Listener Feedback #98

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-261.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-261-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 261, recorded August 11, 2010: Your questions, Steve's answers #98.

It's time for Security Now!, the show that covers all of your security and privacy needs. Steve Gibson is the man about town, covering everything having to do with security, from GRC.com.

Steve Gibson: The man about town.

Leo: Man about security.

Steve: You come up with something new each week, Leo.

Leo: You're very dapper...

Steve: My secure bunker look...

Leo: Yes. The man about bunker, I should say. No, you're very dapper. You've even got the moustache. I could just see you with a monocle, a little top hat, a cane. Kind of look like Mr. Peanut, actually. No.

Steve: Oh, that's good.

Leo: No, you're very dapper. You have that Ted Turner kind of dapper look.

Steve: Stop encouraging you now.

Leo: Hi, Steve. How are you?

Steve: Great. Great to see you.

Leo: Yeah, I've been on vacation. I've been - the last show I did was, I think, this show, or This Week in Google; and then I took off for a trip back East with my daughter to bring her to college. And now I just got back. You're my first show back in.

Steve: Fantastic. I love it that you leave immediately after recording one and then get back just before we need to record the next one.

Leo: I couldn't miss this. Now in our - still in our fifth year.

Steve: Struggling out of our fifth year.

Leo: But this might be the last episode in our fifth year, a Q&A episode. Am I right?

Steve: The consensus is that this is the last episode of year five. So, yes.

Leo: It's really great because this show, of all shows, attracts the engineering mind, the serious geek. And of course we always have this "did you start counting with zero" kind of an issue and all of that stuff.

Steve: And, I mean, we've got threads over in the newsgroups at GRC about, wait a minute, the show numbering, and which year, when the leap year is factored in, blah blah. It's like, oh, goodness. So, yeah, anyway, we have a Q&A, #98.

Leo: And what would that be in hex? No, no.

Steve: Lots of news this week. And eight neat questions and comments and thoughts from our listeners. So another great podcast, I think, ahead of us.

Leo: Let's kick it into gear. We'll start right away with security updates, as we do every week.

Steve: Well, Microsoft has broken another record, all-time record for the number of vulnerabilities patched at once. We are just past the second Tuesday of August. So of course we know that means Microsoft's release. Now, it would have been 15 sets of updates had they not pushed the emergency one out last week for the shell LNK vulnerability.

Leo: Holy moly.

Steve: And we've got some news about that, too. But so they only did that one in emergency mode, waiting till the second Tuesday of August to release 14 more sets of updates, curing the most number of problems they've ever cured at once, which is at least 34 security holes, depending upon the way you count them.

There were problems, multiple problems in Windows Secure Channel system; in the XML Core Services, in their MPEG level 3, MP3 codecs; and a full update round for IE that fixed a bunch of things; their SMB service, which is the filesharing, file and printer sharing stuff. This old Cinepak codec actually had some problems. A problem with Office Word that could be exploited if you opened a maliciously crafted RTF, or Rich Text Format, email message. They had problems in their .NET common language runtime, the CLR, and their Silverlight, which is sort of their competitor to Adobe's Flash. Problems in the Windows kernel, kernel mode drivers. Movie Maker had a problem if you opened a malicious Movie Maker project file. And then, of course, Excel, if you had a malicious Excel file.

Even TCP/IP didn't get out from not having something. There was a problem that allowed an attacker to get root privileges if it was able to log onto your system over TCP/IP, a privilege escalation. And then something called Tracing Features for Services. I don't even know what that is, but that had some problems. So pretty much everything.

Leo: You know, it gives lie to the idea that, as time goes by, they might get - kind of have it locked down.

Steve: We've talked about this often; and, I mean, this is still the case. The problem is these systems are so complex, and they keep messing with it. They keep changing things and writing code. And the new stuff has...

Leo: Do you think they're introduce- so these are introducing - bugs that they've introduced.

Steve: Well, it's certainly a variety. For example, the big one of last week, the shell LNK exploit, we know that that probably goes back to NT.

Leo: Nothing new there.

Steve: So that's been there forever. But certainly they are doing new things. And then there are problems, well, I think we're going to be talking about it, there's an unpatched - no, that's in Adobe. There is, oh, yeah, there's a new zero-day flaw in the Windows

kernel that they introduced as a policy, that I will talk about here toward the end of our news. So it's just - it's a little bit of everything, unfortunately. But, I mean, I'm glad they're fixing these things.

I'm annoyed, though, that we know that, for example, XP SP2 has all these problems, which they're no longer fixing. So that's - but again, you have to, I mean, I understand that they can't forever be responsible for their really old OSes, and they want to move people forward. I'm probably going to experiment with SP3 again, although it bit me when I initially tried. The good news is I was able to just quickly remove it, and everything was okay. But it's disconcerting, for example, for me, to read that list of catastrophes and know that none of them are being fixed for me now, although they're very likely still present. I did my standard "oh, let's go see" Microsoft Update. And it said, oh, yeah, we got a couple things for Office. It's like, oh, okay, thanks a lot. I mean....

Leo: Awww.

Steve: I didn't get all the goodies.

Leo: Left him behind, aw.

Steve: Yeah, so...

Leo: Well, hey, I would never want to in any way imply that, because they're fixing them, there's something wrong. No, let's encourage everybody to step forward when there's a problem and fix it, so that's good. And you're right. You can't expect somebody to support everything forever. I just feel like there's so many old versions of Windows on the 'Net that - I'm not saying support people who aren't going to upgrade. But I'm saying, for the health of the 'Net, you might want to update.

Steve: Well, and still in use, especially this jump from SP2, which was a big one, I mean, I could completely forgive them not going back beyond that. But SP2, as we remember, was the big, if you'll pardon the phrase, "security update" for Windows that turned the firewall on by default, I mean, it was a major change to XP. In fact, it was where they disabled raw sockets because they realized that had been a mistake, as I had been trying to explain to them since XP first, since, well, before XP was first released. And so many things got fixed in SP2. And because then SP3 has problems that many people have experienced, there's like an install base of SP2 people who haven't moved yet to Vista or Windows 7. So I think that's - if I have a problem with SP3, I'll probably just bite the bullet and go to Windows 7. Sooner or later I'm going to have to because I can't stay back here. It's just not safe.

