it, like all of my stuff. And it tells you good things about your processor. So people are using it a lot for that.

Anyway, he says, "Thanks for all your great work and expertise. I also very much enjoy Security Now! with yourself and Leo Laporte. Now my SpinRite testimonial. I just got off the phone with your helpful, knowledgeable, and nice sales/customer service lady," and that would be Sue. He said, "Today I had my SpinRite moment - a major catastrophic hard drive failure caused by power outages and surges from a fast-moving lightning storm system here in the East, 70 mph winds from heavy thunderstorms, and the surge protector did not work."

Leo: That's not unusual. Lightning, I mean, imagine how many volts are coming through a lightning strike.

Steve: Yeah, yeah.

Leo: That will jump over anything.

Steve: He says, "The drive was caught in an endless loop, and I knew there were disk errors from using other lame third-party utilities," he says, "three different ones. My OS files were there, but my efforts to repair did not work. One tool said I had 'disk errors,' and the restore points in XP Pro of course would not work. The drive controller chip was possibly fried, as well, and my drive seemed toasted, as well. Of course, I had an image that was about three weeks old, but the drive had the image on it in a different partition, and both were now unreadable.

"So I purchased SpinRite 6 after hearing about it frequently on the Security Now! podcast, after figuring it was my only option, as the malfunctioning disk could not be restored from my saved image or backup, and the reinstallation was also inaccessible, and I needed to get it working again so I could image or do a repair installation of the OS.

"I used your well-designed program to create a bootable SpinRite disk. I started it up, after following the easy-to-follow instructions, and waited. Well, 14 hours later, on a 320-gig drive, there were 12 recovered sectors. And I was then able to boot and have the disk detected in another machine as my motherboard was RMA'd to Intel." So it really did fry things on his machine.

Leo: Yeah. And that'll happen.

Steve: He said, "I did a repair installation, and the machine is back to normal with no files lost. It boots fine, and SpinRite saved the day. It was well worth the cost and time saved, easy to use, and after nearly 20 years of making systems, this was the first time I needed to use it. But I know it will not be the last. Thanks for a great and easy-to-use product. David G. Speigner.

Leo: That's what's neat about SpinRite is, yeah, you buy it, and you have it.

Steve: Forever.

Leo: And you will absolutely use it again.

Steve: Forever. Yup.

Leo: Yeah. It's just always going to be there. Steve, I am ready, if you are.

Steve: Absolutely.

Leo: We've got some questions for you, Steve. Starting with Vegard in Norway, wondering about the security of Bluetooth keyboards. We talked last time about wireless keyboards in general. He says, Steve, what about the security on Apple's Bluetooth keyboard? This is a very widely used keyboard now because it works with the iPad. I've used it. Isn't anything Bluetooth more secure than that simple 8-bit XOR that you were talking about with some of the other RF keyboards?

Steve: Yeah, I wanted to quickly calm everyone's nerves over the issue of keyboard security. We have another question later on about Logitech wireless keyboards that I mentioned earlier in the show. But, yes, anything Bluetooth is, well, okay. Anything Bluetooth is way more secure than a simple 8-bit XOR, if for no other reason than almost nothing could be less secure than...

Leo: Than 8-bit XOR.

Steve: ...than an 8-bit XOR. I mean...

Leo: It's not saying much, in other words.

Steve: Well, exactly. So...

Leo: But it does have the pairing and the authorization, I mean, it has some security model in it.

Steve: Oh, Bluetooth is good security, very good security. And in fact one of my - it's on my short list of future topics because a number of people have asked over the years. And so we're going to absolutely do an entire Security Now! podcast on the technology of Bluetooth security, since Bluetooth is getting increasing use now all the time. I also have one of those Bluetooth wireless keyboards. It's great with the iPad, it just works beautifully, and I like the keyboard very much. And so...

Leo: Oh, it's beautiful. It's small. It's, yeah, it's very elegant.

Steve: Yeah. I mean, so it just makes it - it pairs beautifully. And there is absolutely no problem with using a Bluetooth keyboard from a security standpoint. So I did want to let people know, it's not certainly the case that anything wireless is a problem. It's just that first-generation sort of cheesy, very inexpensive wireless keyboard was found to be really insecure because, I mean, literally zero encryption, just flipping some bits that were always flipped the same way. So very uninspired.

Leo: Yeah. And we hear about Bluetooth snarfing and stuff. There are ways to hack Bluetooth.

Steve: Yes. In fact I remember, Leo, that we discussed, in general we discussed the problem of leaving Bluetooth in discoverable mode. We did a segment on your Screen Savers show up in Canada once, or Call For Help, I guess it was. And just turning on Bluetooth in our laptop, we saw that everybody had left their phone that way. Everybody's phone was discoverable. There was, like, 12 of them or something.

Leo: Wasn't that funny? Yeah.

Steve: Yeah. And so...

Leo: But we learned our lesson, however, at that time.

Steve: Yes. And that is the danger. You do not want to leave your Bluetooth devices discoverable. I've never understood why the user interface isn't set up so that it just flips it back off.

Leo: It is now, I think, in almost every device I've ever seen.

