IE9

Description: After catching up with a great deal of security news and interesting computer industry miscellanea, Steve shares everything he has recently learned from his extensive study into the new security and privacy features of IE9.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-293.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-293-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 293, recorded March 23rd, 2011: IE9.

It's time for Security Now!, the show that covers your security, your privacy, everything you need to know about protecting yourself online and, in the process, I think does a pretty darn good job of teaching all of us the fundamentals of computing technology. And that's thanks to this guy, Mr. Steve Gibson, who's been doing it for an awful long time now, starting with the light pen he wrote for the Apple II computer; his many columns, loved those columns in InfoWorld magazine. What was the name of that column?

Steve Gibson: It was Tech Talk, was the name of that, yeah. I originally called it Behind the Screens, but CompuServe had a trademark on that name, and so we were told we had to change it. So I just said, well, Tech Talk.

Leo: How long did you do that?

Steve: That was eight years.

Leo: Wow.

Steve: Or maybe nine years.

Leo: I learned so much from that.

Steve: It was a great column. It ended up, I mean, Dvorak was there with me at InfoWorld, and Robert X. Cringely, and...

Leo: Oh, yeah, the original, not the current one.

Steve: Right.

Leo: There have been many of them. I don't think the current Cringely is actually the same Cringely as was there in the early days.

Steve: I don't know one way or the other.

Leo: It's a character. It's like Betty Crocker.

Steve: Right.

Leo: Well, I have to say, and I'll give you full credit, there were a few people that early - because I started getting into computers late '70s. Did start early on writing, I wrote for Byte a little, wrote for InfoWorld, did reviews. But I was learning in the early '80s. And the way I learned was you, Dvorak, Jerry Pournelle in Byte magazine...

Steve: Yeah, Byte magazine.

Leo: Steve Ciarcia's "Circuit Cellar" in Byte magazine. It was just a handful of columns, and I read them religiously. InfoWorld was weekly, which was great, so I read it every week. And that's how I learned. That's how I, you know, it was great. So I owe you. I don't think I've ever thanked you. But I owe you a debt of gratitude.

Steve: Well, as you said, it's all about fundamentals. And I guess I view everything from that standpoint, from that foundation. And so it gives me a perspective that other people don't have who haven't been doing it since they were four years old.

Leo: I do wonder how kids today - because we were all, you know, personal computing was a new industry. So we were all kind of learning together. And there was this great exciting time.

Steve: It would just be overwhelming today, Leo. I mean, it's so big, you'd have to be looking at it, thinking, where do I start? Like, what do I do? How do I make a difference? It would be daunting, I think.

Leo: And there are no, I mean, those magazines are long gone. There are no magazines anymore really to speak of. They're all very small.

Steve: Dr. Dobb's Journal, that was another one of the good ones.

Leo: Yes. "Running Light Without Overbyte." I read that religiously, cover to cover. That was a great magazine.

Steve: Yeah.

Leo: And nowadays, I mean, there's a lot of stuff, there's a lot of content on the web. But I don't know, it's mostly fan content, content about content, and less so about the inner workings. Even AnandTech and the other kind of geek sites are more about benchmarking and building a computer than about the fundamentals. So I'm glad we do this because I think this is one of the last few places where you could say - we've got 293 episodes, and you could go back, and you could start at the beginning and learn as much as I learned from Steve's columns over the years. Take you a little less than eight years to read it.

Steve: I think probably it sneaks up on people because we didn't start out by saying we're going to tell you about the fundamentals because some people might have started to snore, thinking, well, why does that matter? But by sort of folding that stuff in, it's like, oh, I'm glad to know where this came from because it gives it some richness and some background.

Leo: Well, you've done it as needed. So we can't talk about crypto unless you understand the fundamentals of crypto. So it's always been - yeah. Well, today what are we talking about?

Steve: I think we need to cover IE9. I have spent all my time, well, a lot of my time, when not playing with iPad 2 - which finally did come a couple days ago, and I like it, Leo. It's just, to me, I would agree with you. I can't see a reason, a compelling reason for someone with the first iPad to upgrade to the second, especially when there are strong rumors about a third, which is probably no more than another year away. And it's really going to be the one we want.

But to me the second iPad just feels like a second-generation device. It feels substantially more polished and refined. I mean, physically holding it, it just - and of course holding it is what you do a lot with a tablet, much more than a computer. And it does seem to have a faster frame rate when you're dragging pages and doing the little animations that are sort of just part of making it a nice experience. So I like it a lot. But I spent a lot of time with IE9, which was not easy for me because you can't install it on XP, which is, as we know, the operating system I'm still proudly sitting in front of.

Leo: Microsoft is thinking of you specifically, Steve. They're trying to force you to

move forward.

Steve: Well, it's funny, too, because there have been a lot - there was a lot of press noise about IE9, and of course about Firefox 4, with actually recently the Firefox 4 people saying that they were outstripping the download rate for IE9. And IE9 was pretty, I mean, it was significant, too. It was several million copies of IE9 downloaded since its release. On the other hand, no one...

Leo: Well, Microsoft has hundreds of millions of users, you know.

Steve: Yes. And nobody with XP. I mean, remember, there's still a huge XP base. It's not like I'm the only one left still using XP...

Leo: I think it's still the majority in many countries. I don't know about the U.S., but...

Steve: Yes. And so none of those people are downloading IE9 because it won't. It just says, I'm not compatible with your operating system.

Leo: Do you think that that's a technical limitation or a marketing issue?

Steve: I would say both. They could have certainly made it compatible, as is IE8. Although IE9, as I'm sure Paul will have told you, is in fact deeply integrated with Windows Explorer, with the tray and the taskbar and the pin-ons and - or pin-ins or ons or ups or, I mean, I didn't bother spending much time with some of the frosting of IE9 because I know that you and Paul and a lot of other people in the industry are going to do that. I'm looking more at privacy and security aspects.

Leo: That's what we want from you, absolutely, yeah.

Steve: Right. So but I do think that the decision they made was to take advantage of some of the new UI features that were added in Vista and then carried further in Win7. And so, you know, they could have probably made it work, but it wouldn't have had those things. And they probably just said, hey, it's time to give up on backward compatibility. Which is surprising for them.

Leo: I love this. In the chatroom somebody said, "Why is Steve using XP?" And he's getting a little schooling from one of our chatters, Popojijo. He says, "Because new is inherently the nemesis of security." We have trained them well.

Steve: That's great. Yes. In fact, someone asked me had I moved yet to Firefox 4, and I said, unh-unh. No, that was, like a couple days ago. Let's let it settle down a little bit.

Leo: It's just too young.

Steve: Yeah. I installed it on my MacBook Air so that I could sort of diddle with it over there on a little island all by itself. And the other thing, too, is that it immediately, I don't have nearly the number of add-ons for Firefox 4 that I do have for Firefox 3. But it immediately said, oops, this is not compatible, and that's not compatible. In fact, NoScript doesn't even display the little options down in the taskbar in...

Leo: Oh, that's disappointing.

Steve: Yeah. Although many people tweeted me and emailed me. I don't even want to look at the mailbag next week for the Q&A about, duh, Steve, NoScript does have button add-ons. You just go to customize your toolbar, toolbar buttons. Remember I was talking about how...

Leo: Oh, yeah, you wanted an on/off switch, yeah.

Steve: Oh, they're coming out my ears now. So, yeah.

Leo: Well, I apologize for not knowing that myself. So you can write to me. Don't berate Steve.

Steve: It's very nice. Very nice. So thank you, everybody who tweeted and who wrote. And I was immediately schooled, as was our poor chatroom person who said, why doesn't Steve always run the latest and greatest? It's like, well, I'll get there eventually.

