Internet Explorer 8

Description: Steve and Leo closely examine and discuss Microsoft's just released major version 8 of Internet Explorer. Steve has studied this major new web browser closely, so he examines the many new features and foibles from the standpoint of its short- and long-term impact on Internet security.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-189.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-189-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 189 for March 26, 2009: Internet Explorer 8. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!. Are you ready? Fasten your seatbelts, put on your tinfoil helmets, and get ready to find out what the latest security issues are online and off. Mr. Steve Gibson is here. He's the king of security, the man who runs the Gibson Research Corporation, home of SpinRite, some great free software like ShieldsUP!. And he joins us - the guy who discovered spyware - he joins us every week to talk about it. Hi, Steve.

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

Leo: I always look forward to my old friend Steve. The second podcast we did on the TWiT Network was this show.

Steve: Yeah. And when you suggested it, I had never heard the term. I think Mark Thompson had used it once. And you said a - I said, a what cast?

Leo: A huh hah?

Steve: I mean, it just sounded like some, you know, pod person or something. It's like, what the heck?

Leo: Well, we are glad that you decided to do it. And you've been the most consistent podcaster we've had.

Steve: Oh, I'm stubborn.

Leo: This show is huge.

Steve: Once you get me going, you can't get me stopped.

Leo: Today.

Steve: When you first suggested it, I was thinking, oh, lord, I hope he doesn't ask me again.

Leo: I don't want to do it.

Steve: But it ended up, I mean, it's been the best thing. I really enjoy it. It requires some discipline. But I wrote the column, the weekly column for InfoWorld...

Leo: It's kind of like that, I guess.

Steve: ...for eight years.

Leo: Yeah.

Steve: And never missed one. Although I did have to shut the column down when SpinRite 3 was late because people were saying, hey, he hasn't shipped SpinRite 3. Why is he still doing a column? It's like, okay, fine. Good point. So...

Leo: Well, you don't do a column anymore.

Steve: Nope.

Leo: And SpinRite 6 is pretty stable, so...

Steve: Yes, indeed. We haven't changed a byte of code since release, in five years.

Leo: What? Has it been that long?

Steve: Yeah, '04.

Leo: I remember when it came out. Wow. And do you plan on doing a 7?

Steve: There are some things that I want to do. For example, Mac incompatibility is a problem.

Leo: Oh, we would love it if you would make this work on the Mac.

Steve: Mac's keyboard is, internally, it's a USB keyboard. And SpinRite assumes - in order to do the multitasking that SpinRite does, it can't use the BIOS for a keyboard. It needs to check the hardware directly in order to keep everything running at full speed. And so I'm literally talking to the PC hardware in order to allow that to - all the SpinRite work to happen in the background. And I can, you know, I've got new technology now, so I can come up with other ways around that from what I did originally 20 years ago. But, yeah, so there will be a 7.

I'm going to get a bunch of stuff that's backlogged at the moment. We will soon be talking about this very cool DNS benchmark, which is running now. But all the group, the guys in our newsgroups have just asked for a number of additional features that are just going to put some polish on it. That'll get done. Then we go, we finish up the spoofability stuff, which is all the technology is finished and done, just not yet public. Then the cookie stuff. And all of that's finished, but not yet public. And then I start serious work on CryptoLink, which I'm real excited about. So my plan is to end up with two products, CryptoLink and SpinRite, and then switch back and forth, moving them each forward over time.

Leo: Sounds great. Sounds great. So you're not done. Far from it.

Steve: No, I'm not done.

Leo: No rest for the weary. You don't get to do your PDP-8 programming for a while.

Steve: Well, I'll sneak that in. I've actually been relearning the 8, as I mentioned on the Gray-Haired Computing extra podcast that we did, and appreciating how cute it is. I did spend a couple hours over the weekend building one of the - the first of the three front panels for it.

Leo: Oh, that's neat.

Steve: So I'm sort of squeezing a little bit of time in for that, just because, you know, call that my "hobby mode."

