Listener Feedback #120

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-306.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-306-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 306, recorded June 22, 2011: Your questions, Steve's answers, #120.

It's time for Security Now!, the show that covers your security and privacy online with our good friend, one of my oldest friends, Steve Gibson. He's not that old, but he's one of my...

Steve Gibson: Oldest in several senses of the word.

Leo: I've known Steve for a long time. We first met each other when he was doing his early security research on spyware. Actually it was the "Click of Death," wasn't it, for...

Steve: Yeah.

Leo: ...ZIP drives, way back when, on The Screensavers.

Steve: Right. SpinRite 5, I think it was, was the first version which supported anything that you hooked onto your machine. And people were hooking their Iomega ZIP drives to it and reporting that it fixed this notorious problem. Well, it turns out that it wasn't something that SpinRite could fix. It was an electromechanical problem with the drive. So I thought, well, okay, they're not going to be having good luck with SpinRite. So I quickly created a piece of freeware called TIP, Trouble in Paradise.

Leo: Trouble in Paradise. I remember that so well.

Steve: And that's when I first came up to the studio in South San Francisco, and you and I sat down and reminisced.

Leo: More than 10 years ago.

Steve: Yeah.

Leo: And we started doing this show, let's see, five, almost six years, well, we're in our sixth year now. So didn't waste time getting a show on with you. After the TV show went away, we started doing Security Now!.

Steve: I was No. 2 after This Week in Tech on Sundays.

Leo: You were. That's right. That's exactly right. Today we have a Q&A episode. That means our 120th Q&A episode.

Steve: I know. And there is, I mean, this was an insane week. I mean, we know that we had a major screw-up by Dropbox. And Bitcoin had all kinds of things happening. CNET has published an amazing spreadsheet of recent attacks and breaches. They've had to start creating a database of them because there are so many.

Leo: Wow.

Steve: And you had a great story on GigaOM, which...

Leo: Yeah, we could talk about that. That was a very nice story.

Steve: Yeah. But we've got updates and news and attacks and breaches galore. And there's so much that I thought, well, I want to squeeze in a couple questions. So I found three that I liked, just quickly. And one, the final one, is one that we can - that sort of is open for discussion. So we've got a great podcast full of news and updates on what's been going on.

Leo: Wow, I love that. It's actually something we started adding to the podcast after about 150 episodes. We said, we should really cover also breaches. Maybe not even that long. Maybe longer ago. All right, Steve Gibson. Let's get some news, some security news.

Steve: So the Mozilla gang surprised everybody by releasing Firefox ahead of schedule.

Leo: Wait a minute. I just installed 4. You mean...

Steve: I know.

Leo: ...I'm behind?

Steve: And you know me. I have not yet installed 4. I'm at, what, 3.6.17, I think is the most recent in the 3.6 train. And we talked about before that Mozilla is going to be working to move people off of their earlier v3 Firefoxes, although 3.6 is still safe to stay on for a while. So they're deliberately, they've made a deliberate effort, that is, the Mozilla people, to get Firefoxes out more often. And one might wonder maybe if they've overachieved in this instance.

Leo: Overachievers. Those darn overachievers.

Steve: So, I mean, yeah, 4 just happened. Now we already have 5. So a major, ahead of the first decimal point release in a very short time. They said they were going to do it by the end of the month, and it went live yesterday, from when we're recording this, on Tuesday, June 21.

Leo: It happened right during our TNT show, I think. Tom noticed and said, whoa. Whoa.

Steve: So five remote code exploits were fixed that existed in 4. And I did have, I have an instance of 4 around, so that I'm able to look at it and play with it and see how it behaves and so forth. And I noticed it's prompting me to move to 5. So it's like, oh, okay. Somewhere I saw something random, so I haven't verified this, but something said that 4 was not going to be upgraded.

Leo: What?

Steve: That is, and I think they were at 4.0.1 is the last thing I saw. But they're just instead going to move everyone to 5. So five remote code exploits, among them multiple WebGL crashes. And we'll be talking about WebGL in a second here because Microsoft apparently agrees with me in their security feelings about it. I did notice that they moved the DNT, the Do Not Track option, to the top. It's the first entry on the privacy tab, which I congratulate them for. I think that's great.

And LastPass does need to be updated. I think it's just that the LastPass client that runs in Mozilla sees that you're running on 5 and says, oh, I'm not sure I'm compatible with that. So what I got a kick out of was that in the change list for LastPass for the update, it says it'll work with versions 5, 6, and 7 of Firefox. So I think this time they're planning ahead.

Leo: They're ready for the future.

Steve: Because that might happen next week.

Leo: Yeah.

Steve: Who knows?

Leo: Wow.

Steve: So, yeah. And when I looked at 5, it said that the only thing I'm using that was not known to be compatible was I'm running the HTML Validator, which I really like. It puts a little red "X" down in the corner of my status bar, and it just helps me with my own web page design stuff. If there's something that comes up, I go, whoa, what did I forget? And so it's handy to have that. And so I wouldn't - and I wouldn't want to have it anyway, so...

Leo: So I'm on 4.0.1, and I just - it said "applying update." So will it automatically just take me to 5 now? Is that...

Steve: Well, it ought to give you - Mozilla's policy, and we discussed this a couple weeks ago, is they will not push people to a major version update without their knowledge. But they are modifying their policy to be a little more in line with what Chrome is doing, so that they'll, like, move people along and just sort of keep you updated more automagically. But major version updates you do get a say-so in, which is a good thing. So, and when I did it, oh, I know, I went, under 4, go Help > About, and I think that's where I saw the Update button. And when I pressed it, then it popped up a box that said, oh, let's go to 5. And oh, by the way, here. And I said Okay, and I clicked Next. And then it said, oops, here's the one thing you've got installed, an add-in that is not compatible with 5 yet.

Leo: It moved me to 5.

Steve: Yo.

Leo: So that's interesting.

Steve: Welcome to Version 5.

Leo: Wow. You know, I wonder, are we seeing some inflation because of Chrome? Because Chrome, you know, is at 12 now. And I wonder if they just - it's version

inflation.

Steve: Oh, wouldn't that be annoying?

Leo: Yeah, I hope that's not the case. But we've seen it happen before.

Steve: Yeah, you're right. It does sound familiar. It's like, oh, well, wait, you're on 6. You're on v6. You must be ahead of them. It's like, or no, your security's so bad that you have to keep counting faster.

Leo: It does say your Flash Player is out of date. Never fear, we can help.

Steve: Oh, speaking of which, Adobe has been driving me absolutely nuts. Every machine I turn on, oh, wait a minute, stop, we've got updates for Flash, we've got updates for Reader, we've got updates for Acrobat. And it's like, oh, my goodness. And of course those all require you shut down all your browsers, and often you have to reboot. So I'm sure all of our listeners who are using Adobe stuff still - actually I'm seriously looking at moving away from Acrobat. I use Acrobat to create PDFs still.

Leo: Oh, there's so many better programs, I think.

Steve: Yeah. I'm going to go find one because this is just crazy.

Leo: Try, yeah, my favorite's Foxit right now. I use Foxit Phantom.

Steve: Okay. Foxit, I will go there.

Leo: Yeah, give them a try. They have a free trial. You have to buy the program, but I like it a lot. And I'm sure our chatroom will have some other suggestions.

Steve: Well, but I also - I've bought many instances of Acrobat because there it's one use per license, and they track them all. And so it's so annoying because I'm like, I'll set up a new machine, and it's like, oh, I'm out of Acrobat licenses. So I've got to go somewhere else and remove it from something that I'm not really using in order to free one up, and then put it in over here. So it's like, okay, this is - they've lost me finally. I'm a brand guy, but not anymore. This is crazy.

Leo: Others are saying Sumatra.

Steve: Sumatra.

Leo: I haven't seen Sumatra. But it's a reader. You use - you're saying you're using...

Steve: Oh, no, I want a PDF...

Leo: You're using Distiller. You're using the whole thing.

Steve: Yep, I'm using the whole thing. And Distiller pops up and does a great job. In fact, I've got some PDFs from hell that I'll see if Foxit is able to...

Leo: That's a good test, isn't it.