Steve: Yes. And I've really seen a change over the last few years where you manually make it discoverable, and then it takes responsibility itself for flipping it back off because that's how Paris Hilton loses her phone book and so forth.

Leo: Oh, Paris has many ways to lose her phone book. She's discovered every technique possible. Al Murray, Gainesville, Florida wonders about Computrace's LoJack for laptop security. We've seen a lot of ads for this. Steve, I just bought and received a Dell notebook, noticed in the BIOS configuration it had a Computrace option that was not activated. Seeking more information, I did a search and found it's a product from Absolute Software. They also do the LoJack software. I think they license the LoJack name because it's the same idea. LoJack's for a car.

Steve: Right.

Leo: I would really like your thoughts on using this product on my Netbook since we all know how easy it is to have a laptop or a Netbook lost or stolen. Should I use Computrace or the LoJack? Are they the same product? By the way, I can't remember when I first bought SpinRite, but it has saved my bacon many, many times. Love your podcast. Thanks, Al.

Steve: Okay. So in general I think it's a good idea. I love the idea of this being in the BIOS because that moves it to a place where it's just not prone for deletion or discovery or removal. What it does is it takes advantage of the increasing size and sophistication of contemporary BIOSes to actually build a network client into the laptop itself. Meaning that, when the laptop is on, without, I mean, in an OS-independent fashion, I mean, you don't even have to have an operating system loaded because it's not using the OS at all, it's just using a block of code in the BIOS and the fact that the network adapter, whether WiFi or wired, is part of the hardware, so the BIOS knows how to talk to that hardware. Again, it doesn't need drivers. Drivers are used to interface the operating system to the hardware; but in the BIOS, the BIOS knows what it's got.

So Computrace has licensed to Dell their technology, and Dell builds it in, as do many Netbook and laptop makers, build it in as a feature which you can turn on. Now, it's not free. The whole deal is you need to subscribe to this. And so I guess the issue of, is it worth it, should I turn it on, which Al is asking, is a function of your use of your laptop, your likelihood of it getting away from you, the possibility that it's got confidential data on it, the likelihood of recovery and so forth. What it costs is $40 for a single year, or $90 for three years.

So what happens is, when your laptop is turned on, once a day - because again it also has access to the clock and calendar, so it knows how often it's being turned on, when it's being turned on, if it's already been turned on that day and so forth, it won't do it more than once a day. When it's turned on and hasn't been for 24 hours, the laptop itself, separate from your operating system, is able to use your network adapters and contact Computrace. It essentially sort of sends them a ping and identifies itself by serial number. And this is something set up when you activate this feature in the laptop. There's an account number and identity and so forth.

And so Computrace is receiving pings from all the laptops which have subscribed to their service all over the world. Every day they're receiving these. So if you lose your laptop, or your car is broken into and it's stolen, or you leave it in the airport, which is where most laptops get lost or misplaced or stolen, or you leave it in the seatback - I know, Leo, you've gone through many Kindles that way.

Leo: Yes. Yes.

Steve: So if one way or another it gets out of your control, and it doesn't look like it's going to come back, you the subscriber contact Computrace and say, hi, I'm Al Murray in Gainesville, Florida. Here's my account number. I need you to figure out what we should do. So you give them your account number, and they now wait for your stolen laptop to be used by the bad guys, to be turned on, to be plugged in, to be whatever. And as soon as that happens, if your laptop can reach the Internet, if it's near a WiFi or if it's plugged into the bad guys' hub, it reaches out, pings Computrace as it always does. This time they're primed. Computrace is able to tell the laptop immediately that it's been stolen, so the laptop knows that it's in, like, I've-been-stolen mode.

That does a couple things. One thing it does is it increases its communications from once a day to every 15 minutes, so that they're able to track it. It also is able to use standard - we've talked about this several times - the amazing geolocation of WiFi to figure out where it's located. So it's able to report its physical location to Computrace. And of course they get the IP address that it's pinging them from. So they have the IP address. They have the WiFi-based geolocation data. And Computrace is then able to deal with the local (to the laptop), local law enforcement authorities and set about seeing if they're able to get it back.

Now, the other thing that Al could ask Computrace to do, if he is more concerned about his information, depending upon what kind of information he's got on the laptop, he can ask Computrace to lock down the laptop and/or wipe the hard drive. So that can all be done remotely at his desire, based on the conditions of how it got lost and how long it's been gone and so forth. So the laptop can lock itself down and refuse to function, simply putting up a notice of some sort saying I've been stolen, you're bad guys, you're not going to get access to me, sorry. And so for 40 bucks a year, 90 bucks for three years, depending upon your use of the laptop, sounds like it might be useful.

Leo: There's a program for Macintosh called Undercover that's very similar, but it uses some other techniques. It uses Skyhook to locate itself, but it also knows all the IP addresses for Apple stores. And since people often bring their stolen laptops, I guess, to Apple stores, it immediately goes, I know where I am.

Steve: Interesting. Interesting.

Leo: It sends pictures from the camera of the person who stole your Mac.

Steve: Oh, that's a good one, too.