Leo: And some would say, well, that's Microsoft's commercial interest in not updating it. But I really think it's just also they feel like, well, we just can't keep putting money into this.

Steve: Yeah. And it's got to be tough to do all their aggression testing and make sure that they haven't broken other things. I mean, frankly, the pro side of this is it's amazing

to me that this hasn't all just completely collapsed, this whole incredible infrastructure of crappy code, that it just hasn't collapsed under its own weight.

Leo: It does feel like you're kind of pasting over holes in the Titanic, like...

Steve: It's holding your breath and pinching your nose.

Leo: Yeah, exactly. And I think that's probably what they're thinking is, well, look, we rewrote everything. We got Windows 7. We got Windows Vista. Come on, just, guys, we've fixed it all, come up here. Stop staying down there in the basement. But I just - look, Microsoft makes plenty of money. They can afford - oh, come on. They made, what was it, eight or nine billion dollars in the last three months. Take 100 million of that, a small percentage of that, and fund upgrades for old versions of Windows. Not because you're trying to support legacy users, but just because you're trying to protect the Internet as a whole.

Steve: Well, and that's really an interesting question, too, Leo. What's happened is we've gone from the notion of, gee, I'd like to spend more money to get the newer version of Windows. Somehow, without us sort of noticing when it happened, it became, oh my god, I'd better spend more money or I'm going to be hacked. I'm going to be in trouble. So now, I mean, here I'm under pressure to upgrade, although I'm completely happy with the OS that I purchased. But now I can't stay here because it's going to be soon unsafe.

Leo: Right. Well, you know, people call the radio show all the time saying, I'm running Windows 95 on a 386. And of course I would love to say, stop. Go out and buy a new computer. Come on, what are you, crazy? But you've got to respect the fact that people don't have unlimited funds. Maybe this computer worked fine, it works fine, it does what they want it to do. Who am I to say they should spend 500 bucks on a new computer if it works?

Steve: And besides, nothing infects them anymore, Leo. They've got different DNA.

Leo: Maybe they've bypassed...

Steve: The same viruses can't infect them anymore. None of this stuff we're talking about affects Windows 95.

Leo: Actually, you're better off on Windows 95 than you are on Windows XP, probably. All right.

Steve: If it does what you want. Well, and not to be forgotten, Adobe is of course in our weekly roundup of updates on both platforms. Flash Player has just had six critical memory corruption vulnerabilities fixed. And it did update itself on various systems. When I switch over them it says, oh, we've got a new version of Flash Player. So

everyone should make sure, if they're worried, that they're now at 10.1.82.76. That's the current release, jumping up from 10.1.53.64, which had these six critical memory corruption vulnerabilities which are now patched in the latest. So Flash Player got fixed.

And an unpatched new problem has been found in PDF format in both Adobe Reader and Acrobat, for which there is as yet no fix. It's publicly known. I haven't seen any proof of concept nor any exploit. But it turns out that there's a problem in the integer math font parsing code for TrueType. There's an overflow error which can be exploited to run arbitrary code. So I'm sure that Adobe is working on that.

And now this brings question to, like, what their update policy is going to be because they just did a Flash Player update on the second Tuesday because they're synchronizing with Microsoft. I assume now that they're in the - remember that they were going to be doing only quarterly second Tuesday of the months. Then they said, okay, well, that didn't even last one quarter. So now they're at monthly second Tuesday of the month to synchronize with Microsoft. So I presume that, unless something really bad happens within the next month, we'll be waiting a month for them to fix this problem which has now been found. But hopefully, if it becomes a real targeted exploit, they will agree to do an out-of-cycle update. So we'll kind of keep our eye on that and let our listeners know how that evolves.

There's been much conversation about this shell LNK vulnerability which is now really being exploited heavily in the wild, and the fact that it isn't, hasn't been patched for SP2, just as we were talking about. And a bunch of different postings on the 'Net have found ways around this. The very first ones were distasteful, sort of, I mean, I've been checking them out because of course I'm affected by this, as are, I know, many of our listeners because I've seen our mailbag.

The most interesting one is a little troubling. I don't - I'm not going to recommend this. And I don't have any experience with it yet because just this morning, as I was pulling things together for this podcast, I ran across the most recent news on this issue of what can you do for SP2. I did read, as I mentioned last week, a comment that people under Windows service agreements with Microsoft could get this patched for SP2. Now, it turns out that, if you look at the download which is available from Microsoft's site for SP3, in the version tab, if you right-click on the executable and look at its version information, it says in there that this is for Windows XP SP2 and Windows XP SP3. So it says it, that it runs on SP2. If you attempt to execute it, though, you get a little popup message box that says, oh, sorry, your current service pack level is not supported. You need Windows SP3.

Well, it turns out that there is a single registry value which can be changed from 200, which is to say, it turns out this registry key specifies what service pack you have installed. You can change it from 200 to 300, that is, to fool the installer into thinking you have SP3 installed. If you then reboot your system, after changing this key, then this patch installs. So that's been confirmed. But even better, it turns out that the Windows XP embedded version of the same fix will install without you having to play any games at all. And it, too, in its version tab says that it's compatible both with XP SP2 and SP3.

In order to take our listeners to that, first of all, if you just Google XP space embedded space and then the knowledge base number, which is KB2286198 - so you Google "XP embedded KB2286198," the first link that comes up is Microsoft's page offering you the Windows XP embedded version of the shell LNK fix. And its version tab says it runs under SP2 and 3, and it does. And so I think that's the cleanest way of fixing this. And I wouldn't be at all surprised if Microsoft knows all this, if this is sort of their way of letting people who are stuck on SP2 for any of a myriad of reasons, get themselves fixed.