Steve: Yeah. So just keeping track of, speaking of updates and upgrades, of Windows XP, just to give a support countdown, I would like to let everyone know, and I'm glad because I'm still sitting in front of XP, we still have 1,020 days left of official support from Microsoft on Windows XP.

Leo: Whew. But it's SP3 only.

Steve: Yes, SP3 only.

Leo: Yeah. So actually that's - I was going to ask you this because somebody called on the radio show and was reinstalling XP. Presumably, if you install XP early version, non-service pack version, they will let you get SP3, and then they will continue to support from that point on; right?

Steve: Oh, absolutely. And that's been their policy, for example, we can check it by looking at Windows 2000, and that's definitely the case that you're able to get Service Pack - where did they leave off, 4 or 5 on Windows 2000. So, yeah. Okay. So Microsoft, I got a bunch of tweets from people following me on Twitter saying, well, Steve, Microsoft agrees with you about WebGL. On their TechNet blog, they posted a blog titled "WebGL Considered Harmful." And they said, "Our analysis has led us to conclude that Microsoft products supporting WebGL would have difficulty passing Microsoft's Security Development Lifecycle requirements. Some key concerns include: Browser support for WebGL directly exposes hardware functionality to the web in a way that we consider to be overly permissive."

Leo: Oh. That's kind of ironic coming from the creators of ActiveX.

Steve: I know, I know.

Leo: There's a little irony there.

Steve: Well, and we've got one, we'll be talking about another irony here because they're now running around boasting about how autorun malware has finally been tamed. And it's like, wait a minute, whoa, okay, we're getting ahead of ourselves. So, secondly they said...

Leo: Save it, save it.

Steve: About WebGL they said, "Browser support for WebGL security servicing responsibility relies too heavily on third parties to secure the web experience."

Leo: Oh, that's interesting.

Steve: Meaning that the graphics device drivers end up, by nature of the way the WebGL architecture is, they end up with responsibility that there's no way for Microsoft to police. And finally they said, "Problematic system denial of service scenarios." So to remind our listeners, the problem with WebGL is that the nature of the way it works is you visit a website which literally downloads graphics-rendering code into your system's GPU, into your Graphics Processing Unit, and runs it. And this is native GPO machine language, essentially, which the site provides to your machine when you visit.

Well, I mean, this sounds like anyone's horror story. It's not clear that you can break out of the GPU, although that's of course the concern. So there's a denial of service scenario where you could go to a site that just deliberately puts in an infinite loop into your GPU and essentially crashes your entire system. I mean, it locks it up, and nothing works, and you can imagine some script kiddies having fun doing that for a while. It's not clear that it breaks out into, you know, outside of the graphics containment. But this does pass down through the device driver.

And Microsoft, to their credit, is saying, eh, you know, we're going to keep it out of IE for a while until we see whether there's any way to implement this in a safer fashion. And there are groups working on being able to offer the benefit without this. So this feels like first-generation, oh, let's just get it done. Go to a website, and we're going to download native code into your machine. It's like, oh, okay, that's - why would that not raise some suspicion? So it certainly has.

There was a bunch of news about a new trojan that Symantec was the first to discover. They found it in the wild last Thursday, and they dubbed it Infostealer.Coinbit, which is...

Leo: Uh-oh.

Steve: ...the words flipped from Bitcoin.

Leo: Uh-oh.

Steve: And it literally, well, it gets into your machine and makes a beeline for where your Bitcoin wallet is stored by default.

Leo: It's wallet.dat; right?

Steve: Exactly. If it finds it, it sends your wallet to an attacker via a server located in Poland. Now, and this sent shockwaves through the security community. And a lot of users are like, oh, my god, you know. So bitcoins are not safe. Well, okay. You've got something bad in your machine, so that's a problem. But it is absolutely the case, and any Bitcoin user has to know this because this is rubbed in your face when you start using Bitcoin, the designer of Bitcoin understood this and made it very clear that the entire security of your wallet is your responsibility. That is, this is virtual currency. You have nothing to prove your ownership of bitcoins other than this data that's in your wallet. I mean, it is your money. And so if your hard drive...

Leo: Just like cash would be, really.

Steve: Yes, exactly. If your hard drive crashes, which unfortunately, well, except maybe for people who sell recovery software...

Leo: Who would that be? Who would do that?

Steve: If your hard drive crashes, and you don't have that file backed up, that money is gone. There is no way, and they make it very clear, absolutely no way to prove that you ever had that money. So first rule is back that file up. I mean, have it somewhere safe. The problem is, if it gets loose, which is a different problem, if it gets loose out of your control, shipped off to Poland, then whoever has that file also has your money. And the way the system works, you can't - and, I mean, this is why it's so clever, and we discussed this in detail in our podcast we devoted to how Bitcoin works, there is no way to duplicate bitcoins. So the first person to transact those bitcoins renders the copy of the bitcoins, even if it's the original copy, it renders them invalid.

Now, wallets can be strongly encrypted, but that depends upon the strength of the password. So everybody listening to this that has any investment in bitcoins, if you didn't create a password, a strong password for your wallet, you absolutely want to do so because, if you have encrypted your wallet, and it's gone off to Poland, then the only thing the person can do at the other end is to try to crack the password. And we know all about how that works. And if it uses a weak password, it's much more likely to be crackable. So...

Leo: Encryption is not built into Bitcoin. You would use something external.

Steve: Oh, no, no. It's part of the client. You're able, yeah, it's able to encrypt the wallet for you, and you provide it with the passphrase that you want to use for that encryption.

Leo: And that would be secure even though they got your wallet.dat.

Steve: Exactly. That would be secure because that's not part of - it's something that you enter in order to open your wallet so the client can have access to it. So absolutely use a strong password is the first takeaway. The second is, back up your file because, even if somebody else can't get it, if you can't either, that's a problem.

Leo: If you delete it, you threw your money out.

Steve: Yeah. And great big money happening in Bitcoin land. We have a lot of discussion of Bitcoin coming up here because they, well, the major Bitcoin exchange, MtGox, lost their database. And actually it's, well, we'll talk about that in a second. But that was a problem. And the currency crashed.

So Microsoft has declared victory over autorun malware. Anyone who's interested can Google the phrase, "Autorun-abusing malware (Where are they now?)" That will get you to Microsoft's TechNet blog link, where they're strutting around and boasting about the fact that ever since they turned off and changed their policies about autorun, the autorun abusing malware has been, I mean, the degree of abuse has just been collapsing. And that page does have some really interesting graphs that corroborate that fact. And so I say to that, sheesh. I mean...

Leo: I don't know, strong language.

Steve: I know. That's a big word. You can put some extra e's in there: sheeeeesh. They finally turn off what all security-conscious users have been doing and urging everyone else to do for years. And this comes back to another one of my favorite phrases that I call the "tyranny of the default." Which we saw with the firewall in XP. Microsoft boasts about how XP has a built-in firewall. And this is Ballmer strutting around onstage before XP was released. But they had it disabled by default. So nobody had it turned on. And there were, like, all these remote exploits coming into Windows. It wasn't until SP2 that they finally turned it on by default.

The point is, the key is "by default." And it's why, for example, I'm upset about third-party cookies being enabled by default, I mean upset from a tracking standpoint, because most users just leave the settings there. I mean, most users don't change the default. So the fact that autorun has been traditionally on by default meant that that's what everyone was using, was autorun was on, and Stuxnet and other worms and viruses have just been having a ball with that.

So finally Microsoft decides that's not a good idea. They do so reluctantly, I mean, with amazing, world-class reluctance because they don't want to disable a feature in any of their OSes that was ever turned on because they're afraid of the secondary effects that that will have. But, boy. When they do, then they boast about the fact that, oh, look, autorun is not a problem anymore. Yeah, well, it only took them how long? I guess Windows has always had it.

Leo: Hey, a little mea culpa. I've been talking with our sysadmin, Bear, and he says, yes, in fact, we were hacked. So I'm not going to talk about - we've cleaned it. It's safe now. Don't think that there was an issue. And I don't - he says he'd prefer that we don't talk about what the hack was until he's got it all locked down. But it was not an error. There was...

Steve: And we should tell our listeners of the podcast because this was all before...