Leo: Yeah. Every eight minutes. And then, if you can't get it back, it simu- I love this. It simulates hardware failure by making the screen gradually darken to unusable, and hoping that the thief will then bring it somewhere...

Steve: Toss it out.

Leo: Yeah, toss it out. It also does - you know, iPhones now, and iPads, have the Find My iPhone, and I see Android phones do this, too, with Lookout. They scream if they're lost.

Steve: I've been stolen, agh.

Leo: I've been stolen. Or you can find it, if you dropped it, you left it in a seat cushion, or you left it in a restaurant, you can have it scream. It's interesting, I mean, people lose these portable devices so often that it's not surprising there are many solutions now for this.

Question 3, from Krister Jonsson - we've got a lot of Scandinavian listeners - in Lycksele, Sweden, wonders about anonymous web surveys. Hello, I've been asked to fill out surveys and questionnaires at work. The surveys are supposed to be anonymous, but quite often I get a link containing a unique ID so that the person who made the survey can see who finished the survey and who hasn't done it yet. I always ask, how can I trust that the survey really is anonymous, and so far the answers I get are along the lines, well, yeah, you can have a unique ID. That's so I know if I you fill out the survey. But I can't connect that ID to you. Of course they could have a list with all the IDs. And they know who got what ID, and it wouldn't be too hard for them to store the IDs with the answers.

To me this feels like playing cards with somebody saying, "Trust me, I don't cheat," while they leave the room to supposedly shuffle the cards. I like that. Is there a way to design a web survey so that respondents can trust the system, while at the same time those offering the survey and wanting the results can know who has answered or not? This actually ties to something The Wall Street Journal has accused Facebook of doing, or actually Facebook third-party game and applications are doing. They also send, need a unique ID of some kind, and often send the Facebook userID, which can then be used to scrape public information from the page. The Journal considered that a privacy violation. You know, it's public, it only scrapes the public information, so I don't know if that's as bad as it sounds. A lot of pages do this. This is not unusual; right?

Steve: Well, and I thought about this question.

Leo: Interesting problem.

Steve: Yeah. And the problem is, if you don't trust the survey-taking system - so it sounds like, for example, this is at work. So management is saying, okay, all you minions, we want to know what you really think. And we're going to help you to tell us what you really think by making this anonymous. And the minions are suspicious, of course, saying, well, but if I tell you what I really think, and you know it's me, and I tell you that you have bad breath, then you might hold it against me when it comes for my next job review or whatever.

So you can imagine, you can see that this sounds like it's a potentially adversarial situation where management really does probably want to know what the employees really think. The employees probably really want to tell management what they really think. But the anonymity barrier and this lack of trust in the survey system is preventing both sides from getting what they want.

So the only thing I could think of, and I pondered this for a while, is if, first of all, if people could approach a computer without having to identify themselves, that is, not log on because obviously then they know who they are. If they could, like, use any computer, or like say it was in the coffee room or something, so it was like it was there to be anonymous. And they fill out the survey, and then they receive some sort of a unique token, like write the following thing down, these numbers and digits. And that's to prove that you filled it out.

Okay, now we still have the problem that that is tied to them, to their answers. So the only thing I could think was that, I mean, and this is annoying. But if everyone really wants anonymity, if management really wants the truth, and the employees really want to be able to tell the truth without being identified, is everybody then who says they filled out the questionnaire writes down these tokens, and they all throw them in a hat and scramble them. So that process disassociates the people with the tokens. Management is able to say, okay, we know everybody who threw the tokens in the hat. And we know that we have the same number of tokens as we have people. And all the tokens are valid. So we know that everybody answered the questionnaire.

Leo: That's a good idea.

Steve: So we don't, I mean, there has to be some decoupling somehow between answering the questionnaire, I mean, if you really don't...

Leo: But you wouldn't...

Steve: If you don't...

Leo: You would only know somebody didn't answer it. You wouldn't know who.

Steve: Correct. And that's the problem. And but that's the benefit is - so you would know that someone didn't answer. But you couldn't know who. But if you had, if everyone said I answered, and they threw their little tokens in the hat, then you scrambled them up, and you saw that the right number of people...

Leo: Answered them, yeah...

Steve: ...answered them, then you wouldn't know who was associated with what. You would only know that, yes, that everyone had taken the questionnaire. I mean, it really is a problem to disconnect that kind of verification from the questionnaire in a system you don't trust because that's the problem is we're assuming that this is not an anonymous system. I mean, if the software were designed correctly, absolutely, it would be possible to give someone a token which is completely disconnected from who they are. But that would require that the employees being given the questionnaire trust the management not to want to try to figure out who they are. I would suspect it's in management's best interest not to know so that they get the truth from the employees. But again, if there isn't that trust, throwing the tokens in a hat and scrambling them up, it says, okay, now I don't have to trust you. We just know that the right number of people did answer the question.

Leo: You'd get that information if you just look at how many people answered.

Steve: Right. Yeah, very good point.

Leo: It's not going to get you any farther than you are, really. It's an interesting question. Somebody in the chatroom said, well, I have the same problem when I'm told this is an anonymous phone survey. But they've got my number. It's not really anonymous.