I also created a little short, a SnipURL: snipurl.com/linkme. It'll just redirect you. It's much easier to type in: snipurl.com/linkme. That just bounces you directly to the same Microsoft page. You can download that directly from Microsoft, make no changes to anything. That one will install and fix the problem. And people who have done it have performed the tests of the vulnerability afterwards, and their system, their SP2 system is then no longer vulnerable. So, I mean, this is not officially sanctioned; but I'm going to give it a try. I'll report on how it worked out next week. My guess is it's probably completely safe, especially since the EXE itself does the testing, doesn't complain about there being a problem, and their version tab says it runs under SP2 and SP3.

Leo: Somebody in the chatroom actually asks a good question. How do you know if the fix has taken?

Steve: There are, floating around the 'Net, some tests for this. I got one from the original discoverer of this LNK vulnerability. I haven't tried it yet, and I'm going to have to go off on a secure system that's not on my network because, unfortunately, he named it "suckme.rar." And I'm a little reluctant to just jump on that...

Leo: Oh, these hackers.

Steve: ...with my - those funny hackers.

Leo: They've got such a sense of humor.

Steve: I'm just a little reluctant to just jump on that with my main system. So...

Leo: I don't blame you.

Steve: ...I'll find an experimental test system where I verify it safely, or maybe do it in a VM or something. So I haven't gotten to it, but I will report on all this next week.

Leo: The test is if all of a sudden your machine starts speaking Russian, you haven't fixed it.

Steve: Exactly.

Leo: Jawohl, comrade. Welcome.

Steve: Many of our listeners reported that PayPal is discontinuing the PayPal plug-in. Not a huge loss. I found it kind of funky to use.

Leo: This is that one-time, that would generate a one-time credit card number?

Steve: That's the best, yes, that was the best part of it was that you could get a virtual credit card. And in fact, Leo, I have to say it saved me recently because about a year ago, or maybe it was more, maybe it was two years ago that I was working on - I think it was two years ago. I was working on the DNS spoofability system. I wanted to get a wildcard SSL certificate, and I didn't want to pay a lot for it because I was sort of just - it was experimental. So I got it from GoDaddy. I think it was *.dns.grc.com or something. Because wildcard certificates are a lot more expensive, especially if you get them from VeriSign, where I do purchase the rest of my certificates. And that then came due a couple months ago for renewal.

Well, I didn't want to renew it. And I got a couple of emails from GoDaddy reminding me that it was coming up for renewal. I just ignored them. Then I got a complaint from them that the credit card that I had used to purchase the certificate two years before would not accept their charges for renewal. Well, of course I'm very glad that I used a virtual credit card from PayPal and that they didn't have my master, behind-the-scenes credit card because they were just going to charge me, without my permission or authorization, for a renewal of that certificate. I know you like GoDaddy a lot, but I was...

Leo: No. You're talking to the wrong person.

Steve: Oh.

Leo: Oh, no. Just one of many reasons I'm not a fan.

Steve: Oh, good. I'm glad to know that because I was...

Leo: Oh, gosh, no. We don't - we have an advertiser that we far prefer, Hover.com, over GoDaddy because they don't pull hijinks like this. In fact, I got a call the other day from Bob Parsons, who wanted to edumacate me on why GoDaddy is so good. I'm just not, I'm sorry, I know why GoDaddy is not good. I don't want to be edumacated, thank you.

Steve: Well, here's one more reason. When they were complaining they couldn't charge my credit card without my permission or authorization...

Leo: Yeah. Gee, sorry.

Steve: Thanks anyway.

Leo: Sorry.

Steve: In the news we've got two congressmen, Ed Markey, a Democrat from Massachusetts, and Joe Barton, a Republican in Texas, who have a history of working together on privacy-related things. They've just recently sent - the Wall Street Journal ran a series of stories on Internet privacy and, like, disclosure of personal information sort of stuff which concerned a number of people in Congress.

Leo: And it was really bogus because it was about tracking cookies and things we've known about for years.

Steve: Exactly, stuff we've covered well. But I guess what's happening is they're beginning to make some rumblings about thinking about some legislation. And I hope they do it wisely. Anyway, they sent 15 letters to major websites, including Microsoft, Yahoo!, Comcast, MSN, AOL, CareerBuilder, MySpace, and others. Hopefully Facebook, as well, although I didn't see them enumerated. And they were specifically asking how do they monetize the private information that they obtain from their visitors, and how much money do they make from doing that? I love that question because of course behind the money is the motivation.

So, and quoting from the letter, they said: "We are troubled by the findings in this report" - referring to the Wall Street Journal report - "which suggest that the price of consumers' unfettered use of the Internet increasingly is surrender of their personal information, preferences and intimate details to websites, data monitoring companies, marketers and other information-gathering firms that seek to track them online and develop digital dossiers for a range of purposes, including marketing. As Congress prepares to consider comprehensive privacy legislation, we request responses to the questions that follow to better understand your companies' practices in this area." And then of course Microsoft responds, oh, we're very willing to work with Congress and hope to do everything we can to shore up our users' privacy.

Leo: Actually, I'm a little concerned because Google has - was it the Journal? Somebody revealed a Google internal document in which they're starting to look at, how can we monetize all that stuff we know about people?

Steve: I heard it described as sort of a soul-searching document.

Leo: Yeah. And I'm glad they're searching their soul. I hope they do the right thing.

Steve: Yeah.

Leo: And maybe we can push them in that direction a little bit. I'll see if I can find that article. We'll certainly be talking about that on This Week in Google, which is right after this show.

Steve: RIM has decided to install three of their BlackBerry servers in Saudi Arabia, in order to give the Saudi government access to the textual content of instant messaging and email as it passes through BlackBerry devices in that country. So that's how that controversy settled out. Remember that they were officially going to shut down

BlackBerry access, I think it was on October 11. So that caught RIM's attention, and RIM decided to solve the problem by moving servers there. And apparently, Lebanon has already recently stated that it, too, plans to start talks with RIM in order to allow Lebanese security agencies to monitor communications conducted through the BlackBerry network. So that looks like that's going to be pretty much the way this is done. The BlackBerry technology itself is extremely robust. I've spent a little time poking around, looking at what they do in terms of their architecture.