Leo: This was before the show? Oh, okay, yeah. People were getting an error when they went to our chatroom on the web browser on live.twit.tv. And the error was coming from Chrome. The weird thing is we didn't see it all the time. Only some people saw it. We couldn't figure it out. I was skeptical. I went to the Google malware database, and we came up clean there. But that's just a database. So I'm thinking this was some sort of active monitoring that Chrome must be doing, which I don't know of, I don't know about. And it wasn't hitting everybody. But that might have been the nature of what was hacked. In any event, there was something going on. And I've talked to Bear. He says, you know, this happens to any public-facing website. We're running a variety of scripts. We keep them up to date pretty assiduously. But there are occasionally flaws. So we got it fixed.

Steve: Well, on that page is a place where you can enter a username and a password.

Leo: Could be that. Could be that script.

Steve: And that's all scary. And then it takes you, yeah, exactly, and it takes you then to an IRC client where you can type things in. And again, we've talked about how this kind of thing happens. Any time you are soliciting user input, there's a risk of malicious input somehow tricking the back end, whatever you've got back there, and executing that input when it's just meant to be benign username and password.

Leo: I didn't realize we also - the reason it wasn't hitting everybody, I didn't even know this, we have three servers. I mean, I know we have many servers. But I didn't know that it was being load-balanced between three servers. So you'd only get it one time in three or whatever, you know.

Steve: So the hacker was able to compromise...

Leo: One of the three.

Steve: ...the database of one of the servers; right.

Leo: Was not a database hack. I'll say that much.

Steve: Okay.

Leo: But I'll give you more - I'm not covering it up, I just want to make sure everything's cleaned up before we say anything.

Steve: Yeah, yeah. So this is just completely random, but I thought interesting. You and I have talked about this before. Sophos, the security research company, noted that, well, actually their blog posting was pretty funny. They said: "Please update your antivirus at least once every five years."

Leo: At least.

Steve: Just, you know, for us. Because after seven years the MyDoom worm still exists and is still actively trying to spread.

Leo: Hard to believe. And it wouldn't if you had an up-to-date antivirus.

Steve: It is, exactly. Because that's got to be so - that's in every AV pattern database that has ever been created since MyDoom, which was seven years ago. And remember it spreads by email, and it's a worm. And, I mean, everybody knows about it now, yet there are still machines out there that have it live and running and trying to propagate. And as you and I have said before, these old Internet-wide worms will never completely go away. There will always be some machine forgotten in a closet somewhere, connected to the Internet, that will be out scanning IP addresses, trying to plant MyDoom or MSBlast.

Leo: It's basically the herpes of the Internet. Just endemic.

Steve: Exactly, exactly. So...

Leo: Somebody in the chatroom says, "Every five years? Who has time for that?"

Steve: It's just such a hassle to have to reboot every five years after you update your passwords, your patterns. Speaking of passwords, my friend Simon Zerafa, who finds all kinds of interesting stuff for me and sends them to me via Twitter, found another site. Actually he was the source of HasSonyBeenHackedThisWeek that we'll be talking about in a second. But meanwhile we have ShouldIChangeMyPassword.com. This is clever. I'm not endorsing it at all because it's also a little frightening. But clever. So https://shouldichangemypassword.com.

Leo: I love it.

Steve: It is great. It is an aggregation of all of the publicly available...

Leo: By the way, I think Lieutenant Uhura is hailing you on Channel 4.

Steve: That's a generic incoming email from my Blackberry.

Leo: I like it. I don't know if everybody heard that, but that was great.

Steve: I forgot to put it in the other room, so...

Leo: No, that's fine, I don't care.

Steve: Yeah, so, exactly, that's who it is. So ShouldIChangeMyPassword.com. It's an aggregation of all the hacked databases of usernames and passwords, just the passwords, that have been made public so far. So this is some guy. He's @dagrz on Twitter. So again it's @dagrz. And he says, "If you have any questions or concerns, please contact me on Twitter @dagrz." On his page he says no passwords are stored in the ShouldIChangeMyPassword.com database. And below he says, "The email you enter will NOT be stored, transmitted, or otherwise used beyond this check."

For what it's worth, Ghostery only reports that he's got Facebook Connect and Google Analytics on the page. And in every way it appears legit. I mean, my feeling is it is. But he is soliciting that we put our email address into his website. So if this wasn't a good guy, he's obviously come up with the world's coolest email address harvesting hack. Which he's probably not doing. I completely, I mean, again, it looks completely legitimate, and he's got only the best of intent.

So what this obviously does is, it allows you to put your email address into this website, which will then attempt to look it up in any of the known public previously and recently hacked exploits and see whether it's there, meaning that your email address has leaked publicly. So it's a quick way of checking that, which is really cool. A number of less security kneejerk organizations than ours have talked about it. He's got a media link on that page, I think three or four different articles that said, hey, this the most wonderful thing ever. Which again, I think it's very cool.

Leo: He's got my email address. Let me put it this way. I did it.

Steve: And you've not been hacked.

Leo: No, I don't think so.

Steve: I did not put one in. I did not put mine in.

Leo: Oh, I see what you're saying. No, when I did it, it said, no, you hadn't - your email does not show up in this database.

Steve: Ah, good.

Leo: I don't know whether he did anything with my email address.

Steve: No. And I'm sure, I mean, I have...

Leo: You know what, my email address is everywhere.

Steve: That's a good point. It's the Leo address, Leo?

Leo: Yeah. I mean, I'm on every mailing list there is, so...

Steve: I can't even imagine the spam. Oh, that's right, you've solved that problem.

Leo: I don't have it. I've got...

Steve: Using MailRoute.

Leo: Yeah.

Steve: So anyway, I just wanted to bring it to our listeners' attention in case anyone is interested. And maybe you've got, like, throwaway email addresses, or scratch ones, or something you care less about. I just, you know, I can't put mine there. But...

Leo: Let me show - because we have a viewer in-studio visiting us today who just ran it on his iPad. And he had been hacked. I'm going to cover up his email address here and just show you real quickly.

Steve: Okay, so that, okay, even you saying that, Leo, the idea that it actually works, for me that tilts the balance.

Leo: Yeah, I mean, yeah.

Steve: Like over in the yes, I really want to know that.

Leo: It says, "Your email username and password have been compromised at least one time. The most recent recorded occurrence, June 19th, 2011."

Steve: Three days ago.

Leo: That's three days ago. "You should change all your passwords as soon as possible." So this means that LulzSec did - it was in that database.

Steve: Yes.

Leo: Wow. Good you ran that. Well done.

Steve: Okay. So ShouldIChangeMyPassword.com.

Leo: Very interesting. I'm going to go back there right now.

Steve: It seems worthwhile. Put a few more in. And I do, you know, the guy, it's over HTTPS, so he took the trouble of creating, of getting an SSL cert for that.

Leo: I think this is legit. This has to be legit.

Steve: Yeah. I do, too. But again...

Leo: So Greg, thank you for - Greg Taylor's in here with his son Timothy. Thank you for doing this.

Steve: So I would say recognize the fact that you're putting your email address into a website. On the other hand, we do it all the time, whenever we're signing up for anything else. So I think I'm probably being overly cautious, especially when it could provide that kind of a valuable service, like it just did to one of the guests sitting in front of you, Leo.

There was news of quantum crypto being cracked, and I got a tweet storm.

Leo: After last week, even.

Steve: Yeah. I got a tweet storm from this, unfortunately. It has not been cracked. So I just wanted to put everyone's mind at rest. What happened was there's this one mode of basically quantum communications which is believed to be uncrackable, where you use quantum entanglement, essentially, in order to lock photons together and detect them in photodiodes. And the idea being that any alteration that occurs in the light path between the two endpoints would absolutely be detectable because that would break the quantum entanglement.

What some researchers did just for the heck of it was they made the system work differently by doing a man-in-the-middle attack, but essentially moving the system out of a quantum entangled mode into standard light mode. And because the particular crypto system that had been built as - I mean, no one's using any of this yet. But because the system hadn't been built to detect whether quantum entangled photons were being

received or just regular happy photons, it kept on working.

And so all the people who didn't look at the fine print said, oh, my god. I mean, and the headline said "Quantum Crypto Cracked." Well, so it hasn't been. And I'm sure the people who set up the entangled photon communications are able to detect, now that they've been advised that this is a problem, that they should make sure the regular old non-entangled photons are not used instead.