Steve: Right.

Leo: So Krister, there is no answer for you. And if you're going to answer surveys, you're going to have to assume that it's not necessarily anonymous.

Steve: Well, and again, web-based is a problem because it's online. If you print the survey out...

Leo: Then it's anonymous, yeah.

Steve: ...and then fill it out with your other hand, so even your handwriting is wacky, then put all those in a hat and scramble them up, then it's anonymous.

Leo: Right. Yeah, the problem is the web. And this was kind of the response to the Facebook issue is you're not anonymous on the web. All websites know who you are. They know your IP address. So you're fundamentally not anonymous.

Steve: No. And last week's episode was the Evercookie, so...

Leo: Right, you could even get worse.

Steve: ...it's hard to shake this stuff off.

Leo: Scot in Seattle wonders about the security of his Windows Gadgets. Is there any danger, Steve, with Windows Desktop Gadgets? Those are the things, if you use Windows Vista or Windows 7, they're the little doohickeys you could put on the screen. I use a clock, a CPU monitor, weather, that kind of thing. I see a ton of them listed on the Microsoft website. Some are from Microsoft, but most are not written by real companies like Amazon or Google. They're just individuals. Is it dangerous to download and use a Desktop Gadget written by someone you don't know and not by an established company that signs their gadgets? Scot in Seattle. Yeah, I'm guilty of that. I download third-party - I download them from Microsoft. But I don't know how much vetting is done, and I don't even know how secure the gadget model is. Have you looked into that?

Steve: Yeah, I have, actually. And it's not.

Leo: Oh, okay. There we go.

Steve: Not secure. It's just the same as running...

Leo: It's JavaScript; right?

Steve: It's JavaScript and XML and CSS. Basically it's sort of web-ized gizmos. And they're subject to all the same security problems as everything else. Microsoft goes to some level of effort to try to educate the authors about checking the buffer bounds, making sure you use a specified character set, UTF-8, for example, I mean, they go to some lengths to try to help people write secure gadgets. But we know how well that's going to work.

So the gadgets could be deliberately malicious, or they could unfortunately be flawed. So if a gadget were very popular, for example some weather gadget, it might be possible to send it bad data which causes a buffer overflow in it, and would allow someone remote access to your machine. So that kind of vulnerability exists in the Windows Gadget Desktop space just as it does in regular applications. Unfortunately we're getting more gizmos, and they're vulnerable.

Leo: And by extension, in case you're interested, on the Macintosh Yahoo! Widgets or the Macintosh Dashboard Widgets, they're also JavaScript, CSS, and XML. They're all done the same way. So they're exactly the same security issues.

Steve: They're modern.

Leo: Yeah. And I presume on the Mac side it's WebKit that renders that gadget. I don't - I presume it's IE that renders the gadgets on the Windows.

Steve: Yup, exactly.

Leo: Jason Crow in Rochester, Minnesota wonders about an Evercookie workaround. If you listened to the last episode, you know about the Evercookie. Question for you, Steve: If I have an image of my OS partition - like a ghost - and I restore that image on a regular basis, say every three days or four days, does Evercookie have a way of working around the ghost and saving its supercookies? Could Evercookie be storing information, let's say on somewhere not part of the image, on the boot partition or on a D: drive? Do you think other tracking schemes could? Thanks, Jason. And I guess by extension Microsoft SteadyState or Faronics Deep Freeze. These are all programs that restore your system to a previously known good state automatically.

Steve: Yes. And so here's the problem. We know what Evercookie is doing because it's open source, and freely available, and clearly documented. So the author has said, here are all the things I'm doing. And he sort of did it more as a capability demonstration, but just to show how sticky these things could be. So it may not be that today it's looking around at other drive letters, other places to squirrel away its data. But gee, that's a handy idea. So tomorrow it certainly could be.

Leo: Yeah, it's just a question of whoever maliciously implements it thinking of other ways to do it.

Steve: Yes, yeah. The idea is, when you've got scripting on your system, anything that scripting can do can be done.

Leo: Yeah.

Steve: And that's all I have to say about that.

Leo: That's all there is to say. Yes, the answer is yes.

Steve: Yeah, it's bad.

Leo: We've seen viruses that go into BIOS, into the CMOS nonvolatile memory of BIOS. We've seen viruses that sit on master boot records. They're always going to try to be somewhere that is not overwritten.

Steve: Yes. The only thing, the only thing I can imagine that would really give containment, essentially, it would seem to me that, for example, VMware has that snapshotting feature where you're able to run an image, but snapshot it first, and save no changes. If you were careful to circumscribe the environment, that is, not map external drives into that, not allow other things to have access, in a virtual machine you're always sort of starting with a generic system, that is, all of the VMs from VMware look like the same hardware. They look like pretty much they're identical because the VM brings that characteristic with it. It's masking all these details of the outside externalized system. So that's a really good way of preventing tracking.

And if you set up that snapshot feature, then nothing that changes in the VM is kept. It's very much, as Leo was saying, like SteadyState. And then we talked about this before, but I'll remind our listeners because, I mean, there was a lot of concern raised about this, is booting a temporary desktop, booting one of the Linux boot CDs that fires a system up and gives you a desktop with Firefox on it...