Leo: I think that's the problem, because these repressive governments cannot read what's going on.

Steve: Exactly.

Leo: So they want access to the server.

Steve: Yup. And Germany has been making grumbling noises, too, so...

Leo: Oh, great. That's nice. Well, you can't trust those Canadians, you know. They could be reading all of our mail. Frankly, Canada to me is like Switzerland. I would rather things go through Canada than my national government.

Steve: Yeah, it's about the safest place, I think you're right, I could imagine it goes.

Leo: You can see why the Saudis and other countries prefer not.

Steve: Yeah. Firefox 4 is coming. We've had two betas so far. The third beta is due later this week. And one of the new features was blogged about recently that hit the news, which is that the Firefox guys have decided they're going to add the silent update feature, much as Google's Chrome browser has, to Firefox. Major versions won't happen. So, for example, a big jump from 4 to 4.5 or from 4 anything to 5, when that happens, that'll still be interactive and will not be done clandestinely. But periodic incremental fixes for problems, that they are going to do transparently. Unlike Chrome, there will be an option in the UI controls of Firefox to not have this be done transparent, to make it overt, clear, and interactive. But the default will be, don't bother me with this stuff, just keep the browser running right.

And I hope they do it better than they have in 3. I've noticed that I'll often, if I, like, manually check to see what version I'm on, when I'm seeing news about some important updates, it'll have, like, gotten stuck partway through downloading an update that it was trying to get ready to do. I don't know where the problem is. It might be that I've got about 80 tabs open, and so it's weighted down a little bit. So it could just be me. But it'd be good if that process is running. And I'm all for having this stuff just fixed. I think for the typical user it makes a lot of sense for a high-profile security target like a web browser to just be fixing itself all the time.

I mean, some people say, oh, well, that gives them too much control. How do I trust what they're doing? Well, we're running their software anyway. So you're inherently

trusting what they're doing if you're using their browser. How does manually clicking yes, okay, change anything? I guess the one downside is, if something broke with an update, you would not - you'd lose that causal connection. You wouldn't realize, oh, wait, that might - it's because I just did that update that something's now not working. If it happens transparently, then you don't know why something just broke, so there is that. But on balance I think having these things fixed, especially if it allows them to push out fixes more quickly if something bad happens. It's like the Firefox guys who were at the Black Hat and DefCon conferences, who said we'll be watching very closely and prepared to push out any update as soon as it happens.

Oh, and speaking of news from last week, I was talking about NoScript v2. And while we were recording last week someone in the chatroom said, oh, it's out, it's out. And it hadn't been that morning. We're now at 2.0.1. And I did update to it, and I wanted to confirm that under that Advanced tab, under the ABE, the application-level blocking, there is a new checkbox, which is checked by default, which does add the feature that we talked about which blocks the local DNS rebinding problem.

This version of Firefox goes out and finds your current IP address and then automatically adds that to a filter preventing a script running in the browser from using that IP address to access your router's WAN interface from the LAN side in order to prevent its having access to your router. So they added that in NoScript, which is really becoming a nice, an increasingly powerful addition to Firefox. It'd be nice to begin to see some of these things maybe actually migrate into the Firefox substrate instead of always being in NoScript.

So this is just really nice the way Robert Greenfield wrote this. He says, "Dear Mr. Gibson, et al," because he sent this through GRC's main email. "It is with utmost joy that I write to you today. I've been a systems consultant and software engineer for over 26 years, and co-authored and co-edited a book on cyber forensics with a professor from Webster University here in St. Louis, Missouri. As a contractor the past 15 years of my career, I've had the opportunity to consult with numerous firms about all manner of issues.

"One issue that is dear to my heart is, naturally, data recovery. Normally the tales of woe I have on lost data or other such issues are about other individuals and companies. But this time it is a true tale of my own that I must relate. I've been using SpinRite 6 for personal use as a preemptive measure on all my computer systems at home, and recommending your utility to everyone I consult with, as well.

"Last week, before leaving for a trip out of town to visit my parents in Colorado, a laptop in my house was dropped - not by me - and caused some damage to the hard disk inside. While the computer still booted up" - and he has in parens "(barely)" - "it would freeze up and had all sorts of issues doing anything at all. The drive wasn't making any bad noises, though. So I got my copy of SpinRite 6 out and booted the system off the CD ROM using the ISO image that was burned from the software. As expected, the drive showed a number of severely damaged and even unusable sectors with the software early on.

"While the time projection for completion was growing and growing, as SpinRite discovered more and more bad areas, I decided to leave the laptop on, running the software over the few days I would be out of town. Upon return I looked at the screen, and it showed that it had completed the analysis and repair. I used Level 2. The person who dropped the laptop was excited to know that they may not be ostracized completely for life after all, and wanted me to reboot it right away. I made her suffer a bit with angst as I reviewed all of SpinRite's logs and summary info before restarting (just to extract a few more beads of perspiration from the perpetrator) and then rebooted when enough

squirming had been done. Voila. The system booted right back up and worked flawlessly.

"Yes, the drive did suffer a head crash and will have to be replaced quite soon for the safety of the data and capacity. But the system works, and all the data was recovered. I was a true believer before anyway. But now I'm even more so. Perhaps there needs to be a cadre of SpinRite 6.0 evangelists just like Microsoft's various technology evangelists. If so, count me in. SpinRite has always been a tool that I have recommended, both for prophylactic use as well as restoration and repair. But this one incident struck home so deeply that I felt compelled to tell you.

"I've carried on a link on my website to yours for quite some time, and I can honestly say that I don't put links up there without careful thought and review. This incident has only enhanced my already firm conviction that your software is invaluable. Thanks for a fantastic product that truly saved the day. Robert Greenfield, system consultant, software engineer, Lindenberg Technologies, LLC."