Leo: You've got to have a hobby, dude.

Steve: Got to have a hobby.

Leo: All right. So today we're going to talk about the new Internet Explorer.

Steve: We're going to talk about - naturally from a Security Now! perspective. I mean, I don't care about new UI widgets, the slices, web slices and accelerators. I mean, those are nice UI things. My focus, as always, is what does this mean from a security standpoint? What features have they given IE, which of course IE has notoriously been, is now, the number one vector of infection for machines. So we'd like to see Microsoft hopefully moving IE forward. I've spent enough time with it, I've gone over all the developer notes, all of the backgrounders and all that. And I've got a complete readout for our listeners on IE8, and should they care.

Leo: Great. All right, Mr. G. What's the latest in the world of security?

Steve: Two little bits in security news. One I thought was really interesting. A botnet has now been found running autonomously in routers.

Leo: Are you saying it's an artificial intelligence?

Steve: Well, no. It's not a Skynet yet. Let's hope it doesn't go in that direction.

Leo: But you wouldn't think routers would have the juice to do that.

Steve: Well, it turns out that these routers that are Linux-based, they are running a Linux core. There was one where this botnet, about 100,000 of them, apparently, it's a router by NetComm called the NB5. And the problem with this is that for some length of time the router was being shipped with firmware that had the web interface and the SSH telnet protocol both open and exposed to the Internet.

Leo: Oh, please.

Steve: So, I mean, so it's a classic mistake. So they have this...

Leo: Was it a default password or something?

Steve: Oh, yeah, yeah. And in fact there was one version of firmware that needed no password at all, that you just connected to it by stumbling on its port. And of course, again, we were talking the other day about default, like the default port for SSH. And one of our - it was in the Q&A last week, in one of the - our listener who asked the question mentioned that he was running it on a different port. And I said, yay, that's important because - im-port-ant. Anyway.

Leo: [Laughing] Im-port-ant.

Steve: So this DSL router, it ends up being found by other bots in the net that are scanning; so it's a worm also. And they then leverage the web interface and the exposed telnet port to transfer themselves into it. They're not able to write themselves permanently, so they're just living in RAM. But this botnet agent is able to copy itself, spreading virally, like in a worm, really. There is, I guess, no verb for that. "Wormily" doesn't really work.

Leo: Yeah, I like "wormily."

Steve: Okay, "wormilate." So it just wormilates and worms its way across the Internet. And apparently where this was found, I mean, it uses standard IRC Chat to organize itself. And it's apparently about 100,000 routers strong at the moment. Now, the company NetComm has since fixed their firmware and closed these otherwise default open ports. Yet firmware is not something that everyone is updating all the time. And so much so that there's 100,000 of these that, even though the firmware has been patched, these particular routers haven't been.

If we happen to have any listeners who have this NetComm NB5, all you need to do is power cycle it, and that'll flush any worms out that may have crawled in. And you could use a port scanning site like mine, like ShieldsUP!, because when you scan with ShieldsUP! we will be checking your public IP, not your private IP behind the router. So we'll show you your own public IP. That's what we would check. And we would show you port 80 and 22, the telnet port, as being open by default. Unless your ISP is blocking that, in which case, you know, some ISPs are, like, do not allow you to run web servers. So they would be blocking port 80. So it could be open, but we would still not see it. On the other hand, nothing else on the 'Net would see it, either, except perhaps somebody who was also on your same ISP, depending upon where that port 80 filter was.

So anyway, you would want to make sure, if you had this NetComm NB5 router, make sure that you've got its WAN-side administration stuff disabled by default because some versions of firmware didn't do that.