Leo: That would work.

Steve: That works.

Leo: There's no way that could - because it doesn't reference anything in, you know, you'd have to get stuff in RAM. I don't know how you'd do that.

Steve: Yeah. Well, exactly. And so it's going to clean out an area. It's going to load into that. You can surf in there. And when you shut it down, again, so long as you don't deliberately penetrate the bounds of that, I mean, there are ways, like, to map external drives in and things. But if you don't do that...

Leo: Don't do that, yeah.

Steve: ...then you have an absolutely transient surfing experience. And every time you boot it, it's going to start over, just like it did before. And no cookie will be able to hold onto you.

Leo: No cookie can survive. Steven Musumeche, or something like that, in New Orleans...

Steve: Boy, you're good with those names, Leo. That's swell. I couldn't do better than that.

Leo: You say that, but who knows? It could be pronounced Sade, I don't know. Musumeche, Musumeche in New Orleans wonders - I know how to say that, New Orleans - wonders about wireless keyboard encryption. Steve, I use the Logitech K320 wireless keyboard. They say it's not using 8-bit XORs, it's using AES-128. What do you think? That's pretty good.

Steve: So, yes. I...

Leo: I'll take that.

Steve: I decided there was a lot of concern, as I mentioned earlier, raised about the whole issue of wireless keyboards. So I did some research, read some whitepapers and some security evaluations and so forth. And the good news is Logitech got it 100 percent correct. They did a beautiful job. I sort of smiled when they were talking about how they don't bother encrypting the mouse because all it does is send relative movement. And I thought, wow, why does that sound familiar? That's exactly what we said last week. There's no need to encrypt mice. Keyboards, however, of course, is a different story. And they handle that beautifully. There's nonvolatile memory in the keyboard and in what they call their little unifying receiver. This is Logitech's new technology.

Leo: Oh, yeah, yeah. I use that, yeah. It's a little tiny dongle.

Steve: Yes, you and I have a lot of those because we love those little MX mice.

Leo: Yup.

Steve: With the frictionless wheel. I've got them in all my laptops. So this is a little tiny receiver that just looks like a little bit of a head on top of a USB connector. You stick it in your USB port of your laptop, and you just leave it alone, or your desktop or whatever. And the idea, they call it a unifying receiver because one receiver is used for multiple devices. Up to six can be paired with a single receiver.

Leo: Now, it's not Bluetooth, is it. It's some proprietary thing.

Steve: Yeah, it's 2.4GHz.

Leo: Oh, interesting.

Steve: And they make the comment that 2.4GHz has a range of several tens of meters so encryption of keyboard strokes is very important. So at the factory, nonvolatile memory in the keyboard and in the unifying receiver are synchronized with the same 128-bit symmetric key, which the AES algorithm uses to encrypt keystrokes. So if you repair the keyboard, because for example you might pair it with a different receiver that hasn't seen that keyboard before, the pairing process does exactly the right thing. There are pseudorandom number generators at each end. They are able to...

Leo: Really.

Steve: Oh, yeah.

Leo: That's amazing.

Steve: They're able to establish a new key without it ever going over the wire, over the air, in the clear, in order to synchronize a new key that they agree upon on the fly. That's written into nonvolatile RAM and kept there.

Leo: That's mindboggling, that that little thing can do that.

Steve: Yes. They did a beautiful job.

Leo: Wow. I guess if you could put it in a VeriSign card or a PayPal football, you could put it in a little dongle there.

Steve: Or, well, and I'm thinking of the YubiKey, too, that's like super thin and does all that same kind of stuff.

Leo: Right, right.

Steve: So, yeah, this does...

Leo: That's impressive.

Steve: It's really nice. Very nice. So I haven't looked at anybody else's. But I know that the unifying receiver technology that Logitech has is doing this. And it does say in the specs, just in the regular top-level specs, 128-bit AES encryption. So that's the way they implemented it. I would imagine anything that Logitech has done, even if it's not the K320 wireless keyboard, that also says that would be using the same technology, which means you can trust it.

Leo: I am impressed. And kudos to Logitech because they used XORing in some of their earlier stuff.

Steve: Yup.

Leo: But they've obviously learned their lesson. So you could use that with confidence. Wow. That's amazing. David Eckard in Durham, North Carolina, wonders about IP space depletion. And we ain't talkin' the Shuttle here. He says, "Subject: 95% used up." He said, according to this article, and he quotes a CNET article, IPv4 addresses are now all but 5 percent done. And they're calling for an orderly move to IPv6. This is something Vint Cerf, the father of the Internet, has been saying for a while. Although he's been saying it for years, and it turned out it wasn't really a crisis until recently.

Our correspondent David says, I still say there hasn't been enough work done on the transition. IPv4 devices like my iPod Touch simply can't go to an IPv6 website and vice versa. This requires a translator computer. Translator computers are still in the development stage, as can be seen by various articles. We have seen Comcast in particular working on this very issue. I also expect cell carriers to participate when those come available as 16 million class A addresses are simply NOT enough. Can you talk about this? What do you think?