Leo: Isn't that nice.

Steve: And he's www.lindenbergtech.com.

Leo: Very cool.

Steve: So a very, very nice testimonial. Thank you so much, Robert. You know, I forgot to talk to you about Maker Faire. Was it fun?

Leo: Oh. If you ever get a chance to go to a Maker Faire, yeah, it's really - it's what we were talking about with your portable dog killer. It's the spirit of creation. There were two boys there, maybe 11 years old, who'd built a marshmallow gun. And, I mean, there was a dad there who built an off-road little red wagon for his daughter, and she's riding along in it. This thing has suspension, it's about six feet off the ground. It's got, like, massive suspension on it. It was just - it's people who are inspired to make things, exactly as we were talking about. So if you ever get a chance to see a Maker Faire, they're going to New York in September.

Steve: Well, now, there is one in San Mateo, too; isn't there?

Leo: That's where it is every year, yeah.

Steve: Yeah, so there's no excuse for me not to.

Leo: You should come up. Visit Mom and Makers.

Steve: Yeah.

Leo: Yeah, it's really, really cool.

Steve: Very cool. Do you have footage on your trip there?

Leo: There is. There's a whole special just on the Maker Faire. So if you go to TWiT.tv/specials, the Maker Faire Special is there. And somebody was asking me about that my daughter Abby, before she left for college, was going to give a speech at a conference called Tomorrow's Web. The conference was called off literally the day before. And she very - I thought this was really cool. She said, "Well, dad, why don't we just bring the speakers to the studio and have them do their presentations for the audience?" So we did that, and it was amazing - a couple of hours with kids 17, 18, and 19, talking about what they saw as the future of the Internet. It was so inspiring. So we turned that into a TWiT Special, too. And that should be out, if it's not out already, that should be out any day now, a special version of her show, Abby's Road, her farewell edition. Although I encourage her to keep doing the show while she's at school. But we'll see. She's busy. Let us get to our Q&A. Are you ready, sir?

Steve: Absolutely. Let's go.

Leo: I've got a lot of questions for Mr. Gibson, starting with Glenn Edward in Nottingham, Maryland. He says, "Why can't PC OSes be top-down secure?" Dear Steve: In spite of Mr. Ballmer extolling how Windows is the most secure operating system ever, the recent LNK shell exploit was able to bypass easily user privilege limits. This implies that much of what Windows does isn't geared toward following security rules. Otherwise, how could any one system file that becomes compromised bypass any level of security established by the system?

I always assumed that UAC, User Accounts Control, came ahead of something that mostly displays icons and text on the screen. And one would think there would be a hierarchy of programming and user privilege within Windows, I mean, since Windows asks for username, password and permission before it does much else. But it also seems so shockingly stupid that a malformed icon, of all things, received from a browser or flash drive could trump all that security. I think we kind of mentioned that, too, in the show. Whatever programming it is that asks for one's password at the start should act as a sentry in preventing other programs that follow from affecting what takes place in higher privilege levels. Or even in the user-inaccessible root account.

But it's sounding more and more as if this isn't so with Windows, in spite of the 15 years' time Microsoft has had to perfect this. Is Linux any better constructed as far as following strict security protocols? Is any other UNIX-based PC operating software? How about Mac OS? Am I expecting too much? Glenn Edward, Nottingham, Maryland. We mentioned that, that this user privilege escalation seemed like a flaw, a big flaw.

Steve: Well, yes. But I liked Glenn's question because it sort of said, what's wrong with, like, the whole system? More like from a holistic standpoint. Isn't there a hierarchy of some sort? Isn't there, I mean, how can it be that something like this can create such a

breach in the system? And then he talks about how we've had 15 years. But really, when you think about it, Leo, one of the things - and maybe you've had this experience. I've noticed, when I've had occasion to use a very old system, I mean, like, 10 years old, like Windows 2000 or almost even NT, it's surprisingly familiar. I mean, there really hasn't been that much change.

Leo: No.

Steve: There's been window dressing. And with XP we got kind of Candy Land user interface, and more so with Vista. It's like, okay, how can we get people to upgrade? But the fundamental architecture of Windows hasn't changed during all this time. And the truth is that, while there is sort of some lip service paid to security in the architecture of Windows, all there really was originally was this concept of logging on. That's all there was. In 95 and 98, which really the rest of Windows is directly descended from, all you sort of had was identifying yourself to the computer so that multiple users could share a computer. And since multiple users typically didn't, there really wasn't even that much attention paid to that.

Now, in fairness, with the NT file system and privileges, there was more ability to protect things. But it's never really been leveraged in Windows. So what Glenn is sort of asking, and I'm sort of, I guess, refining from my perspective, is this isn't a secure operating system. I mean, it never has been. And we've seen the pain that Microsoft has gone through to, well, as they have tried to add features. The problem is, adding security features is very difficult when you're starting from an operating system that doesn't have them because this huge base of software has been written to assume there's no security. That is, the software assumes it can go put files wherever it wants to.

I mean, even benignly, not malicious software, just good stuff says, oh, I'm going to put some stuff in the registry here, and I'm going to put some stuff over in the temp folder, and I'm going to stuff some stuff in the Windows System32 folder, blah blah blah. I mean, doing that, if software was all written perfectly and was all deliberately benign, we'd be fine. But the fact is we know it's incredibly difficult and incredibly expensive to write software perfectly. And we also know that there's lots of, not only mistakenly insecure software, but deliberately malicious software, all that can leverage the fact that Windows really never, never has been a secure operating system.

So when he asks about UNIX-based stuff and about Mac OS and even, for example, Linux, I would say that in general those systems are more secure because they have a different heritage. They have a heritage that's more a non- sort of UI-based operating system, more of a command console-based system that then a graphical user interface was put on top of. And they were always more developed with security in mind than Windows was, that basically just had a logon password was all the security Windows had. Everything else has come along afterwards with Windows. And you just can't do that much without breaking so much software. I mean, Microsoft would probably now love to crank up the security, after the fact. But unfortunately it's too late.