Leo: IE9 our subject. We also have some security updates, some security news, of course. Wouldn't be a show if we didn't keep you up to date on the latest. I like that. That's something we added, I think, around show 100. For the first few hundred shows we didn't talk about security news so much because we wanted to be a timeless show. But then we realized that it's important. So let's start with the security updates, I guess, because, well, it's funny, you didn't put this in your notes, but I just was doing an update. Apple did a big update.

Steve: Right, huge, 300-and-some-odd-meg update of OS X. Just, you know, catching up security stuff, standard next version of OS X. And it took, oh, about an hour for me to get downloaded. And then it sits and rebuilds itself in a sort of a non-applications-running mode, and then restarts, and you've got the next version.

Leo: It doesn't seem like anything's changed, but I know there are a lot of security patches and all sorts of stuff.

Steve: Right. Yeah, no big feature changes. We talked last week about the recently

discovered, at the time recently, zero and bad, zero-day exploit for Flash, which was being exploited by people who had a malicious Shockwave Flash file embedded in an Excel file. Then there was, like, a third layer. I can't quite remember what it was. But anyway, it was being used for targeted attacks that Google said were politically motivated somehow, based on their observation. And Google Security also recommended - oh, I'm getting myself confused. That was the MHTML mistake that was politically motivated, that Google said use the Fixit to disable yourself. And we still have no fix for that over on the Microsoft side. But we did get a fix for the auth DLL problem, which was actually part of Reader and Acrobat, but exploited through Flash.

And so two days ago from when we're recording this, on March 21st, Adobe did release updates for their various versions of 9, Adobe Reader and Acrobat 9. They are holding to not releasing one for X, or 10, because they're saying that their built-in protections are holding over on that side. And so they're going to wait until summertime to update on their schedule, in their normal cycle, their quarterly cycle. But they were unable to do that for people who were still using 8 and 9.

So I did want to let everyone know, you can just go adobe.com/support/security, and there's separate updates for Flash and for Reader or Acrobat, depending on which one you have installed on your system. And I've got to say, I'm liking what Chrome is doing, under Google's management. They auto-patched Flash for themselves the prior Wednesday the 16th, just...

Leo: That's interesting. So they are taking responsibility for the version of Flash that comes with Chrome.

Steve: Yes, they are. Which I find is interesting. I don't know what their arrangement is with Adobe that allows them to do that. But they responded instantly with this. And it just - people who were using Chrome just had it fixed.

Leo: The more I use it, the more I love it, I've got to tell you.

Steve: Yeah, and boy, is it speedy. I've looked at some benchmarks relative to IE9 that we'll be talking about here in a minute. And Chrome is really out there. I mean, it is really, really speedy. We don't have any updates from Microsoft. I did want to remind everyone, though, that IE8 was pwned during Pwn2Own at the Vancouver security conference a couple weeks ago, using three undisclosed but still unpatched vulnerabilities. The person who came up with that has I'm sure communicated them to Microsoft, and Microsoft is fixing them. And as long as they stay secret, and no one else discovers them independently, then that's a good thing. But of course knowing that they're there does encourage people to go after them. So the clock is ticking on that.

The week's biggest security news was that RSA announced they got broken into.

Leo: Yeah. I was so hoping you'd talk about this because I'd love to know what this means.

Steve: Not only am I talking about it, I did my first blog posting in a long while because I was so annoyed with what little they said. Their senior VP guy put out an

announcement on their site, and they even made an SEC filing, a filing with the Securities and Exchange Commission...

Leo: Really, wow.

Steve: ...like, because they felt they had to because...

Leo: It had material impact on their business.

Steve: Well, materially affect their stock evaluation. So excerpting from, like, the most annoying chunk from what they wrote - and anyone who's interested can go to steve.grc.com, and it's my most recent blog posting there that has had a lot of really great feedback added to it since I put it up earlier this week. RSA wrote, and get a load of this bureaucratic say-nothing speak. Oh, it's unbelievable.

"Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations."

Well, okay. If you have a multifactor authentication system, and one factor relies on a piece of hardware whose numbers are changing - the SecurID is basically what we've talked about, like with the PayPal dongle, the VIP technology, that's what it is. It's a time-based, changing every 30 seconds, six- or eight-digit, typically six, LCD screen thing.

Leo: So is it - I have this VeriSign identity protection.

Steve: Same thing.

Leo: But is this the one, or is this using RSA?

Steve: No, no, no. This is...

Leo: This would be one from RSA.

Steve: Well, no. The VeriSign is from VeriSign. VeriSign uses Vasco, I think, as their provider. And, but, I mean, it's the same technology. It's cryptographically driven, time based, six characters, you know, six digits. And the point is that it's driven by a unique key that nobody knows. Well, somebody knows it now. And that's the point.

Leo: So you mean all of the cards on the RSA technology are compromised.

Steve: We don't know that.

Leo: Okay.

Steve: So what RSA is claiming is they said - okay. So reading from my own blog posting, I said, "On March 17th, 2011, Art Coviello, RSA Security's Executive Chairman, posted a disturbingly murky statement on their website" - and I have a link to that on my blog posting - "disclosing their discovery of [what they called] an 'APT' (Advanced Persistent Threat). In other words, they discovered that bad guys had been rummaging around within their internal network for some time" - hence "persistent" - "and had managed to penetrate one of their most sensitive and secret databases," the SecurID system.

Leo: Unbelievable.

Steve: I know. And so what has upset many people, not just myself, but, I mean, many people, is that RSA, that's essentially all they've said. But then they also said other things, like make sure not to let people see the serial number on your RSA dongle.

Leo: Oh. I just did. Mine's VeriSign. Hope they haven't been compromised.

Steve: Oh, no, VeriSign's completely different, so I don't want to confuse anybody.

Leo: I understand, yeah.

Steve: Completely different. RSA has something called SecurID that is their take on adding a hardware token or a software token. You can also do software. But a lot...

Leo: By the way, I want to just point out that this is widely used in government.

Steve: Oh, yes, yes, yes.

Leo: And by spooks.

Steve: 40 million. When SANS, the SANS Security Institute was reporting this, they mentioned that 40 million SecurID tokens had been deployed, which are often used to conduct financial transactions and by government and major corporations.

Leo: Dr. Mom says the hospital healthcare system she works for uses those keys for record access.

Steve: Yeah, I mean, this is big. So in my blog posting, essentially I took the position of, okay, they're not saying anything. But what they did say was that their SecurID two-factor authentication system had been compromised. Well, okay. There's only one thing that is a secret, and that is the mapping between the serial number that's printed publicly, for the public to see on the outside of the SecurID tokens, and the matching cryptographic key which determines uniquely the sequence of numbers from one 30-second interval to the next. So if anything has been compromised, that's what's been compromised because there's nothing else to be compromised.

Leo: In fact, that's their entire business.

Steve: And that's the worst thing that could possibly be compromised.

Leo: Geez. Oh, my god.

Steve: So it's really bad. So, and there is, down, way down toward the end of the comments, I link to another person's blog posting that I liked a lot because he essentially took them even further to task than I did. And there have been people privy now who have seen the letters that RSA has sent to their corporate customers. Basically they're CYA letters which are essentially telling the customers to be much more careful with their own networks and with their own disclosure of things relating to SecurID, like don't let people know what the serial numbers are.

See, it used to be fine because no one knew what the secret key was that the serial number mapped to. But if that database has escaped RSA, if that's been exfiltrated - and, I mean, to be sympathetic to RSA, and I was at one point, I said, you know, bad things happen. And if people are using toy operating systems, which is what we're all sitting in front of, I mean, Windows is a toy. Look at what a catastrophe it is from a malware and virus standpoint. So here's a corporation like RSA that you really want to have bulletproof, industry-strength security. But they've got to be using Windows or Macs. And these machines are not secure. That's why we have a podcast. And so unfortunately - and they talked about it being, oh, a very sophisticated cyber attack. And I'm hoping that it wasn't that somebody didn't just open a bad PDF file and get themselves...