Steve: Okay. So if you haven't, Leo, click that link and look at the chart. That CNET article has a very nice graph of where we stand and where we've been since the beginning of '06. One way, okay, we know that IPv4 addresses are 32 bits long. So, and we know that IP addresses are in the so-called "dotted quad" format. 192.168.0.1, for example, is one we've all seen for private IPs. So the top, that first number is - it identifies a block of IPs where the other three numbers are sort of subsidiary to it. So anything starting with a 4, for example, Level 3 owns all of the 4-dot space. And, for example, 5-dot has been unallocated, and as far as I know it still is. That was what the clever developer, Alex of Hamachi, was using because there were no five-dot IPs out on the public Internet. It had never been allocated.

So to give our listeners a sense for where we are, at the beginning of '06 there still remained 62 unallocated, what's called a "slash eight network," meaning only the top, specifying just the top eight bits of the network address out of a total of 256 of them, which is how many combinations in a single byte. 62, even in '06, were still unallocated; so, what, just shy of one quarter of the entire Internet, because 64 is one quarter of 256 possibilities. So 62 were unallocated in 2006. One year later, that number had dropped to 49 in '07. One year later, in '08, to 41. In '09, to 32. At the beginning of 2010, we were at 22. Today we're at 12.

Leo: Wow.

Steve: So, yeah.

Leo: That's a dramatic drop.

Steve: Yeah. And so things like 5-dot will not be available for long. In fact, my feeling is, my summation to sort of sum this up overall for David and our listeners, is I think 2011 is going to be very interesting.

Leo: Interesting in not a good way.

Steve: Yeah. I mean, at the rate it's been dropping, we burned up, between '08 and '09, we went from 41 to 32. So that burned up nine. From the beginning of '09 to '10, to 2010, we went from 32 to 22. So we burned up 10 more. Between 2010 and now we went from 22 to 12, meaning we burned up another 10 in less than a year.

Leo: It's accelerating.

Steve: Yes. It was nine for the prior year, 10 for the year after, and now we're already at 10, and we're not done with this year. Which says, and this is what the predictions are, that before this time, before October is through of 2011, we're done. We're out.

Leo: But it sounds like, I mean, at least from our correspondent, we're not ready. Are we not ready?

Steve: I completely agree. We're not yet using IPv6. My cable modem has an IPv4 address. When I look in my iPad...

Leo: And you know it is because it's four dotted quads; right?

Steve: Yes, exactly. Now, and that's the difference. IPv6 goes from 32 bits to 128 bits. Now, again, we glibly talk about bits. But remember that every single bit doubles the number. So if we just went from 32 bits to 33 bits, if we just added one bit, that would double the number. I mean, that would last a long time. Well, they didn't just add one bit. They went from 32 bits to 128. They added 96 bits.

Leo: So instead of...

Steve: 96 doublings.

Leo: Instead of 192.168.1.1, we're going to see 192.168.1.1.1.1.1? Is it eight?

Steve: The new IP addresses are insane. They're insanely long. Now, what they did was they folded the IPv4 space, as you would expect, into the IPv6. So IPv4, what we have now, 32 bits, it occupies one little infinitesimal microscopic nano-size corner of, I mean...

Leo: Of the space, yeah.

Steve: ...everything we have now. It's just - it's vanishingly small. It disappears in the IPv6 space. Which is fine, except that we're not really using IPv6 yet. I mean, the specs are solid. The hardware is there. For example, XP, old XP that I'm still sitting in front of, it has an IPv6 TCP/IP stack. You can literally, there's a command you can give to a command prompt that turns it on. And then it works. I mean, it's there. But it's not turned on by default.

And when I go out with my iPad and look under network settings, when I'm hooked into some WiFi, I've been given an IPv4 address. So, like, a public IPv4 address, meaning some public IP, not 192.168.something or other. So what that says is that the world is still actually using IPv4 because no one wants to do anything until they absolutely have to. Which is why...

Leo: Well, we have to.

Steve: Which is why 2011 is going to be so interesting.

Leo: So I'm looking at an IPv6 address. First of all, it's in hex.

Steve: Yup.

Leo: And instead of dotted quads, it's eight, dotted octos.

Steve: Yes.

Leo: And it's colons, not dotted. So it's four hex digits in eight groups of four. So it is a - I guess it's a quad still. But it's - so okay. And that's huge. I mean, if you just even look at it, it looks huge.

Steve: Oh, yeah.

Leo: It's hex.

Steve: People had a hard time remembering IP addresses. Well, you don't even try with this thing.

Leo: Oh, you don't. This looks like a MAC address times two, basically.

Steve: So the idea is this IPv6 space is so big, everybody who wants some can have it. The problem is...

Leo: You can have your own Class A address.

Steve: ...you can't do anything with it right now.

Leo: Right. Well, so are they going to go to universities, I mean, there are people who have Class A addresses that aren't using them. Are they going to go to these guys who are, you know, there's the bandwidth hogs. Now there's IP address hogs. Are they going to go to them and say you've got to release them?