Leo: That's where Apple had an advantage because they just cut off people. They said, sorry. It wasn't a big enough install base. They could just say, if you're using OS 9, bye bye. And they needed to because OS 9 was ghastly.

Steve: Yeah. And Apple has done little bridging things, like where they had emulators to

cross you over for a while. And then they say, okay, we're not doing that anymore.

Leo: How long is an OS good for? I mean, it seems like after 10 years things change so much that you really should start from scratch. I don't know. Maybe you can't make a rule of thumb.

Steve: Well, one of the nice arguments is that we're seeing that now in the mobile industry. That is, that the new OSes are not these big desktop platform OSes, but they're the handheld OSes. There's an opportunity, for example, when Google creates Android - and it's going to have its own problems. Connectivity is a fertile medium for malicious conduct. But, for example, Android, and to some degree the iPhone OS, well, I think to the same degree, they had this notion of sandboxing applications from the beginning. There was never a concept of sandboxing applications in Windows. And we know that to try to do so after the fact creates an incredible number of problems. So the newer platforms I think are in the newer application spaces. And we're pretty much stuck where we are, for example, with Windows.

Leo: Yeah. Sad to say. Question 2, Scott Finneran in Blue Mountains, Australia - how cool - noted that cars can be hacked through their wireless tire sensors. This story just crossed a couple of days ago.

Steve: Yup.

Leo: And it ties into what we were talking about with security flaws in car software. Steve, as an embedded software engineer in a different industry, I've enjoyed your recent Security Now! discussions about security issues in auto electronics. You've probably seen this already, but another attack vector has been proven exploitable. And he quotes an Ars Technica article that was just a couple of days ago, "Cars Hacked Through Wireless Tire Sensors." What's the story?

Steve: Well, just I saw this, and a number of our listeners picked up on it and sent me links. So I just picked this one from Scott just because I had to choose one. So it turns out that, as of 2008, I don't remember what month in 2008, but sometime in 2008 it was mandated by law that all cars that were produced from 2008 on had to include tire pressure sensors which fed in real-time - or near real-time, apparently it's every minute to 90 seconds - every tire on the car...

Leo: I have that on my car.

Steve: Yes, is sending information to the so-called ECUs, the Electronic Control Units, about the state of their tire pressure, their current inflation pressure. So if you think about it, it's an interesting problem because the tires obviously are spinning around, so they can't use wires or they'd get tangled up around the axle, like, immediately.

Leo: Yeah. Sort of a short-term solution there.

Steve: And you might think, well, you don't want to use, like, commutator strips or something, like a DC motor has. So they use RF. They use radio. There's a little radio transmitter and receiver that goes between the tire and hopefully not very far away the unmoving hub that is near the tire. Well, it turns out that these sensors, these transmitters, have a 32-bit ID, so not many bits, and no encryption of any kind. So they're fundamentally insecure. You can receive the signal from the tires up to 40 meters away, so 120 feet. And that allows you, of course, to track people by their tire sensors, which are sending out a little blip with this ID every 60 to 90 seconds.

And unfortunately, it turns out, what some researchers at Rutgers and the University of South Carolina, they got together, and it turns out you can also spoof the tire sensors because there's no crypto. They have a simple, short protocol. Obviously you don't want to put much money in these things that are spinning around in your tires. And they have been able to completely fool the instrumentation in the car, creating all kinds of weird dashboard confusion that is bad, to crash the ECUs, and in fact even damage them to the point where rebooting them doesn't bring them back to life. They have to be replaced.

Leo: Oh, my goodness.

Steve: Ars Technica talked about it, but I found some other information, and I'll just read from this. It said, "The researchers had found that each sensor has a unique 32-bit ID, and that communication between the tag and the control unit was unencrypted, meaning it could be intercepted by third parties from as far away as 40 meters. 'If the sensor IDs were captured at roadside tracking points and stored in databases, third parties could infer or prove that the driver has visited potentially sensitive locations such as medical clinics, political meetings, or nightclubs,' the researchers write, in a paper that accompanies the presentation." They're giving a presentation this week at the USENIX Conference.

"Such messages could also be forged. An attacker could flood the control unit with low pressure readings that would repeatedly set off the warning light [in the instrumentation], causing the driver to lose confidence in the sensor readings, the researchers contend. An attacker could also send nonsensical messages to the control unit, confusing or possibly even breaking the unit. 'We have observed that it was possible to convince the TPMS [the Tire Pressure Measurement System] control unit to display readings that were clearly impossible,' the researchers write. In one case, the researchers had confounded the control unit so badly that it could no longer operate properly, even after rebooting, and had to be replaced by the dealer.

Leo: Wow.

Steve: So, anyway, just another example of the problems that are available for exploitation.

Leo: Yeah. Nathan Jackson, Cincinnati, Ohio, with a note about TrueCrypt System Encryption: Steve and Leo, I just thought I'd let you know that currently TrueCrypt System Encryption will cause a Blue Screen of Death when the computer hibernates if the disk controller driver you're using is non-Microsoft, for instance an AMD or Intel controller. Just thought the other listeners should know that prior to performing

the encryption process. They must have fixed that by now.

Steve: Well, I looked around, and I was unable to find any corroboration one way or the other. I wanted to just share it with our listeners in case they ran into something like this. The good news is, I mean, it's not catastrophic to anything if your system blue screens when you're hibernating. I mean, you'd rather not because it means you need to reboot and start over again. But I just, as I was running across this, I thought, well, if that's the case, we ought to let people know. So I wanted to just pass it along.

Leo: Unconfirmed, but something to pay attention to. And they're very good about updating TrueCrypt.

Steve: Yeah. The problem, of course, is that it's very difficult to do what they're doing. And that's the other thing. We mentioned that with Windows 7, with the new version of TrueCrypt, they are for the first time using the hooks that Microsoft built in for handling encryption of the hibernation file. But otherwise it's very tricky.