Leo: Yeah, oh, boy.

Steve: Because that's how this stuff happens all the time. So I really, I am sympathetic to the fact that somebody got into their network. But it's very, very difficult not to have people getting into the networks of large corporations when people really want to get into the networks of large corporations. And now here's the problem, is that, after the fact, they discover this so-called APT, persistent threat. Well, how do you answer the question, what did they get? How do you know what they got?

Leo: You don't know.

Steve: You really don't know. It's exactly analogous to what we've talked about. If you've got malware in your system, if your system has got a rootkit on it or malware that you've discovered, you can never again be sure of the security of that machine. You have to go back to an image made from a time before that thing got in and then work forward. Or format the hard drive and hope that it didn't infect the firmware of your display adapter.

Leo: Oy. We talked about that last week, for folks who just said, what?

Steve: Exactly. So I really, I'm seriously sympathetic to RSA's condition. And they're a big corporation. They're owned by EMC, an even bigger corporation. They've got obligations to their shareholders. They've got obligations to all of the 40 million users of their SecurID tokens who are now wondering, is this secure or not? So, I mean, I have suggested, drawn the conclusion, that since something got away from them that relates to SecurID, and the only thing that they have that relates to SecurID is that mapping database between the publicly known serial numbers and the secret cryptographic keys on all those devices, they may not know how much of it got out. We hope it didn't all get out. But we're talking about replacing all of those. I mean, they're not secure now. So what RSA seems to be telling their customers is, well, try to keep all the other factors as secure as possible because the one you bought from us...

Leo: You're screwed.

Steve: Yeah.

Leo: Oh, boy.

Steve: It's not good. So, meanwhile, RIM - Research In Motion, our BlackBerry creators...

Leo: I just ordered the new PlayBook. I'm excited.

Steve: I was going to ask you, Leo. If I were to get a Android tablet, what do you think? Because the PlayBook is supposed to support Android.

Leo: No, the PlayBook is not. It's QNX.

Steve: No, I know, but it apparently supports Android apps.

Leo: What?

Steve: You haven't heard that? Yeah.

Leo: Oh, that's exciting. That's good news. That opens up, of course, a giant app store.

Steve: Yeah. Well, we'll talk about that in a minute because in my errata I'm talking about Amazon.

Leo: Yeah, there are a lot of third-party - third-party. There are a lot of companies making Android tablets, including the new Samsung Galaxy tab. There's a seven-inch, but there's a 10.1 coming. There's the Xoom we've talked about with Motorola. Lot of kind of off brands. Archos makes them. But I think that these - it's still a little rugged, a little rough. I was very impressed with the seven-inch PlayBook when I played with it briefly.

Steve: Ah, so you have had your hands on it.

Leo: Oh, yeah. I had it for the Regis and Kelly show. And very impressed with its multitasking. QNX is a really robust real-time operating system.

Steve: Oh, it's been around forever and ever, yeah.

Leo: So I think that was an interesting and good choice. Now, of course, it's not known as a touch operating system, but the touch seemed to work quite well.

Steve: Oh, good.

Leo: So we'll see. I ordered it. It comes April 19th.

Steve: Oh, yay. Cool. So anyway, what I was saying about RIM and BlackBerry is that they were unnerved by the fact that they got pwned also during CanSecWest a couple weeks ago. And they're now advising all their customers - wait for it, wait for it...

Leo: Buy an iPhone.

Steve: Disable JavaScript.

Leo: Oh, well, there you go.

Steve: Where have we heard that before?

Leo: But right as rain.

Steve: Exactly. So it's a flaw in their WebKit-based browser in the BlackBerry. And you need to disable JavaScript. Now, JavaScript is not the problem. But you need JavaScript - wait for it, wait for it - to exploit the flaw. Yes.

Leo: Of course you do.

Steve: So just turn JavaScript off on your BlackBerry. I don't ever use my BlackBerry browser because it's the crappiest browser on the planet.

Leo: It's a terrible browser, yeah.

Steve: Oh, my god, it's just like - it's just horrible.

Leo: I'm surprised to hear it's WebKit based because it doesn't seem like it's got anything going for it.

Steve: Yeah, it sort of hurts the reputation of WebKit. I don't know what it's doing most of the time, but it's just - I don't have my BlackBerry to browse. I have it for messaging. And I think it's the best messaging platform there is, so that's what I have it for.

India, speaking of BlackBerry, India and BlackBerry are in the news again with Robert Crow, who's the BlackBerry VP of Industry and Government Relations, quoted as saying, "Holy smokes" because India's Home Ministry, which is responsible for domestic security, has informed BlackBerry that it will require the ability to intercept communication data sent via email capabilities of the BlackBerry handset. And Crow was quoted, it said according to Crow, "These demands could potentially open up the doors to further problems, such as whether the government tracking of ambassadorial conversations or even transfer of financial files would be off limits."

BlackBerry's concern is that, first of all, they really care about the security that they're offering to the users of their handsets. They have repeatedly told the Indian authorities that it's impossible to do what they want. And they've reiterated that, that they don't have the keys; that their fundamental architecture is an end-to-end encryption, and there's nothing they can do.

Now, and the point they're making here is that apparently they're not very confident of the infrastructure in India to responsibly manage opening these doors. Which, sure, they could update their firmware, and they could rejigger things and fundamentally dramatically weaken their platform. But if they did so, what kind of abuse would this

open themselves to if suddenly it became known that people without much authorization were able to get access to email messaging. It would substantially hurt the platform. So they're at an impasse. India has not given any deadlines. And, significantly, they have not singled out BlackBerry. There are other VPN and peer-to-peer technology providers, like Skype, that have been given the same ultimatum.

Leo: Really. Oh, interesting.

Steve: Yeah. So I don't see how this is anything more than huffing and puffing on India's part, but we keep talking about this. It doesn't go away. And this has just happened again. So, he said, "You connect the dots and you're saying, 'Holy smokes.'"

I wanted to let our U.K. listeners know, and I know we have many people who follow the podcast from the U.K., that the major ISPs there have all signed on to a voluntary policy where they're going to specifically delineate what they're doing with bandwidth shaping. BT, Virgin Media, Sky and others have signed a voluntary code of practice, saying that they'll provide consumers with clear traffic management policy information explaining when Internet connection speeds are throttled, why they are, and what effect that throttling will likely have on consumers' broadband service.

Leo: That's all we want to know.

Steve: Yes. And the disclosures will also state whether the provider has arrangements with specific content providers to prioritize their traffic. So basically coming clean.

Leo: Great.

Steve: Which is really, really good news.

Leo: If you're going to do it, at least let us know so we can choose. That's great.

Steve: So, yeah, I was really glad to see that. So Friday morning I got a call from Good Morning America.

Leo: Really.

Steve: They wanted someone who could talk on the issue of celebrities' cell phones and email accounts and things being hacked. And I said, well, I can do that. And they said, oh, we'd like to talk to you. And so we talked for about 45 minutes. And then the producer of this pending segment said, "Steve, come on up and let's put you on camera and just say everything that you said again." Well, I brought my MacBook Air up with a copy of Firesheep.

Leo: That must have been fun.

Steve: Let's put it this way. The aim of the segment changed when they saw what was going on. And I don't yet know when it's going to air, but I will certainly tweet. I won't be able to, unless there's a coincidence of timing, and I can do it on the podcast, I will. But I'll tweet when I know.

Leo: Can you tell us how many people was on that list on the left there?