The only other real news is I did want to comment that since our last podcast a week ago, Acrobat, Adobe's Acrobat and the Acrobat Reader, for the down version of Reader, that is, versions 7 and 8, now have updates. I went and checked and updated mine earlier this morning because they were supposed to have it done on the 18th, I think it was. I think it was the 11th and the 18th. The 11th for version 9, then they were waiting a week or being delayed a week to update versions 7 and 8. And I went there on the

18th and didn't find it. So anyway, it is there now for anybody who's still using Acrobat. You mentioned, Leo, that why not just update Reader? And it's because I've got the whole Acrobat package, not just the Reader. Anybody else probably would be served well to just update their Reader, although you can stay with 7 or 8 and now at least solve these security problems.

Leo: Very good.

Steve: Which brings up an interesting little side note. I recently accepted responsibility for an infected laptop. A friend that I set up about a year ago got herself infected on, it happened to be March 12 at 9:15 p.m., because that's the timestamp on all the infected files. And I found something really interesting. This was - she got herself infected by sort of a generic trojan downloader that downloaded a bunch of things.

What I found interesting was when, looking at what it downloaded, there was a Windows metafile. There was a PDF. There was an HTM file, or an EXE with an HTM extension. And in looking closely at them, basically this was a spray of all recently known openings in Windows, but all with the same agent, the same infectious agent. So essentially this was a spray at the machine, looking for any porous openings in the configuration and patch level and security of the laptop. And something got in one way or the other and grabbed her laptop. I thought it was interesting to see, like, a PDF with the most recent PDF hack, and the Windows metafile hack, and all the different things we've talked about. This thing was, whatever it was she did, was spraying her machine, like, trying to find a way in. And unfortunately it did.

Leo: We've talked about that before, that these companies in Russia sell kits, exploit kits, with a bunch of exploits in them. And they put them all in one web page. And if you happen to hit that web page it's going to try everything because maybe you patched this, but maybe you didn't patch that.

Steve: Exactly.

Leo: And of course, if she hadn't patched anything...

Steve: That would have had a field day.

Leo: I guess just all of them come in; right? Holy cow.

Steve: In classic errata, I misspoke, I think it was last week, one of the Q&As, I mentioned that SSH used SSL. And it's not the case. SSH has its own transport. The reason I got confused was that TLS is Transport Layer Security, and SSH calls their protocol Transport Layer Protocol. So it's like, okay, let's for the record make that clear, that SSH is not using SSL tunneling. It's got its own, which is also secure and has virtually the same set of protocols and operation. And fundamentally it is SSL, but not formally. It has its own.

Leo: It's using - what kind of encryption is it using?

Steve: Oh, it's got, in the same way - and we'll be talking about SSL protocol here very soon, as I've promised. SSL has, like, a dictionary of encryption, as does SSH. So there are mandatory encryption, for example, Triple DES is a requirement for SSH. But you might also have 128-bit, 192-bit, or 256-bit AES. And so the endpoints are able to negotiate dynamically and say, here's the encryptions that I know about. Which do you know about? And then they end up, like, choosing the strongest that they both know about in order to - and that's a negotiation performed on the fly at the connection initiation.

Leo: Okay.

Steve: Another little tidbit is every so often I find a fantastic little piece of freeware. And people have said, oh, Steve, you should do that all the time, or tell us what all your freeware is. And it's like, well, I tell you the good things I find. I found AllSnap, that I love, where it snaps, for Windows, it snaps the borders of windows to other windows or to the screen, which I really like for quickly aligning things. Then more recently I told everyone about KatMouse, which has this wonderful effect of automatically scrolling with the mouse wheel whatever your mouse cursor is floating over, without having to click in the window in order to bring it to the top or make it current, you know, in order to give it so-called focus. It automatically sends the scrolling of your mouse wheel to whatever you're hovering over, which is great.

Well, I don't know what it was that I was looking for, but without really intending to I stumbled on something else which I absolutely love. It's an add-on called Prio, as in priority. And the author's focus is to allow you to assign sticky process priorities to things. For example, if you wanted to make sure that you didn't have a low frame rate in Skype, you could increase the priority of the Skype process, and this thing would remember it.