So, I mean, I tend to believe that there could be a problem like this, and it may be something that they know about. I just wanted to suggest to our listeners, if they needed this, for example [audio dropout] the controller drivers [audio dropout] the Microsoft native driver, and then be able to get this functionality to work if it was going to still be a problem.

Leo: Question 4, and I hope I'm saying your name right, Jeroen van den Berg in Gouda, Netherlands wonders how to check if his router is vulnerable to this DNS rebinding attack we talked about last week. Wondering how I could check. My understanding is, it's pretty simple. You check your WAN IP via whatsmyip.com, use that IP in your browser. If your router's web interface shows up, your router is vulnerable. Is that the test?

Steve: Well, I loved his question because it gives me an opportunity to say something that I should have said. Actually, I briefly said it, but I didn't highlight it nearly strongly enough last week, which is the whole rebinding thing, the whole problem, allows script running in your browser to get a connection to your router. But absent any other major security flaws from that interface, the only thing it can do is log in, if you have left your router username and password set to their defaults. The good news is that the DD-WRT router, when you install it, the first thing it asks you to do, it makes you change your username and password.

Leo: And some commercial routers now do that, too, I think. So, which is very good.

Steve: Which is really good. So I did want to - I wanted just to make sure people understood that, yes, you really - you don't want your router to be accessible. I would also say, as always, and this is standard advice, is disable Universal Plug and Play support for your router because that's another glaring vulnerability that this kind of exploit will probably tomorrow be used for because, if you've got script running in your browser, and it's got socket-level access, as for example Java gives it, and Flash does,

then Universal Plug and Play is another way for your router to get reconfigured without there being any user interface. But definitely change your username and password so that it's not the default.

What happens is, when the script brings up the page, it can look at the page and obtain all the information it needs to, to know what the username and password is because the page often contains the manufacturer's make and model and ID and other stuff in the page that you receive, and so it can then look up the default username and password for that make and model of router and log in.

The other thing I wanted to mention was that there was a mention here in this question of whatsmyip.com. And I went there because I wanted to see whether they supported SSL connections. It's crucial that an IP-displaying site be able to do that over SSL, or you very often get the wrong IP, which unfortunately many of these simple sites don't recognize. The bad news is, whatsmyip.com is gone. It expired in February.

Leo: Yeah, I just went there and it's a holding site.

Steve: Yes. And so I thought, well, what about .net? Well, whatsmyip.net does exist. And it's okay. But it does not support SSL. And whatsmyip.org exists, but you have to turn scripting on in order for that to work. So the one I like the most - and I'm thinking I ought to just do one because, I mean, it's a few hours of work, and it could just be GRC.com/ip or something, and everyone would be able to trust, and I would do it over SSL, and I would make sure it was over SSL and so forth. But the one that I like is the one which NoScript v2 is using, and it's what it's silently using in the background in order to get your WAN IP. And we talked about that URL last week. But unfortunately it's spelled funny and hard to get to.

So I created, as I like to, a SnipURL. So snipurl.com/whatsmyip. And that would redirect you to a secure URL, even if it's not. That is, you don't have to put in snipurl.com over SSL, just regular, put it in your browser, snipurl.com/whatsmyip, and that will redirect you to, over an SSL connection, to this IP Echo page, which simply shows it in simple little text string on your page.

Leo: I guess he in his email might have had a typo because there is, and the people in the chatroom are telling me there is a site, whatismyip.com.

Steve: Okay.

Leo: And that does seem to work. Although I don't know if it's HTTPS. I like yours better because it is secure.

Steve: Yes, and the reason that's important - I should just finish up. People may wonder why it makes a difference, is that the reason my own ShieldsUP site establishes an SSL connection initially is that I want to get the person's real IP. Many cable providers will have a transparent proxy in line so that their customers' web access goes non-SSL web access, goes through a transparent proxy, which then reissues the requests for all of their web material. It's a caching proxy which is used by the ISP to minimize the amount of bandwidth that the ISP uses upstream, and to improve the performance of their own

customers' Internet use.

So, for example, if Google's logo is not changed, then the first person to go to Google will have that logo cached locally in the ISP's caching proxy. And then any other customers of the ISP will just fetch it from the cache. So it's much quicker for the customers, and it minimizes the ISP's use of upstream bandwidth. The problem is that a server sees the IP of the proxy, not the IP of the user. So if you're using any of these IP reporting services that are not over SSL, you have no guarantee that you're not being told that your IP is the proxy IP.

Leo: Makes sense.

Steve: Yeah.

Leo: Get a long one here. I'm going to try to synopsize a little bit because we're running out of time. Rick Huebner in Melbourne, Florida talks a little bit about something we talked about on This Week in Google last week that was the exploit that came out of Russia. It was a wallpaper that had a trojan in it. And as soon as the wallpaper software ran, it would send your contact list out, and all sorts of bad things would happen. We mentioned on TWiG that there is a warning you get when you first install software about what resources the software needs.

Rick says: My problem with the Android install warning screen telling you what resources the application is going to use is that you have no option. So all you can say is yes or no. He says: I wonder why it couldn't be modified to place checkboxes by the resources the application is requesting so I could uncheck them. We also suggested, and he agreed that it was a good idea, that maybe a firewall that would sit on Android and say, hey, this application is asking for this, this application is asking for this, just as Windows does, and then request permission to do so. That does seem like a good idea.

Finally, in a previous episode you were talking about the loss of the 5-dot IP space in the current global IP crunch. You mentioned that Hamachi, owned by LogMeIn now, uses 5-dot. When the subject changed, you never finished the thought. Tell me that ICANN didn't assign the 5-dot addresses as routable? All my familiar members are required to have Hamachi and VNC to request any support from me - I like that - unless they want to FedEx their computer to me. Eagerly waiting for the next Security Now! and, more importantly, CryptoLink. Rick Huebner. So, yeah, I remember we started that conversation. What did happen to 5-dot?

Steve: Okay. It is on the chopping block.

Leo: Oh, boy.