Steve: Well, it got populated and blew their mind. And I think one of the things they're going to do is set it up themselves and reproduce it, just to show how easy it is. But one of the things that I thought was significant was I hadn't looked at the download count for a while, and I haven't for two days. But on Monday we were at 1,334,000 downloads. And by the following day it had gone up by another 3,500. So it is still being downloaded. It still works.

And, now, the good news is, it's having an effect. Ars Technica just yesterday put out a large column, and about halfway down they said something like, and I'm just paraphrasing from memory, but it was like, "Firesheep: How a good UI can change the Internet." And of course you'll remember this is why I was celebrating, with a caveat, why I was celebrating the release of Firesheep. That's why Twitter now has always HTTPS. That's why Facebook has it. It forced Google to go sitewide, more than just using it in Gmail. So, I mean, and I'm really happy that Good Morning America, a widely watched, nationwide network, morning news show is going to aim some more light on this because this will - raising the awareness of the danger. First of all, it's really good to do, to let people know what the dangers are; but to get the word out is so important, too.

Leo: I'm actually surprised they're going to do it because their issue is going to be, this is going to scare the pants off people. And unfortunately the fix is kind of technical. But I'm glad they're doing it. Now, for those who...

Steve: Go ahead.

Leo: For those who don't know what Firesheep is, we did a show on it, and a good description. But the short answer is, turn on WPA2 on an open access point, and don't use open access points that don't have security.

Steve: Right. And for those services that do allow you to use HTTPS, try to do so. Turn those settings on in Facebook and Twitter and on Google accounts. Yeah. So if you put into Google "How do I install and use Firesheep?" you get 886,000 links.

Leo: It's pretty easy. Lots of people want to know that one.

Steve: Yeah. So, wow, 1.3 million downloads since we were talking about this, Leo.

Leo: Isn't that amazing. Jiminy Christmas.

Steve: I got a tweet that I wanted to share from someone, his handle on Twitter is BioTurboNick, who said, "Just found a bunch of trojans via an MSSE full scan that weren't found by the quick scan."

Leo: Oh, that's good to know.

Steve: Yes. He said, "The shocker? They were all Java related." So we had been talking recently about Java and about removing it unless you needed it because it's becoming a problem. I mean, it's like we fix one thing, and then the bad guys move to the next soft target. After we harden that target, they find something else soft. But so this is the built-in, anyone with Windows has it now, the Microsoft tool. And I think you can just, in the Run dialogue, you can put "mrt" or...

Leo: It's "mrt," and it'll open it up.

Steve: Yes.

Leo: And then you can click "Thorough scan." So I tell people on the radio show to do this, and I'm glad that you're - well, not glad, but it does reaffirm my inclination to do a thorough scan if you think you have a problem.

Steve: Right.

Leo: Because it's better.

Steve: Right. I also discovered, to my surprise, just yesterday - and we're in Errata section now, so I get to be a little weird here.

Leo: This is - I don't know if "errata" is the right word. Miscellanea. Tidbits.

Steve: Miscellanea. Oh, you're right, you're right. But William Shatner turned 80 yesterday.

Leo: I heard that, and it stunned me.

Steve: 80.

Leo: I can't believe he's 80.

Steve: He looks fantastic.

Leo: Yes.

Steve: And in my tweet, because I tweeted this, I said, you know, gee, last time we saw him on "Boston Legal" he looked great. Maybe a little heavy, but great. And I got a ton of people tweeting back, saying, uh, Steve, that's not the last time we saw him. Aren't you watching "$#*! My Dad Says"?

Leo: Oh, that's right, he's the star of that show.

Steve: Yeah, and apparently very funny. So I've never seen a single episode of it, but I added it into TiVo, so it'll - I think it's on Thursdays. So tomorrow I'll...

Leo: Well, you know, it's based on Twitter.

Steve: Yes, exactly. And I think you and I talked about it back when it was just going to be happening. And so we're in the first season of it. And many people say it's very, very funny, and Shatner is fantastic. And I can imagine him being real - but, Leo, 80. I've got friends who are in their early '70s who can barely walk.

Leo: I know. I know. Denny Crane. He's looking good.

Steve: He really is.

Leo: Happy birthday.

Steve: I think it's all that time travel he did.

Leo: Yes. Maybe that's it.

Steve: I think that explains it.

Leo: He's actually 400. He's so much older than he looks.

Steve: And there was also something interesting that I ran into on the Techdirt site.

Leo: By the way, before we go on, there's another fellow celebrating a birthday on Saturday.

Steve: Uh-oh.

Leo: And he doesn't look a day over 80, either.

Steve: Thank goodness.

Leo: As long as we're talking birthdays, I've just been informed your birthday is Saturday. Happy birthday, Steve.

Steve: Oh, boy, that chatroom, I tell you.

Leo: They are sharp.

Steve: Can't pull anything over them.

Leo: They are sharp. I know, I don't celebrate either. After 50 it's like, eh, let's not. Let's not talk about this.

Steve: Oh, I don't care. I talked to Mom because I wanted to let her know about the Good Morning America spot that might be happening. And she said...

Leo: "Well, it's about time." What did she say? She said happy birthday.

Steve: She said happy birthday. And she said, "I'll be calling you on Saturday." I said, well, that's our routine. I called her on the 5th, which was her birthday, so...

Leo: Oh, that's so sweet. Well, yeah, happy birthday to you, Steve.

Steve: Thank you. So Techdirt had an interesting posting, someone wondering if using NoScript to bypass The New York Times' newly erected pay wall would be violating the DMCA. And I thought, that's interesting. Now, apparently - so a little bit of back story. The New York Times has generated a huge amount of kerfuffle since announcing that, it's either this week or next week, that they're no longer going to be free.

Leo: Yeah. And it's expensive if you're not a subscriber.

Steve: Oh, Leo, it's like prohibitively expensive. Really expensive. And so it's like, okay, I can find my news elsewhere. I mean, I like The New York Times. I love The New York Times. But, wow, they want a lot of money. So as I understand it, you can see 20 - you can directly look at 20 articles, and then they block you. But if you click on links elsewhere, like on search engines that take you to stories, then they don't block you. And, I mean, I remember thinking the whole thing sounded kind of flaky.

Leo: Wall Street Journal does that for some reason. You cannot see full articles in The Wall Street Journal unless you either are a subscriber or pay for it. But if you find a Wall Street Journal article link on Google News, you get the full article. So all I do, when we share Wall Street Journal articles with our hosts because we're going to talk about them, I just go to Google News, get the article, and send them that link because they can read the whole thing.

Steve: Crazy.

Leo: So I think these companies know and understand that there are loopholes. But they figure most users are not going to know about them or take advantage of them, so that's fine.

Steve: So people who have looked have determined that there's four lines of JavaScript that are, like, blocking people.

Leo: Well, at least they're efficient.

Steve: And that, if you have NoScript on, then this ridiculous "pay wall," as it's called, doesn't get erected. And you can simply use The New York Times without being blocked. And so the question then would be, are you altering the content and violating The New York Times copyright through, like, their terms of service probably change to reflect the paywall. So anyway, it's sort of an interesting question. There's a bookmarklet called NYTClean which is just, being a bookmarklet, it's a little bit of JavaScript in a bookmark, essentially. And if you ever - you can probably Google "NYTClean" to find it. And you just click that, and then it resets your paywall blocking. So I don't know, it seems crazy for them to have done something so weak.

Leo: Well, again, I think that they realize that there are, I mean, how many people use NoScript, compared to their subscriber base?

Steve: Good point. Lots of people will go, oh, shoot. Okay, here's my money because I want...

Leo: I think anything like this relies on goodwill. You can always get around - we don't charge for anything we do. And one of the reasons is I watched what happened when Revision3 started to charge for Diggnation. They said you can get early access if you pay for it. And of course, when you have a technically sophisticated audience,

as they do and we do, it didn't take more than a day or two before people paid for it and then put the early release version out on the Internet so nobody really had to pay for it. They quickly abandoned the plan. I would never do a subscribe version of this because I know that you guys are way too smart and would immediately get around it. But I'm sure that The Wall Street Journal and The New York Times just figure, well, we're going to rely on the goodwill of our readers for the money.