Steve: Yes. Even four years ago, when I signed up for my - when I moved things away from Verio because Verio was shutting down their T1 business and I didn't want to move all my stuff to Cogent, and I tried XO for a while but I kind of got scared off, and I went to Level 3, just a big Tier 1 provider, I had to fill out an IP - they had a name for it.

Leo: Justification form.

Steve: Yes, it was a justification. It's like, prove to us why you need 16 IPs. What are you going to do with them? Justify your use of the space. So already they were feeling jealous of their own space. And I know that chunks are still available because Alex down at Sunbelt, he has a Class C. So he's got a full block of 256 IPs. But those are becoming hard to get because that's a chunk of space. But as you say, Leo, there are old-time universities that, I mean, Stanford I think has two Class A networks, or no, Hewlett-Packard...

Leo: HP has a ridiculous number of addresses.

Steve: Yes, because they were in very early. And they said, oh, well, we'd like a chunk, please. And so they got given a chunk. Well, I'd be very surprised if they're actually needing and using those IPs.

And so, and here's the other thing, Leo. Yes, it's the case that in theory the original concept of the Internet architects, and we're going to be discussing this in detail when we start in on our How the Internet and Networks Work series, which will be the next series we do, their original concept was every single endpoint on the 'Net would have its own dedicated IP. And so you could get to any machine from any other with an IP. Well, the fact is the world's changed. People have networks at home that these gurus back then never imagined. It's true, under IPv6 we could return to every single endpoint has its own IP.

Leo: But there's no need.

Steve: Exactly.

Leo: Because we have routers.

Steve: The fact is, yes, every single endpoint doesn't need its own IP. And so universities, Hewlett-Packard, corporations, I mean, the fact is, I think what we're going to see is a scrambling towards NAT routing to a much greater degree. The pressure to move to, I mean, ultimately we'll be on IPv6. But when the screws get tightened, sometime around summer of 2010, people are going to have to justify their use of IP space. And they're probably, I don't know if there's a provision for recovering IP space from someone who has it. But...

Leo: Well, they can say, look, be a good Internet citizen, HP. Can you give up 10 of your 14 million IP addresses? Although 10 million new addresses aren't going to really solve the problem.

Steve: See, and that's just it, is that everyone understands, ultimately we need to switch. Or we really need to be a lot more aggressive about NAT routing. I mean, the purists, they see red when we talk about NAT routing. They're like, just get it done. Just switch over. The problem is, it's not easy. I mean, I've got routers that are running IPv4. And so, I mean, it's a huge amount of work to make this change. I mean, it really, it changes the fundamental plumbing of the Internet in a way that it doesn't want to get changed.

Leo: So we'd all have to get new routers. Or our internet service providers would have to get new routers. Who has to do this?

Steve: Our routers right now do not support IPv6. So they need firmware updates, assuming that they can be updated.

Leo: Probably can't. I mean, I would imagine that you've got to assign a certain number of registers for the number. That's really, that kind of thing is hard-wired in.

Steve: Yes.

Leo: A 32-bit number is your IP address, that's hard-wired in. To go to 128-bit, that's architecture.

Steve: It may very well be. Sorry, you can no longer use your router. You need to go get a new router. That's a big deal.

Leo: Now, somebody must be making routers with IPv6 compatibility.

Steve: Oh, yes. And...

Leo: So if you're buying a new router, you should make sure of that.

Steve: That would be a very good thing to check off. Make sure you're not going to be obsoleted when the world actually does move, whenever that is.

Leo: Oh, it's going to be ugly.

Steve: It's going to be fun.

Leo: Ah, may you live in interesting times.

Steve: Yes. I really do think we're going to see NAT happen big-time. It's just it's the path of least resistance for quite a while.

Leo: And is there a robust Dynamic DNS solution for people who want to run their own servers, but don't have dedicated IP addresses?

Steve: I mean, Dynamic DNS works. And that really is the - that's the argument that is a good argument against NAT, is that NAT works as long as all you have is clients behind the NAT router.

Leo: Servers want their own address.

Steve: Servers need a way, you need a way from outside uniquely accessing the machine behind the NAT. And port mapping and things are kind of a kludge. They're just - they're bad.

Leo: Ken, did the new switch we just got, does that support - anything new, I would hope - of course these Linksys routers have become a commodity, these cheap, $30,

$40 home routers, they're a commodity. I wonder if they, you know, they're cranking them out at a rapid clip.

Steve: I do know that looking at the UI of mine, there's no sign of IPv6 support - none.

Leo: And Alexandre Garcia in Portugal with our last question of the day, he says maybe the Evercookie is not so Evercookie, not so "ever." Hi there, Steve and Leo. I've been listening to Security Now! since Episode 1. I want to thank you for all your efforts in explaining so well the problems with security in the computer world. Regarding your last topic, the Evercookie, I just want to remind you that Sandboxie is perfect for people concerned with this kind of menace. I've visited the site under a sandboxed instance of IE, and let it set the Evercookie. This is Samy's site, samy.pl. Then I've closed the browser and run it again under Sandboxie. Sure enough, the site was able to set the Evercookie on my system, of course, inside the sandbox. Then I've just flushed the sandbox, visited the site again, using the same IP. The Evercookie site was no longer able to track me at all. So it worked.