Steve: There was a really interesting RFC, the so-called Request For Comment. The document is 3330. So if you just - if you put into Google RFC 3330, that's the formal spec for what regions of the IPv4 space are reserved. And it makes interesting reading because there's a lot of different little gotchas here and there. Especially people who consider themselves Internet gurus I think will get a kick out of looking at it and going,

hey, I didn't know that was reserved for that, or that's reserved for something else. So it's a neat little document. And there's no sign there of the 5-dot, which is absolutely reallocatable. So LogMeIn will probably have to move Hamachi somewhere else. There are some other networks that they could use that aren't quite as clean as the 5-dot. But ultimately it's probably going to get given to somebody. And that would be a problem.

Relative to Android and security permissions, I think I see a problem, which is we're trying to appeal to a very wide range of users.

Leo: Right, right. It's a phone, after all.

Steve: Yes. And, I mean, the fact is, people, as Rick suggests, they do just click on "okay." That's what people do. I'm sure that, if in the license agreement of any of this software it said, "and we're going to steal all your personal information and send it back to Russia..."

Leo: By the way.

Steve: ...people would say okay, fine.

Leo: Yeah, yeah. Yeah, yeah.

Steve: Because no one's going to read that stuff.

Leo: Whatever.

Steve: I mean, they don't.

Leo: No.

Steve: Now, what I would love to see would be - and, I mean, for example, BlackBerry applications do something similar, where they come up, and you get a screen of the application wants the following access to your stuff. And you just sort of, like, okay, fine. I mean, the problem is, even if someone does care, what you really need is: This is what we want; this is why we want it; and, if you turn it off, this will be the consequence to you. So most people are just going to say fine, whatever. But it would be nice for a sophisticated user to have the availability of making informed decisions. But as you said, Leo, summed it up beautifully: It's a phone. Unfortunately, it's also becoming a computer.

Leo: Jack Daniel, who's the guy with the beard at Astaro - well, there you go - wrote: Subject: HacKid Conference. Hey, Steve. I think someone from Astaro may have tweeted this at you. But please check out HacKid.org. I think it's probably Hack

ID, right, not HacKid?

Steve: Oh, it's HacKid, actually.

Leo: It is HacKid, okay, HacKid.org. I think you'll like the idea. HacKid is a hacker/maker conference for kids and their parents covering topics from introductory programming to safety - online and physical - to soldering, and much more. If you like the idea and feel it's appropriate, we'd really appreciate a plug for HacKid on Security Now!. Well, you just got it. From the site: "Kids are our future. Why not give them that spark that will set them on a journey that only 'hacking' can inspire? HacKid was created to educate, stimulate and develop children 5-17 and adults in a variety of educational areas in order to raise awareness and understanding of technology, mathematics and engineering and the impact on society and culture." It's a 501.3c non-profit. Thanks, Jack Daniel. He says he's on the advisory board and helping with planning and running the first event. Hey, that's cool. HacKid.org if you want to get involved.

Steve: It looks really neat. I went to the site, browsed around for a while. It's, I think, affordable. It's $50 per person. They have a bunch of topics that really look interesting. And I got a big kick out of his "Jack Daniel, the guy with the beard" because, if you remember, the first time I saw the Astaro booth was when I was up at the RSA Conference a couple years ago. And I made a point of going over to the Astaro booth. And I remember describing to you, Leo, I said, "Hey, they look like real UNIX guys. There was even a guy with a whole beard."

Leo: Well, that's the guy with the whole beard. This is really neat. There's one coming in Boston, October 9th and 10th.

Steve: Yes, that's the first one.

Leo: Yeah. Well, this is great.

Steve: And then I think in Washington, D.C., I think, is one that they haven't yet scheduled, but they're aiming at that. So I just thought, I know our listeners. I know how many people reacted to the portable dog killer story, just in terms of the feedback I received, who had young kids who

went out in the garage and started taking their old toys apart to try to hack something out of it. And so I wouldn't be at all surprised if our listener base has a bunch of parents who could really get some benefit from this. So I wanted to share the news. And this is not - this is Astaro being involved in this in a non-profit fashion. He's on the advisory board. And it looks like it's a hacker/maker conference for kids.

Leo: I love that. Five to 17, I love that.

Steve: Really, really topically oriented to that age range, which I think is terrific.

Leo: HacKid.org. They have a wiki, and they have a page that describes it. They have an event scheduled for Boston, one coming up in D.C., and they're looking for people who'd like to sponsor similar events elsewhere in the U.S. And I think a hacker space is a great place to do this. So if you've got a hacker space, I know there's some wonderful hacker spaces all over the country, this would be a great thing to do there. I'm doing an event kind of like this, well, more about keeping kids safe, but that's part of this, in November. Maybe we could make it a HacKid. That would be so much fun. Really neat idea. They talk about online safety, how to deal with cyber bullies, physical security, gaming competitions, interactive robot building, how the Internet works, food hacking...

Steve: Food hacking I love. It's like, okay.

Leo: Yeah. Well, Steve, I'm sorry we didn't get to all the questions. But we are out of time. That's my fault. I will endeavor to start on time next time. I apologize. But I'm sure there are many, many, many, many, many questions we could be answering.

Steve: We won't be running out any time soon.

Leo: No. And you can always go to GRC.com/feedback to ask your question for our next session, two weeks hence. What are we going to talk about next week, do you know? Is it a surprise?

Steve: I've got so many things cued up, I haven't picked one yet. But I know it'll be a good one.

Leo: We'll know it when we hear it. We do this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1800 UTC at live.twit.tv. So I do invite you to join us for the live broadcast. Join us in the chatroom at IRC.twit.tv. It's always a great place for feedback. And of course if you go to GRC.com, Steve's site, you'll find 16KB versions of the show, full transcriptions (which are really useful to have) and all the show notes; plus all of Steve's great stuff including SpinRite, the world's best hard drive maintenance utility and a must-have. GRC.com. Thank you, Steve. We'll see you next week...

Steve: Thanks, Leo.

Leo: ...on Security Now!.