Steve: And they're wanting to get some revenue. It's been free forever. And so they're saying, okay, it's time for us to start making money. And it will be very interesting to see how this turns out for them.

Leo: The Times says they don't need more than a few percent of the people who read it to pay to make it worthwhile.

Steve: Oh, cool.

Leo: It's quite annoying. I subscribe. I am actually - I get the dead tree version. So I get it for free.

Steve: So you have free online access.

Leo: Yeah. It's really expensive, though. I don't think I'd pay for it if I didn't get...

Steve: It is. I mean, there's just too many other good places you can go.

Leo: Well, and we're conditioned to getting it for free. So...

Steve: Yes, exactly.

Leo: It breaks the Internet, frankly. It's not - so we'll see. I think it's foolish. But it's their business.

Steve: So the news is really nothing but good at Fukushima. We've talked about the reactor problems since the earthquake and the tsunami. And I've been tweeting about it constantly as I've been just sort of like following their progress in getting electrical power restored. They're filling the reactors from afar by shooting water into the spent fuel rod pools. And the reactors 5 and 6 now have cooling, electrically powered cooling for their spent fuel pools. The reactors did reach cool shutdown, that is, 1 through 4, the ones that were running at the time. And they've got electric power now being brought to them, and they're bringing them back. So basically I think this is going to end up being really an amazing case of phenomenal luck that...

Leo: Oh, that's not good. If you're relying on luck for this stuff, that's not good.

Steve: Yeah. I did have a real - I found a great URL that I wanted to share with people. It's jaif.or.jp/english. And it's a lean site that, several times a day, publishes an updated PDF chart of the status of all six reactors with a tremendous amount of detail, really interesting. So, again, it's jaif.or.jp/english. And so I just wanted to pass that on.

Leo: The Japanese Nuclear Foundation? What is it? It's Japanese Atomic Industrial Forum, that's it.

Steve: Yeah, exactly. And if you look at, if you just click one of the, like, the most recent link at the top there of their PDFs, it's just a spectacular chart. And several pages of it, too, I think six or seven pages of information. So for anyone who is interested in and having their fingers crossed, as I have, as this - I mean, the last thing we wanted was a really bad problem there. So I think they averted it. And just my final little bit of wackiness is the news that Apple has sued Amazon over Amazon's use of the term "App Store." It's like, oh, come on. App Store? Really? Apple, you think you own that term?

Leo: They do have a trademark. I mean...

Steve: Well, and so I wrote to my own trademark guy, my intellectual property guy, this morning. And he wrote back, and he said - I wanted to share what he said because it's a little bit of insider, inside-industry info.

He said, "It is an interesting case. Apple based its U.S. application for the mark APP STORE on a foreign registration from Trinidad, likely hoping to go under the radar as opposed to filing directly like normal." Now, and understand, the reason they did that is that normally "App Store" would never qualify. I mean, it'd be like...

Leo: No, it's too generic.

Steve: Exactly. Well, it's descriptive. And something that's descriptive is immediately disqualified for trademark registration.

Leo: Aha, interesting.

Steve: That's why something like Kleenex, the word "Kleenex" tells you nothing about what the product is. And someone mentioned in the GRC newsgroups that, well, after all, Microsoft got a trademark on "Windows." It's like, yes, but that, the word "windows," even though it actually is a word, it doesn't describe at all what Microsoft's software was. They created that connection. But Apple trying to get "App Store" is really pushing the limit.

So continuing what my attorney said, he said they filed in Trinidad, "likely hoping to go under the radar as opposed to filing directly like normal. It had the opposite effect.

Apple's application was refused registration [in the U.S.] based on descriptiveness...."

Leo: Oh, interesting.

Steve: But then they "overcame the refusal [on appeal] by arguing acquired distinctiveness (basically that it was descriptive, but now due to Apple's marketing and notoriety consumers know the App Store emanates from Apple)."

Leo: That's a good point.

Steve: "USPTO [U.S. Patent and Trademark Office] bought the argument, but Microsoft is now opposing the registration of the application. I believe Amazon saw Microsoft's argument and thought, let's ride Microsoft's coattail." And he finally said, "This is one of the really interesting cases between folks with plenty of resources. This will be played out on many levels and a lot of fun for us with no interest in the case."

Leo: Yeah, because Amazon has an app store now, and it's an Android app store. I use it, and it's pretty good.

Steve: And you've seen all the rumors about Amazon doing an Android tablet? I mean, they'd be perfect for it.

Leo: Turning the Kindle into a - well, you know, the Nook, the color Nook is a pretty capable Android tablet, if you hack it, the Barnes & Noble Nook.

Steve: Oh, no kidding.

Leo: Oh, yeah. And in fact Microsoft, just to complete the circle, is suing Barnes & Noble over Android, preparatory, I think, to claiming that...

Steve: Microsoft?

Leo: Microsoft claims that Android violates its patents. And this is the first of what I expect will be...

Steve: Oh, my god. Then they're going to establish that, and then go after Google.

Leo: Yeah. Well, I think they wait till they have a pretty good war chest before they go after Google.

Steve: Wow.

Leo: So it's just a fascinating, I mean, oh, my god. I always say, you know, compete, don't litigate. And often companies that can't compete end up litigating, and that's just a mess.

Steve: Wow.

Leo: Just a mess.

Steve: Well, I did have a short note from a listener, David W. Roscoe, who wrote to say that SpinRite saved a music studio. He said, "Hello, Steve. I'm a longtime user of and advocate of SpinRite. I've also been a listener of Security Now! from the beginning and have heard you tell a few stories about using SpinRite to recover hard drives from devices that are not computers. I have such a story which you might not have heard yet.

"My brother's a professional musician. He uses a Boss BR-1180CD digital recording studio. It's a tabletop device that he uses to record and mix his songs. One day he told me that it had stopped working after going through a period of increasingly frequent freezing. He said his repair service could fix it by replacing the hard drive, but he would lose the several dozen songs he has stored inside. He did not have any backups and asked me, the family computer geek, whether there was another way. I told him about SpinRite, that I was willing to give it a try on his hard drive. He had nothing to lose, so he let me.

"I opened the device and discovered that it contained a 20GB IDE hard drive. I moved it to one of my computers and ran SpinRite on it, which found a bunch of bad sectors, including some nonrecoverable ones. But the device did not work again when I reinstalled the drive. Apparently one of those nonrecoverable sectors had contained something needed for startup. I will skip the details and say simply that I was able to find the song folders after SpinRite fixed it on the mostly recovered drive, copy them to an initialized replacement drive, and trick the device into thinking that those songs were its own." He is a computer wizard. "My brother got all his songs back and was very pleased. This would not have been possible without SpinRite. Thanks for all the great stuff you've produced and continue to produce. Sincerely, David W. Roscoe."

Leo: Excellent.

Steve: So he solved the problem in a roundabout way on a wacky digital recording studio thing from Boss that happened to have a hard drive in it.

Leo: I wish I could easily get the hard drive out of my iMac, it's a real pain, because my son's hard drive crashed. And I'm sure I could put it in a PC, SpinRite it, and it would all be fine. But the iMac, the big negative, you have to actually take suction cups and remove the glass. It's very - it's ridiculous. Colleen did it, she's got more nerve than I did, some time ago when the hard drive on my iMac here died. And I remember watching her do it. And I thought, oh, geez. Oh, geez. I ain't doing that. No user-serviceable parts inside there.

Steve: She can weld, so she can pretty much do anything.