Sandboxie was able to prevent that the Evercookie could write into my "real" system anywhere. And once again I was happy to be browsing under Sandboxie. Of course if the Evercookie were to store at server side my IP, they could have regenerated the cookies. But at least they weren't able to create permanent changes on my computer. Sandboxie blocked them. Keep up with the good work. Alexandre in Portugal.

Steve: Yeah, I wanted to just add that Sandboxie, which we have done a podcast on in the past, and I'm very impressed with, I thought it was a nice data point that we had, which is the Evercookie does not currently penetrate the sandbox. And given what I've seen, it's probably up there, not quite as robust as a full heavyweight VM, but so much more convenient because it's not a full heavyweight VM. And remember, a VM requires that you give it a chunk of RAM to run another instance of your operating system from. So it doesn't come at zero expense, whereas Sandboxie is way more economical. And, I mean, it just sort of automatically sandboxes your browser. So Sandboxie is a great solution. And when you flush the sandbox, as Alexandre showed, the Evercookie is lost. So that's great news.

Leo: Yay. Happy news. Happy, happy, joy, joy. Steve Gibson is at GRC.com. That's where you should go to get, of course, SpinRite, the best hard-drive maintenance, the must-have hard drive maintenance utility and recovery utility. GRC.com. Somebody asked if it works with these new eight-bit sectors or something?

Steve: Oh, 4,096-byte sectors.

Leo: Yeah.

Steve: Yes, it does.

Leo: Because you use - anything that BIOS works with, you'll work with.

Steve: Right. And those drives do a great job of looking like existing drives. All existing software is compatible with them. The idea was that drives had sectors divided up into 512 bytes, 4,096 bits per sector, with individual sector header information interleaved with every sector. And the manufacturers realized, wait a minute, we're wasting a lot of space with overhead here. We can cut down the per-sector overhead by making jumbo sectors. And so that's just what they did. They're 4,096-byte sectors instead of 4,096-bit sectors. So many fewer physical sectors. But they simulate the same 512-byte sort of subsectors, just by dividing the physical sectors up into smaller pieces. So, yes, we're completely compatible.

Leo: Yay. And then you were saying that your most popular program now at GRC.com...

Steve: Securable.

Leo: ...is Securable. That's interesting. That tells you how secure your hardware is.

Steve: Well, I designed it because it tells you how securable your hardware is. That is, what features your hardware has. But the world realized, hey, it's a simple, fast way of knowing if I've got a 64-bit-capable system.

Leo: Right.

Steve: For, like, Vista 64 and so forth, or Win 7 64.

Leo: I put Win 7 64 on my Mac Pro, runs beautifully.

Steve: Yeah.

Leo: Although I think I'm right in saying this, I think Sandboxie will not work with 64-bit.

Steve: Yeah, I remember that was the case last time we talked about it, yes.

Leo: I'll have to check. Sometimes you move ahead too fast. So get Securable. That's free. ShieldsUP!, all sorts of great stuff, free at GRC.com. And you can get the show there, too: GRC.com/securitynow, 16KB versions for the bandwidth-impaired, transcripts for those who like to read along, of course the full show notes. We also have them at TWiT.tv/sn. And I always put the show notes on the wiki. I should mention that, wiki.twit.tv. Most of our shows either have show notes where our hosts put them there, or our volunteers. We have a lot of volunteers working on that wiki. It's a media wiki, just like Wikipedia. And so a lot of people know how to do that, and they keep that up to date. And that's a really great resource, if you want more information, as well - wiki.twit.tv.

Let's see, what else? If you want to watch us live, we do this show live normally, and we're doing it on Tuesday because tomorrow's a big announcement for Apple, but we do normally record Wednesday, the day before the show comes out, Wednesdays at 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1800 UTC. You can watch that live.twit.tv; chat with us at irc.twit.tv. It's kind of fun to do it live. But of course if you can't make the live broadcast, you can always download audio and video at TWiT.tv/sn. And I would just subscribe. That way you always have it. Steve - oh, next week, do you know what you're going to talk about? Or is this a surprise week?

Steve: Next week we're finally going to talk about "Benchmarking DNS," how to know how fast your DNS servers are. It's been my sort of project for, boy, like a year and a half. And I'm finally ready to take the covers off and show everybody what I've got.

Leo: Yeah, because you wrote a DNS benchmark program, and you've been...

Steve: THE DNS benchmark, Leo.

Leo: THE DNS.

Steve: THE.

Leo: THE DNS benchmark program. Good, that'll be fun. That's next week. If you have questions for Steve, we do that every odd episode now. It's back to odd; right? I can't even tell. We're odd today, aren't we?

Steve: Oh, we're definitely odd.

Leo: So go to GRC.com/feedback to leave questions for Steve, and we'll get to as many as we can. And I think that's all I need to say. But have a great week, and we'll see you next time on Security Now!.

Steve: Thanks, Leo.

Leo: Bye, Steve.