Leo: [Laughing] How can you tell?

Steve: I think we're okay. Yeah, the entangled ones may move a little bit more slowly. I'm just - that's not true. Okay. So Attacks & Breaches. Oh, boy. There have been so many recently - I mean, this is like, we've talked about this, this section of the podcast expanding without limit - that CNET has finally charted them. You can Google the phrase "keep up with the hackers chart," and that's probably the easiest way to find this. Or, sorry, keeping, "keeping up with the hackers chart." If you Google that, you'll find the link to this CNET hackers chart. I also tweeted it myself this morning so that I could refer to it in the podcast. So if you do a search of @SGgrc on Twitter, one of my very recent, I think I did two this morning, one of them is a link to this, which is a Google spreadsheet.

And my little SSL monitor popped up when I went to Google, and I thought, whoa, wait a minute, why is that popping up? It's because Google had recently changed their certificate, and I hadn't been to spreadsheets.google.com before. So I love the fact that I've got that thing monitoring my SSL connections. And I know many of our listeners do, too. And so this is just an amazing spreadsheet. It's not even current, and it's still comprehensive and long. But I think it stops on the 16th, so it's a few, like, maybe five days back. But anyway, very comprehensive and a little bit unnerving when you look at all of what's been going on recently.

What's not, for example, on the spreadsheet yet is that WordPress got hacked just recently. Their blog posting on Tuesday, June 21, which was yesterday from when we're recording this, was titled "Passwords Reset." And they wrote, "Earlier today the WordPress team noticed suspicious commits to several popular plug-ins..." They were AddThis, WPtouch, and W3 Total Cache.

Leo: Well, I use two of the three. That's not good.

Steve: Okay, "...containing cleverly disguised backdoors. We determined the commits were not from their authors. We rolled them back, pushed updates to the plug-ins, and shut down access to the plug-in repository while we looked for anything else unsavory. We're still investigating what happened, but as a prophylactic measure we've decided to force-reset all passwords on WordPress.org. To use the forums, trac, or commit to a plug-in or theme, you'll need to reset your password to a new one. Same for bbPress.org and BuddyPress.org. As a user, make sure you never use the same password for two different services, and we encourage you not to reset your password to be the same as your old one." So don't just...

Leo: Don't be a nitwit, in other words.

Steve: ...enter what you had before, exactly. "Second, if you use AddThis, WPtouch, or W3 Total Cache, and there's a possibility you could have updated in the past day, make sure to visit your updates page and upgrade each to their latest version." So we don't have any more information at this point about what it was that happened there. But someone got into their plug-in system and maliciously, deliberately altered those three plug-ins in order to install backdoors in them. So we'll have to hope CNET adds that to their list.

Leo: Yeah, wow.

Steve: Okay, now Bitcoin. This I also got a huge amount of tweets from our listeners, which if nothing else I'll use to gauge interest. And of course Bitcoin is a curiosity. We've talked about it extensively. We did a podcast on it because the technology is cool. It's also interesting sort of just to watch what's going to happen with it over time. Like, you know, there's been grumblings in the U.S. Congress about legislation to outlaw it or ban it or say they don't like it. I don't know what they can do really because it's a distributed peer-to-peer virtual currency. But...

Leo: You know what, what the senators are talking about is, what scared them is Silk Road, which is the website that uses Bitcoin to sell drugs and drug paraphernalia. It's interesting because Silk Road, I tried to go to the website, you have to be running a TOR. You have to go through TOR to get to Silk Road.

Steve: Be anonymized to get to it, interesting.

Leo: Yeah, it's really interesting how they've layered it all.

Steve: So here's what we know of what happened. In summary, the currency crashed to $0.01 per bitcoin, so one cent...

Leo: A penny, a penny.

Steve: A penny per bitcoin. And our listeners will remember that it was recently at $30. And since I'm still holding the 50 bitcoins that my computer magically minted for me in less than a week, that would have once been $1,500.

Leo: Now it's 50 cents.

Steve: And we did - yes. Well, it's recovered, but...

Leo: Okay.

Steve: So, yes, it went from - for a while it was 50 cents. And we did talk after that

about how the currency had - I think it dropped to about $20 when we talked last week, and that was due to a flurry of trading from people probably like me, who said, hey, I'm cashing out now. 30 bucks sounds like a good deal for a bitcoin. So, okay. But on June 19 at 17:15:36 UTC, some person placed one or more orders to sell hundreds of thousands of bitcoins, causing its exchange rate - now, this is through the MtGox exchange, MtGox.org, I think it is - causing their bitcoin exchange rate to crash from, at the time it was $17, down to $0.01, which is one penny.

Okay. More than $1.1 million was traded during that one or more transactions. And the exchange was overloaded so that it took about half an hour to execute the orders. Then, okay. That was at 17:15. At 17:51 UTC, "Kevin," in quotes because all we have is his first name, bought 261,383 and, if anyone cares, .763 bitcoins, so more than a quarter million, 261,000 bitcoins, for $0.01 each. Meaning he caught that collapse at the bottom, and he spent...

Leo: That's suspicious.

Steve: Isn't that, well, he spent $2,613 to buy up more than a quarter million bitcoins. Which would have been worth $5 million back prior to the collapse. Now, I found a posting from Kevin which I thought was really interesting, so I wanted to share it. He said, "I'm Kevin. Here's my side." And he wrote this two days ago. He said, "I'm Kevin, and I'm the guy who bought" - I have a different number here - "259,684 bitcoins for under $3,000 yesterday. I really wanted to keep this as quiet as possible, but I don't feel I can anymore. Here's my side of what happened. On an exchange like MtGox there are typically hundreds of standing buy orders, where people are offering to buy bitcoins at various amounts and prices."

Leo: Oh, so he had a buy order in place.

Steve: Well, no. I mean, this guy Kevin is clever. So he gives us some background here. "When a large sell order comes in, an exchange will start with the highest priced buy order to match up the buyer and seller, then move down to the next lowest buy order. This repeats until the entire quantity of bitcoins being sold have found buyers."

Leo: Makes sense.

Steve: And of course that also sets the current exchange rate because how far has it come down? Like the most recent transaction was at this many bitcoins, so that's what a bitcoin is worth now. He says, "So this repeats until the entire quantity of bitcoins being sold have found buyers, or there are no more buyers at the minimum price the seller was willing to accept." So the seller could say I want to sell this many, but I'll accept no less than this amount. And so our listeners understand that.

He says, "I was watching, like many of you, a gigantic sell order burning through the bids." So this is that order we talked about before that occurred about 50 minutes before Kevin. "MtGox doesn't execute trades very quickly, so we were watching this huge order slowly eat up every buy order on the books. The price started at around $17.50 and within minutes had been driven below $10.

"At this point I realized this wasn't merely a large seller willing to accept some losses. This was someone attempting to crash the market by selling a huge percentage of the market's total bitcoins all at once. I had around $3,000 U.S. in my MtGox at the time from earlier sales I'd made. I looked at the market stats and realized that there were tons of orders to buy bitcoins at one cent, that is, 0.01, that would likely eat up any remaining bitcoins this seller had on order. I figured, if I put a buy order in" - and I love this - "for 0.0101" - so he puts his buy order in for one hundredth of a cent over a cent.

Leo: Smart.

Steve: Yes, very smart.

Leo: I mean, he doesn't know that he's going to get anything, but why not? You don't have any risk.

Steve: Exactly. And he's able to buy bitcoins at a penny, essentially. He says, "...my order would" - there's Uhura again - "my order would execute first, and I could buy a huge amount of bitcoins from this seller before it hit the bottom."

Leo: Smart man.

Steve: Isn't that cool? "The only problem was that MtGox was running slower than molasses at the time, and everyone was saying that it wasn't accepting trades. I had to try several times, but eventually I got my buy order in, offering to buy as many bitcoins as I could for 0.0101. The site stopped responding completely for a while, probably from so many people hitting refresh to see what was going on. When I got back in, I saw my account." And he posts 06-19-11 at 17:51: Bought bitcoins, 259,684.77 for 0.0101.

Leo: He must have gone [sound].

Steve: Oh. He says, "I had just purchased over 250,000 bitcoins for $2,613."

Leo: Good deal.