Leo: Yeah. Well, she had nerve. That was the thing. I mean, that just takes nerve. It was like, I mean, suction cups to remove the glass, it was crazy. I think I might have to try it, though, just to see. Or a hammer.

IE9 just came out, what, about last week that Microsoft pushed it out. People have been using the release candidate, but now the official version is out. Doesn't automatically update in Windows. You have to, when you open IE8, you get a little button that says, would you like to try IE9? But I think they said something like 25 million people have, so it's out there.

Steve: So it's really good news. I don't think it matters. But it's really good news. It is, in many ways, a state-of-the-art web browser for Windows. And that's just a good thing. As we know, Internet Explorer has been losing market share. The more really good browsers come in, the more people get pried away from IE. I famously got pried away over to Firefox. I'm not going back because I love the Firefox ecosystem. You were on Firefox for a while, having left Safari on the Mac, and now you're a Chrome user.

Leo: Big-time Chrome fan, yeah.

Steve: Yeah. But one of the problems the whole industry has had is that IE has really been a boat anchor from a standards standpoint. Famously, there were some things that, version after version after version, from IE5 on, and these are multiyear gaps between, Microsoft just stubbornly refused to fix or to do the event model - now that I'm a JavaScript programmer, I'm having to work around IE-specific stuff all the time. And, finally, in 9, they have - they've actually gone overboard, if that's possible, with support for standards. And so it represents a massive investment on Microsoft's part to create a browser which is as standards-compliant as they are. And in fact they're now more standards-compliant than anybody else.

Leo: Oh, interesting. Good for them.

Steve: They really are. I've got some numbers here that I'll cover. But so this was two years in the making. They announced their work on 9 shortly after the release of 8. And this was, like, at the developers conference in '09 that they said, okay, we're going to start working on IE9, and they began bringing pieces of it out. It's got strong support for CSS3, Cascading Style Sheets 3, and Scalable Vector Graphics, SVG technology. Their score on the Acid3 test is a 95 out of 100. Whereas IE8, which was two weeks ago, was 20 out of 100.

Leo: Boy, that's a big improvement.

Steve: So it's a huge improvement. And Firefox 3 is a 94. So they - oh, and IE8 just collapses completely and fails, doesn't even - it just is a disaster. So they've really done well there. It's got a new JavaScript engine, code name was Chakra, which compiles to native Intel machine language using its own thread in the background to leverage

multicore processors. So your page comes up, and it starts to go. And then, if you've got a multicore processor, the background Just In Time, the JIT compiler, will take off and basically turn your JavaScript into native code.

Now, what's interesting is that, while it is much faster than any IE before it has ever been, it's still not very fast. Well, I mean, it's a contemporary browser, meaning that it has joined the ranks, finally, of Firefox, Opera, and Chrome. And I guess really Safari is lagging behind now in terms of their technology. But it does support HTML5 audio and video natively. So this is what we're beginning to see is, if all you really need, for example, Flash for is displaying movies, is displaying movie clips or video, you no longer need Flash when you've got HTML5 video support. And HTML5 wants H.264 video, which is our standard MPEG-4 container. So we're moving away from the dependence on Flash for video that we've traditionally had.

Lifehacker, just like a couple days ago, did a set of benchmarks on Firefox, Chrome, Opera, and IE. IE9, meaning. IE9 was - oh, so Firefox 4; Chrome I think 10 and 11, 11 is the dev release of Chrome at this point; Opera 10, or the latest version, I think it's Opera 10; and IE9. IE was the slowest one of those to start up. It was the slowest on JavaScript, but it was able to finish, which IE8 hadn't been able to do. And interestingly, the 64-bit version of IE9, which is not the default even on 64-bit platforms, was four times slower. So probably not optimized. Maybe the Just In Time engine isn't working yet on a 64-bit platform. But again, you'd have to really try to use it because it's not the default, even on 64-bit Windows. The 32-bit is.

It also has the slowest Document Object Model and CSS system. But again, it was able to finish, whereas IE8 couldn't. And it has the highest memory usage. So it's just out a few days ago. And it's pretty much across the board worse than all the others, but vastly better than IE8. However, one place it blows everyone away is in its standards handling. It is extremely standards following. There's a JavaScript test called test262.ecmascript.org. People may want to play with it. It's super easy to use, that's why I want to give everyone the URL: test262.ecmascript.org. That'll come up. Now, IE8 doesn't even display the page, just can't even get there. It runs a huge battery of tests, 10,456 different tests. My current latest version of Firefox 3, out of 10,456 tests, fails 3,661 of them.

Okay. We'll call Firefox 3 prior generation. Now we move to current generation. The latest Chrome, latest version of Chrome, out of, again, 10,456 tests, Chrome failed 497 of those. So it passed a huge percentage, but it failed 497. Firefox 4, just out, was better. It only failed 301. IE9 only failed 17. Which is stunning, 17 out of 10,456. So IE9 really is incredibly standards compliant. And they have a state-of-the-art JavaScript engine. And, I mean, again, when I started off by saying I'm not sure that any of this matters, what I mean of course is that we have really good alternatives to IE9 anyway.

The reason it's worth covering on this podcast is that it has a chance to stay strong. And even though people listening to the podcast may have already switched to Firefox and/or Chrome, all of the people that they support who are still using IE can move to IE9. Next version of Windows will I'm sure have IE9. We've seen that the adoption rate of IE9 among Windows users who are conscious of this is strong. So it matters. Okay.

It also matters in terms of what Microsoft has done from security and privacy, which I'm impressed by. We've talked briefly about Tracking Protection Lists, so-called TPLs. This is - something makes me nervous, and I'm going to explain why. But it's potentially very nice. IE8 had sort of a - what was called InPrivate Filtering, which was part of InPrivate Browsing. And the way InPrivate Filtering worked was, if you went to a bunch of different websites, and IE noticed that there were common third-party sites that kept being

invoked by the first-party sites you went to, IE8 would adaptively - and this is impressive - it would adaptively add them to a filter, saying these are trackers because you're going to all these different first-party sites and, like, you know, DoubleClick.net keeps popping up as being polled by these first-party sites. And so it was a way that IE8 would adaptively recognize tracking behavior. So that was impressive.

The problem is that InPrivate Browsing wasn't something you could turn on and have stay on. You had to deliberately go there every time you started up IE. So it's like, okay, I don't know if Microsoft was afraid to do this full-time, or they wanted to offer it, but they felt that if they allowed you to turn it on and have it be sticky, it would be too aggressive. Who knows. But the good news is that's changed with IE9. We now have these things called Tracking Protection Lists that are files you can get from third parties who maintain them for you. The syntax of the file is very simple. No nightmare of even XML nesting stuff. It's just a simple flat text file.

The first line, in order to qualify, has to have the word "FilterList" in it somewhere, which qualifies it as a tracking protection list. You can then put comments in by starting them with a pound sign. If the first character is a pound sign, the rest of the line is ignored as just being a comment that's human readable. If the first line starts with a colon, then that's a setting line. And at the moment there's only one setting that's supported, and that's Expires= and then a value which must be between 1 and 30, which is the number of days that IE can wait before checking for an update.

So this is very nice. It means that you're able to add one or more of these TPLs, and IE will maintain them for you. It will go back to the source URL, which it keeps, and refresh them as this changes for you. Now, there's additional syntax for specifying what is and is not allowed. If a line begins with a +d, then it's followed with a domain name string specifying what domain this applies to, and then an optional string where the URL must contain that string to qualify. And the "+" means that this is an allowed domain, that is, we're going to allow IE to fetch content from there when this is being fetched in a third-party context.