Steve: "At the trading price immediately before this large sell order happened, that number would have been worth nearly $5 million."

Leo: Wow.

Steve: "After I regained my breath" - because, I mean, you know, obviously he's active in bitcoins. He had some low number, probably historically. Suddenly he has got a quarter million of them, and he knows what they used to be worth.

Leo: Right.

Steve: So he says, "After I regained my breath I tried to figure out what to do. I wasn't sure what was really going on. Over the past few days there had been a lot of talk and complaints about MtGox's security. Lists of MtGox usernames, email addresses, and encrypted passwords were being traded around, which was an obvious sign that security at MtGox had been breached in some way. If there was an attacker in the system, perhaps he was able to log into my account now and force my account to execute some other crazy trade. I attempted to withdraw the bitcoin balance into my own wallet," so essentially move those bitcoins which MtGox had converted from dollars into bitcoins, but they were still holding. So he wanted to transfer them into his own machine, essentially, into his own wallet.

And he said, but he "hit the limit that MtGox has preventing you from withdrawing more than a thousand U.S. dollars' worth of bitcoins at the current market value in a day." And remember that he now had about $2,600 worth at the super low, driven down to a penny price. "This transferred 643.27 bitcoins to my personal Bitcoin account" - and I think he meant to write dollars' worth of bitcoins - "to my personal Bitcoin account before hitting that limit. It was pretty well known that the limit for transferring bitcoins was actually broken in MtGox. It stopped you from moving more than that in one withdrawal, but you could immediately ask for more and get another thousand U.S. dollars' worth over and over." Oh, so they weren't doing their day check, essentially. "I decided against this, since it was exploiting a bug, and I definitely didn't want to do anything suspicious-looking or improper. Anyway, that's all I wanted to share."

Leo: I think that's a fair defense. Don't you?

Steve: Yes. Yeah. I absolutely do.

Leo: It makes sense.

Steve: Yeah. So there is a fabulous graphic of the collapse which is at a site called Leanback.eu. And you can look at it, Leo, because the link is in our notes.

Leo: Pulling it up right now.

Steve: It's just very cool looking. Maybe you can stick it up on the video feed for people who have the video. What we do know is MtGox has confirmed that their entire account database was exfiltrated and posted publicly. They wrote, "It appears that someone who performs audits on our system and had read-only access to our database had their computer compromised."

Leo: Oh, interesting.

Steve: Yes. So it wasn't actually the MtGox system, although there are credible security

analyses of their website that have demonstrated some serious security problems, too. So it's not like they're in the clear here. So they said this allowed someone who got into their auditor's system with read-only access to pull the user account database. That consists of username, email addresses, and password hashes. So they were hashing. Unfortunately, they weren't hashing very well.

61,016 accounts were in the database. Most were hashed with a UNIX MD5-based crypt, which is pretty good, but 1,765 were plain MD5 unsalted, non-iterated hashes. So brain dead, basically. They're going to be in any rainbow table because MD5 has been well rainbowed already. And in fact, those hashes, if people do a Google search for the hashes, they're turning up on the 'Net, and they've been cracked. So accounts have definitely been troubled.

So later, in a blog, MtGox said, "We're happy to report that over 10 percent of our user base have already reclaimed their accounts." And so they must have done an account lock and required people to change their passwords. So they said, "Newly reclaimed accounts require strong passwords which are now secured with an SHA-512," so that's Secure Hash Algorithm, 512-bit, multi-iteration, triple-salted hashing.

Leo: Yum.

Steve: Now, I don't know what triple salting is, but it sounds like it's bad for your blood pressure.

Leo: It does.

Steve: So it's their triple-salted, multi-iterated hashing. So they have certainly increased their security over what they had before. Now, what they're doing is they are rolling back all trades which occurred from that first collapse, which was a fraudulent trade, apparently perpetrated by somebody that was able to get all those bitcoins as a consequence of having compromised accounts, or maybe stealing them because that's something else that happened recently that we'll talk about in a second. So they're going to roll - basically they're invalidating all trades and resetting time to before this occurred and putting the exchange rate back to where it was at $17.50.

So that's the story that many people, many of our listeners had asked about, like, what exactly is it that happened? Also in the news was the fact that some sad user on June 16 had his computer hacked, not through any particular means. We don't know exactly what it was that had got into his machine. But he at the time had 25,000 bitcoins, worth half a million dollars, and they were stolen.

Leo: So he says.

Steve: So he says.

Leo: Can we validate? I mean, is there a way to know that?

Steve: Well, remember, one of the cool things about the whole system is that it is absolutely anonymous. So he says he had those. Let's see. We know how many bitcoins exist, and there is an absolute audit. Part of the technology is you have a log of every single transaction that occurs. So anyway, I remember him being credible. He's been in the community for a long time. You won't believe what his handle is. His handle is "All in Vain," believe it or not.

Leo: So he was depressed already.

Steve: Yes. And it's believed that, because he's been involved for so long, that he was probably an early miner, and he was mining bitcoins and using GPUs and...

Leo: Well, come on, though. How could you get that many?

Steve: Yeah, and why would you not trade them out? Probably he was reasonably expecting, based on history, that the value was high and going up. And so he was thinking, yay, I got 25,000 bitcoins, I'm going to hold onto them. So, yeah, he's not happy right now. And, finally, the EFF has stopped accepting bitcoins as donations.

Leo: Oh. That's a surprise.

Steve: Well, and they have a nice blog post where they explain it. And they said - they gave three reasons. They said, "We don't fully understand the complex legal issues involved with creating a new currency system." And that's sort of the headline of a paragraph where they go into, like, the Congress is not happy. We're not sure where this stands in terms of, like, legal structures and statutes and so forth. I mean, so they recognize that currency really brings with it much more than the cool technology, which is all we talk about and really focus on here. It's really a big deal. But they're just saying we don't understand them, so we're going to say, oops, no. They also said, "We don't want to mislead our donors" about, like, where they stand.

Leo: I send them American dollar. That's a good currency.

Steve: And they said people - yes. And they said, "People were misconstruing our acceptance of bitcoins as an endorsement of Bitcoin itself." And I think that was...

Leo: Absolutely.

Steve: Yes. The fact that the EFF was taking bitcoins as donations said, hey, somebody very reputable, and certainly the EFF is, is accepting them. So that gave them some credibility. They said that they're going to take all the bitcoins that they have accrued and dump them into the Bitcoin faucet so that they are back in circulation. And they feel like they've sort of washed their hands of them. So anyway, that's the story on Bitcoin. But it's not the story on Attacks & Breaches for the week.

Leo: No. Far from it.

Steve: Last Sunday - are you sitting down, Leo? You probably are. You're on a ball.

Leo: I'm on my ball. I guess that's sitting down. I'm floating.

Steve: For four hours last Sunday...

Leo: I know what you're going to say because I already - yeah.

Steve: Yeah. Our friends...

Leo: I already fell off my ball.

Steve: Our friends at Dropbox had a minor little software update glitch, which meant that no one's password was being checked, and anyone could log into anyone's account with no password or any password. Dropbox blogged, and this was Arash Ferdowsi, he blogged on June 20, so two days ago, he said, about "Yesterday's Authentication Bug": "Hi, Dropboxers. Yesterday we made a code update at 1:54 p.m. Pacific time that introduced a bug affecting our authentication mechanism. We discovered this at 5:41 p.m." - so a few minutes less than four hours - "and a fix was live at 5:46 p.m. A very small number of users, much less than 1 percent, logged into Dropbox during that period, some of whom could have logged into an account without the correct password. As a precaution, we ended all logged-in sessions. We're conducting a thorough investigation of related activity to understand whether any accounts were improperly accessed. If we identify any specific instances of unusual activity, we'll immediately notify the account owner. If you're concerned about any activity that has occurred in your account, you can contact us at support@dropbox.com. This should never have happened. We're scrutinizing our controls, and we will be implementing additional safeguards to prevent this from happening again." Signed, Arash.

Now, I don't think there could be any better example of why we absolutely have to adopt a PIE, the PIE in the sky, PIE, Pre-Internet Encryption. If anyone was doing that, if the only things they had stored were strongly encrypted things, then the worst an attacker could have done would have been - there would have been no loss of information. They would have gotten files of pseudorandom noise. They could delete them, but I think Dropbox has an undelete mechanism. So, or they could have modified them. That would have been annoying, if you didn't have backup copies of the original files. So certainly it's bad for people to get into your Dropbox account. But this certainly says you absolutely want to be encrypting this.

So I wanted to bring two things to our listeners' attention. There is an event log as part of Dropbox, and you can just get to it with Dropbox.com/events. And it will show you, pretty much with nice granularity, everything that has happened to your Dropbox account in recent time. And you can choose 10 or 25 entries per page and move back in time. And so if anyone's concerned and is a Dropbox user and may not have been using it during that period, that is to say from 1:54 p.m. Pacific time on Sunday to - and that'd

be the 19th - for four hours after that, you can just check the log to see if anything happened on your account. Or, if you were using it, if anything looks like it wasn't you on your account.

And there is an interesting client-side encryption, a PIE solution, Pre-Internet Encryption, for Dropbox, called SecretSync. It's GetSecretSync.com/ss. And I have looked at them before, and I looked at them again this morning before I put this entry in my notes. And I like what I see. They create their own encrypted folder, and they say put the things that you want to encrypt securely for Dropbox into the SecretSync folder, and it will encrypt them before Dropbox has access to them.

Leo: I like that.

Steve: Yes. It looks clean. It looks legit. There's a link in the upper right of their page to the parent company, which offers this also for Box.net and has a number of other encryption solutions. So it looks good and real. And I don't know why - and they say put things you don't care about the security of in Dropbox, in the regular Dropbox folder. Put the things you do care about in your SecretSync folder. And I don't know why you would put anything in the non-SecretSync folder. But so anyone using Dropbox...

Leo: Oh, there is public, you can use Dropbox for public files. You obviously wouldn't want to encrypt those.

Steve: Ah, okay.

Leo: Yeah, this is great.

Steve: Yes. GetSecretSync.com/ss.

Leo: Now, do we know that they don't know our password?

Steve: I have not fully vetted them. The thing I was able to do with LastPass was a little bit unique because of the nature of who LastPass is and just how forthcoming they were with their technology, showing things like here's our scripts, here's a page where you can demonstrate that the same thing we're doing in our script is what we say we're doing. I mean, it was - I was able to really thoroughly examine it. But I have no reason to mistrust these people.

Leo: They do say it's client-side encryption, which is what we're looking for.

Steve: That's exactly what we want. We want client-side encryption so it's done in your browser. And they use AES-256 encryption. So anything is encrypted before it goes out of your machine, which is exactly what we want.

And, let's see. SEGA Pass was breached and lost 1.3 million account users, 1.3 million.

They said, "Over the past 24 hours we have identified that unauthorized entry was gained to our SEGA Pass database.... The breach resulted in the compromise of email addresses, dates of birth, and encrypted passwords of 1.3 million users, but luckily no personal payment information was acquired by the attackers since SEGA doesn't store it and uses external payment providers. So this isn't super bad, but it's email addresses. And they do say that the passwords were encrypted, but they don't give any details, like was it just an unsalted, single-iteration hash or what. We don't know. But so that makes it to the list. And I checked back in with HasSonyBeenHackedThisWeek, and we still yet a big "YES" on the page. And we're up to...

Leo: I mean, really big.

Steve: Yes. And we're up to 20 times in two months.

Leo: Oh, man.

Steve: They've added a Sony Hack History page just to run through. And in fact the top entry on it right now is suggesting maybe it's time for people to stop using Sony.

Leo: Oh, my goodness.

Steve: Yeah. Because that just - it just goes on. I mean, and you sort of start glazing over. But, I mean, these are all real, legitimate, true hacks.

Leo: Now, I'm a little, now that we're in the club, so to speak, I'm a little less anxious to knock anybody for being hacked. But holy cow. Holy cow.

Steve: Yeah. Now, finally, there was a non-hack that generated a lot of news and for me a lot of incoming tweets. There was the claim that the Lulz Security folks, LulzSec, had hacked the U.K. Census. There was a posting, I think it was on Pastebin, that said that the entire U.K. Census database had been acquired by Lulz Security. Now, it turns out that's not the case. Lulz Security doesn't normally announce in Pastebin, so that raised some suspicions, and they formally stated that they did not hack the U.K. But if anyone was interested in asking for their help, they would be happy to, in their words, destroy the people who did hack the UK, if anyone did. And in fact there's no evidence. The Pastebin file said we're currently looking at the database, and we'll be posting it in the future. So no evidence of this other than a spoof. And it's just believed to be a completely fraudulent spoof. Nothing behind it.

Leo: I can add one more. It's not a hack either, but it's an interesting story. You know I use Pinboard...

Steve: Yes.

Leo: ...instead of Delicious because Delicious, I don't know, Yahoo! gave up on them for a while, and then they sold it to somebody, and I just don't know what the future of Delicious is, and I love Pinboard. Pinboard's written by one of the Delicious founders. It uses the Delicious API. It's a bookmarking system I use for all the shows. So the FBI takes some servers down. Did you see this story?

Steve: I did, but it didn't make it onto my list. Go ahead, Leo.

Leo: Well, let me add it to your list, only because I'm kind of interested in what's going on with Pinboard. And we still don't know. But Pinboard was down for quite some time earlier this week, and it had been so reliable, and they had such a good business model. And I just thought, well, this is going to be - these guys are going to be rock solid. Apparently the FBI, in an attempt to go after...

Steve: One particular site.

Leo: ...one site, a customer of a hosting company called Digital One, they apparently couldn't figure out which server that they wanted, so they took out three racks of equipment, including apparently the Pinboard server. They just took it. Pinboard's running on a backup server. They don't know if theirs was lifted by the FBI, but they just know that their server, their database server is gone.

Steve: It's gone.

Leo: Disappeared. And because Digital One is locked out of the server farm, they can't - they don't know.

Steve: Wow.

Leo: In fact, it doesn't - The New York Times reporting this story doesn't even say - said they don't even know which of their data centers. I mean, this is so ham-handed.

Steve: Yeah. Yeah.

Leo: Curbed Network, a New York publisher, offline. Not because they're suspected, but because they were in those racks. And Pinboard.

Steve: They were in the same rack.

Leo: Yeah.

Steve: Wow.

Leo: So I just - apparently this is part of the LulzSec investigation. And, you know, I'm not anti-FBI. I have a lot of friends in security services, and I know that these guys are actually pretty smart. But that's just ham-handed. If you're Pinboard, it's got to...

Steve: Well, it's more than that, Leo. I mean, it really does, it evidences an absolute lack of caring. I mean, that was deliberate. It's one thing for there to be a mistake made, like for example where a top-level domain, or rather a second-level domain gets taken down, as we reported months ago, in order to take a site off, and it turns out that that was a web hosting domain with many other domains underneath it.

Leo: It's happened before. That was ICE; right? Yeah.

Steve: Yeah, that's a mistake. This was deliberate. This was people at the FBI who said, well, we don't care. We're taking them all.

Leo: Or they were ignorant. They apparently thought that one enclosure equals one server. So they just took the whole enclosure.

Steve: I don't know. You'd have to be so...

Leo: That's stupid.

Steve: You'd have to be the janitor, Leo. I mean, if you've seen a rack of servers, there's no way, I mean...

Leo: It was a bunch of machines.

Steve: It looks like the computer from the old Seaview back on "Voyage to the Bottom of the Sea." I mean, it is - you can't think that's one of anything. It looks like it could run the entire world.

Leo: The Instapaper, which is another service I use, had a server there. It's gone. Marco Arment, who runs Instapaper...

Steve: Instapaper, no kidding.

Leo: Yeah. He said - now, fortunately, he has other servers. But he said, our site is up but slowed by this. Unbelievable. And Arment says he hasn't heard from Digital

One or law enforcement.

Steve: Yeah. I don't give them a pass on this one. I give them a pass on making a mistake, like had happened before. But this, this was, I mean, it wasn't malicious, obviously. But it was deliberate. They had to know. Anyone has to know. I mean, three racks? These servers are probably little 1U slices. So you're going to have hundreds of these little 1U things all blinking and spinning. I mean, it's going to be incredibly heavy, use an amazing amount of power. But, I mean, it's obviously going to be much more than what they were looking for.