So when your web browser is going to some site, if the page you load then makes references to other domains, they're checked against this list. So if that domain name occurs on a line that has a +d on it, it's allowed. If it's a -d, then it's not allowed. And after the domain, also for the -d, can be a string which, if there, must be present for that line to qualify. And then you can also just have a minus sign by itself, without a "d," in which case the string that follows the minus sign, if that appears anywhere in the URL, then it matches, and the minus means disallow. And an asterisk can be a wild character that can match any number of characters which occurs in the string at that point.

So this is a very simple and a very powerful syntax for qualifying and disqualifying fetches to third-party sites. In the case of having - oh, and you can have many lines, which can be mixed with pluses and minuses. The semantics of that is that all of the allow lines are looked at first. And anything that matches any of the allow lines qualifies for allow. Then the disallow lines are looked at, and anything that matches them, any of those queries are thrown out. They're just dropped. And then queries that don't match anything are allowed. So it's explicit allow, then explicit disallow, and then implicit allow is the sequence of processing.

Now, in the UI in IE9 they provide already a bunch of sites that are producing mature tracking protection lists. And they're familiar names. There's the Adblock Plus people who have, I think, is it EverList? It's a name I know because I've got on my adblocker on Firefox. I subscribe to that list, and so it automatically provides updates for me. But here's the problem. I mean, so all that's good news. I looked at some of these TPLs that

are available, and some of them are horrifying because I see a real problem with false positives. The domain-based blocking is fine because, if you block DoubleClick.net, it's DoubleClick.net. And the domain has to match in order for that rule, that block rule, to apply.

But that free-wheeling string blocking scares me. For example, in the EasyList from Adblock Plus, they have a block on the string ".com/ad-." Now, that means, because it's not a domain name block, it's just .com, that means that any resource on any domain, any .com domain that happens to begin with /ad-, even if it's not a domain, I mean, even if it's not an ad, gets blocked. I mean, your browser won't see it. Or ad. or ad/ or ad_. And this goes on. So it's a little worrisome that this thing could false positive.

I'm assuming, and I don't believe that I read carefully or saw this specifically, that it absolutely only applies for third parties. It has to be that this only applies for third parties, or sites would be in danger of blocking themselves. So that's some benefit. But I'm a little concerned about this being a false positive. And then the second problem is that this opens us up to the traditional cat-and-mouse game. If the advertisers know that starting their ads with ad- is going to make them not show up...

Leo: They're not going to do it.

Steve: They'll just change it to "bd" or "ax" or whatever. So basically these...

Leo: Kind of a goofy system, to be honest.

Steve: It is. It is. Unfortunately, again, it puts us immediately in this cat-and-mouse problem where now here's these lists that Microsoft makes available through the UI, which you can add. And, I mean, they're initially useful except that they're also a template for the advertisers to use for how not to name their ads, in order for them to get around it.

Leo: Yeah. Here's how - by the way, in case you're interested in getting around this, here's how.

Steve: Yeah. If you name your ads any of these things, then we're not going to display them. So let's not name them that.

Leo: Do they think that advertisers will opt in as a goodwill gesture?

Steve: I don't know what they're thinking. I mean, this is what Microsoft has come up with as their solution. And it's another one of those, well, okay. It's better than nothing, but it seems to me that it's easy to get around because here's the template for how you do it. Now, the good news is they are also supporting the do-not-track header, which, if we can just please get some legislation, then this is the perfect solution for our problem. They've submitted this to the W3C. Mozilla has submitted this. And amazingly, they're compatible.

Leo: Oh, that's good. That's good.

Steve: Yes. We do not have yet another format for a do-not-track header. It is DNT: 1. And the way IE9 works, if you enable any tracking protection list, if you have any tracking protection, then this header is included with every query it makes. That's just what we would want. And that's the same as under Firefox 4. In the Firefox 4 UI you're able to say, tell sites I do not want to be tracked. And you can turn that on, and then Firefox will add the DNT: 1 header to all its queries.

Leo: Now we just have to get Chrome to do that, and we're set.

Steve: Yes. I wish Google hadn't gone off in this other weird direction with their persistent lists or whatever that was we talked about a couple weeks ago. And so the good news is I think Google will probably do it because, with Firefox and IE9 both doing it, I mean, again, everyone says, oh, yeah, well, people can simply ignore it if they want to. It's like, well, yes, they can. And that's a problem. But if we get legislation that backs it up, then we're starting to move forward correctly. And I'll mention that there is a user - there's, like, a personal TPL, Tracking Protection List, that you can enable and leave blank if you don't actually want any tracking protection lists, but you do want the do-not-track header to be added in IE9. So we have that, and that's a good thing.

In terms of malware protection, IE9 hasn't really advanced that any further. They've added something called - they still support DEP, the Data Execution Protection or Prevention, with a don't-execute bit for processors that support it, and now pretty much all contemporary processors do. And we had that in 8, and we have that also in IE9. They do support Address Space Layout Randomization (ASLR), as IE8 had, that's also there in 9, and Safe Structured Exception Handling [SafeSEH] to handle structured exceptions. There were some exploits of that. That is, the bad guys figured out how to actually use structured exception handling, which is - essentially it's a way for

a programmer to say, if in the following block of code anything bad happens, come here so I can handle it rather than just die.

The problem is, the bad guys figured out, hey, we can subvert structured exception handling so that, when we do have a buffer overflow, it'll come to us rather than killing the application. So naturally they figured out how to commandeer that technology. The good news is that IE9 has enhanced that. They now have something called SEHOP - getting a little carried away with our acronyms. This is Safe Exception Handling Overwrite Protection, which validates the validity of the structured exception handling chain before dispatching exceptions to it. So it makes sure that the bad guys haven't overwritten the structured exception handling before it's being used.

And, significantly, that's being implemented on a per-process basis, not just on a per DLL. These other things, like DEP and ASLR, remember that DLLs had to be recompiled specifically to enable that. And so some - and we've even seen some exploits which took advantage of the fact that a couple DLLs in earlier versions of IE still hadn't been recompiled, and so they were loading into known locations. They were not using ASLR for themselves, and that's all it took for the bad guys to take advantage of that.

And then, finally, IE9 has been compiled under Microsoft's latest state-of-the-art C++ compiler, which - and IE8 was not. IE9 was, and it adds support for something called

Stack Buffer Overrun detection, which is something built in at the compiler level which should make IE9 more robust against those kinds of exploits.

Now, the thing that impresses me the most is, for the common user, is something new in IE9 called SmartScreen Application Reputation. What we're all...

Leo: That's SSAP.

Steve: Or SSAR, SmartScreen Application Reputation.

Leo: SSAPR. We'll call it SSAPR.

Steve: Okay. We will.

Leo: Yes, we will.

Steve: We're all used to seeing the warnings whenever we download anything these days, saying this has been downloaded from the Internet; therefore it's potentially hazardous. Are you sure you want to proceed? Well, what do we do? We all say yes. We know we just downloaded something from the Internet, and we want it, or we wouldn't have downloaded it. So, yes.

Leo: Of course we want that.

Steve: IE9 doesn't do that. And...

Leo: What does it do?

Steve: Which is fantastic, actually. IE9, I'm going to quote from their explanation: "Based on real-world data we estimate that this new warning" which they have, this SmartScreen Application Reputation warning, "will be seen only 2-3 times a year for most...."

Leo: Wow. But if you see it, then pay attention.

Steve: Exactly. That's the point, exactly. This is training people. Instead of training people to ignore it, this is - I mean, and this is sort of what we saw with the evolution of Vista - I'm sorry.

Leo: Of UAC.