Leo: It's not unusual for law enforcement, when they're doing a raid, if they're raiding, for instance, a house, just take everything.

Steve: They do take everything.

Leo: Just take everything because you don't know what's going to be evidence and what's not going to be evidence. But there's such big collateral damage to completely innocent sites. Wow.

Steve: Yeah. I mean, it can't be allowed to happen in the future. I mean, the world and commerce and the economy is coming to depend on this crazy toy that DARPA invented to pass packets around, which we now call the Internet. I mean, it's becoming really real. And so you just can't arbitrarily say, well, we're going to just take away a chunk of it. Anyway, that just...

Leo: I'll be very curious to see if we hear any more, if there's any - nobody's saying anything.

Steve: Yeah. Yeah. I have a bit of errata because I wanted to note that Java applets, I had said that they could only be invoked through JavaScript, which is not the case. So I wanted to correct that. Even with JavaScript disabled, or not using JavaScript, there are native means in HTML for embedding, using the embed tag, a Java applet in a page. So I wanted to correct that. NoScript does control Java applets in addition to JavaScript. And so, for example, if you go to a page that even has JavaScript disabled, you can click on the Java applet and say, yes, I want to just run this one Java applet. NoScript gives you that control. So I wanted to correct that.

And I had a couple quick notes from the Twitterverse. Robin Morley tweeted his experience with Ghostery. He said, "Is a 25 score on Ghostery a new record? Courtesy of Salon.com."

Leo: That's the largest I've seen. That's amazing.

Steve: Yikes. Can you imagine 25 spyware tracking things? Well, and that's the kind of thing you'd expect on Salon.com, I mean, where they're being hosted by virtue of all the

advertisers and so forth. What do I have here? I have, oh, Marc Beaupre in Montreal, Quebec said one way to know whether the site stores your password in cleartext is whether they send the password itself when you perform account recovery.

Leo: Ah. That's true.

Steve: And I thought that was a very nice point. If they hash it, they cannot possibly send you your password in cleartext. So if anyone ever does, you know that they're not hashing it. So, I mean, it's probably obvious in retrospect, but I wanted to just make note of it.

And several people have talked about positives, surprising positives from Microsoft's System Sweeper. And one Rich Staples tweeted me, and he said, "Thanks for the tip on the Microsoft System Sweeper. First test subject was positive." And I've decided that I'm going to deliberately run it on all my machines. I don't believe that any of them have any malware in them, but that's the point, is many people are reporting that System Sweeper is finding rootkits that they had no awareness of. And so, if you don't run it, you don't know. And I've decided, well, when I reboot my systems I'm going to reboot off of a freshly made ISO and just make sure that there's nothing there. So I wanted to encourage listeners who for whatever reason may have gone to unsavory places, may have had their machine acting up, but now they think it's okay. Maybe they found some stuff, and they believe it's removed. Anyway, if there's any reason to think that something might not be right, might not be completely copacetic, I would recommend Microsoft System Sweeper. I'm going to do it on all of mine.

Leo: It does take a while to do, Monkey [indiscernible] points out.

Steve: Yes, it does, yes. And Lorenz Gude sent a nice story from Western Australia, in Perth. He said, "Here's a SpinRite story for Steve. I have a neighbor who has mild Alzheimer's, who's also been forced to give up his flat and move into a nursing home about 20 miles away on the other side of the city. His Compaq notebook computer has become his main way of keeping in contact with his family and friends. He's a bit of a newb, and he often manages to get it pretty tangled up. I fix it for him when I visit him on Thursday afternoons on my way to tai chi. It is his lifeline, so he works hard to learn new things and has progressed from email to Skype to Google Earth.

"Last month, just a couple of days before leaving for the U.S., I paid my friend a last visit, and the inevitable disaster had occurred. The Compaq would not boot. SpinRite immediately came to mind, and I knew that it would be complicated and expensive for him to have the computer fixed commercially. But I didn't have much time. My problem was getting it back to him before I had to fly out. Quick as a flash, my friend saw the solution. I could leave it in his old flat, which was near me, to which we both have keys, and he could retrieve it after I flew out using his electric scooter and Perth's excellent train system - which can accommodate scooters during nonpeak periods, just FYI.

"In the end that was not necessary. When I got the Compaq home, I immediately ran Level 2, and it finished in less than an hour and booted up first time. No time-consuming need to reinstall Windows and all those endless updates. To be safe, I ran SpinRite again on Level 4 overnight and was able to drop the computer off the next day in plenty of time to catch my flight. I know it's still working because I get emails from him regularly. Now, Steve, all we need is SpinRite for the human brain. I hereby volunteer for a Level 4 scan

anytime you're ready." So that was a neat note. Thanks very much, Lorenz.

Leo: Awesome. Let me just check before we get to - we do have a few questions. Let me just check to see, yeah, we're still - Bear is still cleaning up the aftermath of the hack. Just to say it again, I guess it was our chat software. There was a library on the server that was hacked. We're working to figure out how that happened. It was only one of the three servers. It did not propagate to other servers. And as far as I know, I don't think any information - I know there's no information in there except for perhaps a chat password. We'll let you know if those were compromised. I think that's a pretty low security issue, but we'll certainly let you know as soon as we find out. But we want to keep it on the QT for a little bit to make sure that all the holes are patched before we...

Steve: We'll talk about it next week.

Leo: Yeah. Or maybe sooner. Yeah, it looks like it was a file insertion attack. So we're working on - we've got everything, I think we've got everything repaired. We just want to make sure that the hole is plugged before we talk any more about it. And we've got some good sysadmins, and I have absolute confidence in these guys and their ability to lock stuff down. So it just shows you, even with a very well run system and some very aggressive sysadmins, things - stuff happens.

Steve: Okay. So Leo, I looked at the page, and it's a ton of JavaScript. And this is not JavaScript that you guys wrote. This was JavaScript that other people wrote with the best of intentions. But, I mean, that's the problem is that code is incredibly complex and difficult to write. Even with security in mind, there are things that can happen. And, for example, Dropbox made a mistake where they used to have password checking, and that somehow got disabled for four hours. So stuff happens. So, I mean, the problem is that you guys, I mean, this is the only practical thing for you to do, are using scripts from someone else to provide IRC stuff.

Leo: I can give you a little information. There was a - we use a very well-known library that is absolutely a great library. That library was modified. What we don't know is how it was modified. So it's not that we used something that inherently was dangerous, but that something was modified. The point you're making, which is absolutely true, is there's a lot of stuff running on that server, and we don't know exactly how the bad guy got in. So we're working on that. And once we know that, we will let you know, and we'll also let you know what kind of - it's not like we're doing eCommerce here. We don't know much about you.

All right, Steve. We only have time for a couple of questions, so let's do a few just token questions here.

Steve: Yup. It looks like I sort of scaled that correctly.

Leo: Yes, you did. Yes, you did.

Steve: So it's your turn, Leo.

Leo: Oh, I read them, don't I. Sure. All right. Let me get my reading glasses on here. Question #1, John Fecko in Cape Coral, Florida, asked this on Twitter, so it's nice and short: Does encrypting everything that goes into a database prevent SQL injection attacks?

Steve: Which I thought was a great question.

Leo: It is.

Steve: Yes. And the answer is no, unfortunately. Encrypting everything that goes in does encrypt the database, that is, the database's data. But the SQL injection attacks are typically used, not with the data, but with the command, the SQL command. And so the problem is that the way current web server back ends are set up, they have an SQL database which is participating in the creation of the page. So, like, you're on a web forum, and the contents of the forum is coming from the database and being decrypted as it's being brought out to the user's client.

But unfortunately the page itself contains commands, SQL commands which the server interprets as the page is being generated and rendered and sent to the client. So it's when bad guys are able to inject some commands into a site that they're able to get the SQL data that they injected to be treated as a command. And so even if that was encrypted when stored, when it's displayed it's decrypted. So it ends up being that the commands are decrypted just like the data that's being displayed on the page would be decrypted, so the encryption doesn't help you. It helps you if the database file were to get copied somewhere because then it's just going to be gibberish if someone doesn't have the matching key. But essentially the injection attack uses the live data, which necessarily is decrypted in order to become live. So no help there. But great question, John.