Steve: Yeah, of Vista into Windows 7, exactly, with UAC. It's in your face much less often, so it's like, oh, okay, maybe I ought to read this. So they're saying, "...for most consumers compared to today where there is a warning for every software download. The key" - I'm still reading - "the key challenge with malware on the Internet is that attacks are fast moving and quick to change. The importance of application reputation is as an early warning system. There is latency between the outbreak of an attack and when it is detected and [proactively] blocked. Consumers today are unprotected during that time. Think of this new warning as 'stranger danger.' It's an early warning system for undetected malware. No antivirus or protection technology is perfect. It takes time to identify and block malicious sites and applications. Blocking after detection is still an important strategy, but there remains a gap between the start of an attack and when it is detected and blocked. IE9 SmartScreen Application Reputation fills that gap."

And it does it as follows: "When you download a program in IE9, a file identifier and the publisher of the application (if digitally signed) are sent [in real time] to a new application reputation service in the cloud."

Leo: Oh, interesting. Wow.

Steve: Yes. "If the program has an established reputation, there is no warning. If the file is downloaded from a reported malicious site, IE9 blocks the download, just like IE8 does. However, if the file does NOT have an established reputation, IE lets you know in the notification bar and download manager, enabling you to make an informed trust decision." And they give an example of a file called "06-FHU-ICB.exe," and it says, "is not commonly downloaded and could harm your computer." So they affirmatively acknowledge files to be downloaded that have a good reputation, a known reputation. They affirmatively block known dangerous files. And then until a file has established a reputation, only then will you get a notification saying we don't know about this, it's not commonly downloaded, so it could harm your computer. I think this is a huge win for the common casual user. And this is the kind of thing that Microsoft can do, invest in this kind of a large infrastructure and, like, ecosystem for a major feature, that it's really hard to compete with. I salute them. I think this is a tremendous feature. I think it's going to benefit a lot of users.

Leo: Of course we've got to hope they keep this database up to date. But I'm sure they will. Google does something similar. I mean, they'll let you know if it's a known site with some problems when you search.

Steve: Well, and I would imagine it's happening on the fly and automatically. No doubt it ties into the MSRT technology, to their own virus stuff, things you download, I mean, every time you download, it sends notification to the cloud. So we also need to be - once upon a time we would immediately twitch about this from a privacy standpoint. It does mean that your downloads are trackable, which needs to be remembered. I would imagine Microsoft has addressed it by obscuring this. But it does mean that files with a reputation are being checked. So your...

Leo: It doesn't need to be necessarily your download. It could be that, in the process of indexing pages - and I think that's what Google does. If they see malware, they add it to a database.

Steve: Well, but...

Leo: That means Microsoft would have to download everything; right?

Steve: This is you clicking on a link does send that act identifying the file you're trying to download into the cloud.

Leo: Yeah, that's right, yeah.

Steve: So it does mean that you can be tracked. The flipside is, for the common user, you're not having to be warned for files that have a good reputation.

Leo: Right. That sounds sensible. As long as they don't miss, well, I mean, it can give you a false sense of confidence, as well; right?

Steve: If there's no reputation established, then you get the warning. So it's only when...

Leo: Aha.

Steve: Yes. So it's only when a file's been downloaded a lot and then, like, no alarm bells have gone off, no antivirus has been fired, nothing bad has happened, then the cloud says, eh, looks like we're going to trust this. Oh, and it also knows where it's coming from. For example, I sign, I Authenticode-sign my Windows apps, and they're being downloaded from GRC. So I've already established a reputation for myself. So when I come out with a new piece of freeware, Microsoft already knows, oh, GRC, yeah, he's a good guy.

Leo: So the default is to no reputation, for a brand new file no reputation.

Steve: Correct. And then you're just - and that's the thing that Microsoft believes people will only see a couple times a year because...

Leo: I don't know about that. Aren't there a lot of, I mean, I don't know about that. I guess it depends on...

Steve: Well, but consider all the people who download Firefox in Windows. Every single time...

Leo: They're not going to see that, of course.

Steve: Right, right.

Leo: But, I mean, there are some sites that offer new files all the time. I guess if the site is - so you're saying, if the site has a reputation, it'll be okay.

Steve: Correct.

Leo: Yeah. That's interesting. Well, we'll see how it works.

Steve: Yeah. And then the last thing I had in my notes is the User-Agent header has been in IE9 dramatically cleaned up. Remember how bloated...

Leo: It used to be a lot of stuff.

Steve: Oh, my god, Leo. Remember every version of .NET that you'd ever run across in your lifetime, and then other things. I've got this Flash, I've got that, I mean, it had become increasingly long. And it was becoming a tracking problem because your browser, it was one of the things that the Panopticlick site glommed onto and said, oh, look at how unique this is. Who else has exactly this combination of versions of things? Because all that version crap in there, that's all gone. It now says Mozilla/5.0. They bumped it up from 4 to 5 because they are so standards compliant that they figured it was time, and they deserved it, and I agree. Then, open parens, it says "compatible" as it always has; and then MSIE 9.0, because they are; and Windows NT 6.1, meaning 7 because it really is Vista with some different candy coating, so Windows NT 6.1; and then Trident/5.0. Trident is their layout engine. And it used to be 4, and they've bumped that up to 5 for their latest standards compliant. Close parens, and that's it. There's nothing else. [Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)]

Leo: That just shows you how bad it was if that's cleaned up. But all of that information necessary for a web page to know because it's telling the web page how they're going to be rendering.

Steve: Oh, and I forgot to mention also that the do-not-track header does have an appearance in the Document Object Model, meaning that script running on the page can detect whether the do-not-track header is being used. So that allows scripts to be aware of whether the user is requesting no tracking so that sites could be preemptive if they said, hey, you're blocking resources that help pay our bills. We need you to please allow that for us.

Leo: Hmm, interesting.

Steve: So that exists there, too. So, overall, I'm impressed with it. It has caught up from a - largely caught up from a performance standpoint. It is, frankly, it's the standards leader at this point. And these standards are not easy to pass. I mean, if you've got something like Firefox 4, that is typically state of the art with following standards, still

failing 300 tests of ECMAScript 5, although it's 300 out of 10,456, and I looked through them, and they're not horrible game-changer things; and Chrome failing 497 of them, almost 500; but still IE9 only fails 17. Very impressive. So very standards compliant. We'll see how the tracking protection lists fare. A little bit of improvement in their security model, their layered security model. And some nice user-side improvements with the so-called SmartScreen Application Reputation for things that you download. Overall, I'm impressed. I mean, I'm staying with Firefox.

Leo: I was going to say, you're going to switch?

Steve: I love all the goodies. No, I'm not going back. And I can't use IE9 because I'm on XP still.

Leo: Oh, that's right, yeah. You know, I just love Chrome so much, I probably won't. But it's nice to know that you can, and it's safe. And remember, if you're using Windows, you're using IE9 whether you like it or not because Windows uses IE so often to render things, and many applications do, as well. So you don't get the choice in a number of situations.

Steve: Yeah.

Leo: Steve Gibson is at GRC.com, the Gibson Research Corporation. That's where SpinRite lives, the world's finest hard drive recovery and maintenance utility. You've got to have a copy if you've got hard drives. Go there to buy it. You can also get lots of free things at GRC.com, including free copies of this podcast in 16 or 64KB form, complete show notes, and he even gets transcriptions done so you can read along as you listen. GRC.com.

We've got the video on our site, TWiT.tv/sn. In fact, if you want to watch live, we do this show live every Wednesday at 11:00 a.m. Pacific, that's 2:00 p.m. Eastern time at live.twit.tv. And you're invited to stop by, say hi. Coming up in just a little bit, This Week in Google. And then we're going to interview Bob Heil, the microphone guy, who makes the mics you and I use...

Steve: Oh, cool.

Leo: ...on Triangulation. Yeah, Bob's in town, so we thought that would be fun. He's got some great rock-and-roll stories. That's coming up at 4:00 p.m. Pacific, 7:00 Eastern. Thank you, Steve. We'll see you next week.

Steve: Thanks, Leo.

Leo: On Security Now!.