Leo: Patrick, Laramie, Wyoming comments and wonders about latency versus bandwidth: Steve, while I realize this is outside the normal scope of Security Now!, I feel this topic should be discussed. ISPs typically quote their performance numbers in megabits per second. While this number can be useful, it doesn't tell you anything about the performance of the connection. What everyone perceives as a fast Internet connection is actually low latency, not high bandwidth. A low-latency T1, say over fiber, will feel screaming fast, even though it's only 1.44 megabits per second, compared to a high-latency satellite connection, even if the satellite moves data at twice the rate. For all non-saturated networks, latency is the king of the hill, not bandwidth, although bandwidth does make a difference for high amounts of data being transferred, say a video, a large image when you're downloading a file, that kind of thing. Yet all ISPs merely quote bandwidth. I'd rather spec a connection based on latency rather than bandwidth. What do you think? Patrick.

Steve: Well, I think both are important. But he does raise a very good point.

Leo: It's a good point, yes.

Steve: Yes, because the Internet, the way the web experience is, is highly transactional. We've talked often about how the browser makes a query, the server sends the page back, the browser parses the page containing a ton of resources, which the browser then needs to ask for from all over the 'Net. So each of these things. Oh, and sometimes it has to look up a domain name. So it's got to send out DNS queries. The point is many, many little transactions. And so if there was a delay per transaction, many of these are being done in parallel, but many of them have to be done in serial, like the DNS address has to be obtained from the domain name before the client can then make a query out to the remote server and so forth. So it's absolutely the case that a high-bandwidth, high-latency experience for that kind of transactional work will feel very slow.

But to your point, Leo, transferring a big file won't be a problem because TCP has all kinds of fancy technology now, which actually was not as fancy in the beginning. This was added to the TCP spec over time as the Internet grew and as the bandwidths increased. The idea is that, as we talked long ago, early in the podcast, TCP has this notion of a window which allows the sender to send data ahead which hasn't yet been acknowledged by the recipient. And that's necessary, otherwise things would go really slowly. Otherwise latency would be a huge problem. So this notion of being able to send things ahead and have delayed acknowledgement, as it's called, is specifically to address the latency problem. And actually there is a bandwidth-delay product is what it's formally called. The bandwidth-delay product says it's the bandwidth times the delay that you care about, and you want to keep that, you want to work to optimize the bandwidth-delay product. So great question, Patrick, and a very good point.

Leo: Yeah, I just - I won't name names, but I just replaced the - this is another one, and you have a benchmark to test it, the DNS server. A slow DNS server will make you appear to have slow surfing because it takes a while to come back with the domain or IP address. And that latency can also kill you, even if you have a very fast connection. I just replaced, on one of my ISPs, the domain name server for the ISP with OpenDNS, and boom, big, huge difference. Feels like my connection speed is tripled. But it hasn't.

Steve: Yeah. Yeah. And I've had a lot of feedback. Again, we did talk about GRC's DNS Benchmark, which is a bit of freeware from me which does exactly that. And a lot of people have said, hey, I found that - in one guy's case I remember seeing, he said, 4.2.2.1 is the fastest for him, and that's one of the Level 3 servers that's been around forever, and frequently fast. And OpenDNS is very fast, as well. So as you say...

Leo: Yeah. Test it, though.

Steve: ...that can absolutely slow you down.

Leo: Download Steve's tester, and you can find out what the best is. Because it would be different everywhere, I imagine. Every user would have a different experience.

Patrick McAuley in Guelph, Ontario, Canada asks: Abandon passwords? Steve, did you see this Gizmodo piece arguing for abandoning passwords in favor of some entirely new scheme for online identity? He said read the comments after the piece, as well. We'll put the link in the show notes. I already have on the show wiki. You could also Google "Gizmodo, it's time to abandon passwords." Mat Honan wrote this on Gizmodo. What do you think?

Steve: Well, every time I use my little, always present and never very far away from me, football to authenticate to PayPal, I'm glad that they offer it.

Leo: Yes.

Steve: What we clearly need - there was a blurb, it was the SEGA Pass comment blog posting that I read where SEGA said none of our users' financial information was lost because we use a third-party provider. That struck me as, yeah, I mean, that's cool. And if there was one that I absolutely trusted, I would love to offload that responsibility. I mean, for myself, I wrote all my own code and developed my own merchant processing and credit card processing system just because security is paramount for me, and I would hate to ever have to write a letter to my users saying that the people who process our credit cards have been compromised, and therefore you might be in trouble. I would hate that. So if there were somebody that you could offload that responsibility to, that would be fantastic.

Similarly, we really do need some sort of centralized third-party solution. We've talked about OpenID as being sort of a, well, sort of a quick hack for doing that. It's sort of limping along and not really taking off. There is work by the U.S. government, putting together something called, I think it's NTSIC is the - or NSTIC, I can't remember the acronym. But I've got it on my notes to talk about it because the notion is it's like a trusted infrastructure for authenticating users. What we need is some single central place or places, I don't care if there's competition, but right now the problem is we're doing authentication per site. And that's just wrong. We need to have that centralized.

I mean, there's a downside, of course. And that is, if it's centralized, then that's the pot of gold that the bad guys go after. But it is, I will say again, not impossible to have security done right. It just has to be really important to the company to do it right and to care. And so if we authenticated with a single authority and used multifactor authentication if you want to, I mean, for the added security, I certainly would, then websites would bounce us there to authenticate and just get back an anonymous token that says, okay, the same person who created this account before is back. And that's how we would identify ourselves, rather than having to give every single place we visit our name and address and information and so on and so forth.

So, I mean, we're to the point now where this has to happen. It is time for it to happen. The idea that we have to individually create accounts, and then we're responsible, all of the burden, all the onus is on us not to reuse the same password. You're almost tempted not to reuse the same email address, although that's difficult for many users. I control my own server, so I have netflix@grc.com, for example, or I'm able to easily create those on an as-needed basis so that I've got separate identities all over the place, which is unfortunately not convenient for most people. But, yes, we really do need to have this taken care of, Leo. Something has to happen.

Leo: I'd love to see something, well, and this is what I use for SSH. I use public key cryptography to log - I don't use a password. I use, I don't know what you would call it, but I'm automatically authenticated when I log onto my SSH server because I have the key on my server, and it's a known key on that server, and I don't know. What do you call that?

Steve: You are using strong cryptographic security, strong cryptographic authentication.

Leo: Right. So I don't ever enter a password. I just SSH on that computer. And because that key is on that, it's, yeah, I don't know what you call it. But anyway, it works. And I actually asked our admins, I said, is this okay? And they said, oh, yeah, this is preferable. We don't want you to use a password. Just use your SSH key.

Steve: Right.

Leo: And that does - that is great. So that's how I do it.

Steve: Yeah, we're going to get there. We're in the Wild West days still, and the responsibility is ours. I am working on something which is going to be cool. And we'll talk about it in a couple weeks.

Leo: Okay. I can't wait.

Steve: It's in this password space still.

Leo: Steve Gibson is the man in charge of GRC, the Gibson Research Corporation, GRC.com. If you want to download any of his great stuff, including the fantastic SpinRite, the world's best hard drive maintenance and recovery utility, but also lots of freebies on there for security and encryption and passwords and all that stuff, even just fun, like Wizmo. You can also follow him on Twitter. His Twitter handle is @SGgrc. @SGgrc on Twitter. And actually, as we can see now, he responds and follows and does interesting stuff with that Twitter information. So that's good.

Thank you, Steve, for being here. We do the show every Wednesday at 11:00 a.m. Pacific, 2:00 p.m. Eastern. Live.twit.tv is the place to go to watch it. Do keep up, I'll post a blog post on the TWiT.tv site and on my blog about what the security hack was, if information was compromised, if any. If anything, you know, the only information we have is some people on our IRC have passwords. That database could have been compromised. If you have an IRC password, it would probably behoove you to change it. And if you have foolishly used that IRC password on other sites, you might want to change those other sites, as well. We don't have any reason to believe that was compromised. That's just prudent. And we'll find out more, and I will keep you posted because I believe in full disclosure. Steve, thanks, and we'll talk to you next week on Security Now!.

Steve: Talk to you then, Leo.

Leo: Bye bye.