Now, you can use Windows Task Manager now to change the priority of processes. And this is something that Windows really does obey very well. But when you close that process, the system has no sticky memory of that. Well, what I like about this is that it goes far beyond just that, because that doesn't really excite me that much. But it does a bunch of interesting things from a security perspective. It is a very small DLL. It's like 200-some-odd K DLL, which functions as an extension to Windows Task Manager. So you install this, and you don't really notice anything happens until you restart Windows. Then when you run Task Manager, it has added two tabs to Task Manager. In the normal process view, which is where I spend a lot of time, like just sort of in order to enumerate all the processes that are running, see how much memory they're taking and so forth. It colors them based on whether they are signed or not. So you're instantly able to see everything green has a valid digital signature. Anything red does not. So that doesn't mean that it's evil, but it just means that, for whatever reason, it hasn't been digitally signed.

Leo: Nor does it mean it's not evil. I mean, just because it's digitally signed doesn't mean it's completely safe. You just know who it came from.

Steve: Exactly, exactly. Then the other two tabs are really nice. One is a services tab. So you're able to instantly look at all the services that are running, similarly colored with green and red. And, you know, non-signed services are much more rare than non-signed executables. And so there it's like, oh, wait a minute, why is a service that I've got not signed? I just clicked the tab as I was talking, and I noticed that Parallels' DHCP service for virtual NIC is running. Well, first of all it's not signed. But now it's like, wait a minute, why do I even have that running, taking up a chunk of my machine's resources? So after this podcast I'm going to go disable that. Which you're able to do from this interface also.

And then the last thing, the last tab it adds is a TCP/IP monitor tab, that is, essentially a real-time netstat that shows all of the connections that - all of the IP connections your system has, the state that they're in, which processes are using them, and whether those processes are digitally signed or not. Anyway, I absolutely, for people who've been listening to this and saying, hey, that kind of sounds like a good thing, I recommend this without hesitation. It's a very cleanly written, very small, lightweight, not loading down your system, little add-on. And, I mean, it's really enhanced my Windows Task Manager.

Leo: Very cool.

Steve: And my last little bit before we get to the topic is I found a really fun little blurb about SpinRite from someone who asked me not to say his name for reasons that he makes...

Leo: A spy?

Steve: No, he didn't want to embarrass the person who he helped with SpinRite. Actually he sent this on January 1st, 2009, so a couple months ago. And he said - "SpinRite Eases the Path to Retirement" was the subject line. He said, "Hi, Steve. In the unlikely event that you do choose to read this out on Security Now!, I'd appreciate it if you could avoid mentioning my name. My location is fine to reveal." Oh, he's in Toronto, Ontario. He said, "To avoid embarrassing the friend who is the subject of this piece. Thanks." Although actually his friend's name I don't think was revealed, so I don't know if she's someone who listens to Security Now!. But he said, "As a longtime Security Now! listener and a computer user since roughly the dawn of time, I'm suitably paranoid about pretty much everything I do with computers. Which is why I've always detested Outlook's way of lumping everything about your email into a single file. I've never been able to shake off the worry. What happens if the file gets corrupted?"

Leo: Oh, I agree.

Steve: Oh, yeah, I mean, it's bad.

Leo: It's the main reason I don't use Outlook is that big old Outlook.pst file. It's just a bad idea.

Steve: Well, and, for example, Eudora. I use Eudora, and every folder is a separate file. But it's a plaintext file. You're just able to, like, scan through it and...

Leo: And it's a standard Internet mbox format, so other programs can read it. I mean, this is how it should be done.

Steve: Yup. So he says, "What happens if the file gets corrupted?" So I've stuck to programs that don't put all your eggs in one basket, like Eudora and, lately, Thunderbird. Well, eventually it happened, but not to me, to a friend who just retired from a firm she founded 20 years ago, and which had recently been sold to a multinational. She needed to move her email archive over to her newly bought laptop before her old one went back to the company. Easy enough. Copy it to a USB storage device and then set things up as they should be. Except that the 1.4 GB .pst file" - which is what Outlook stores as a single, monolithic file that we talked about.

He says, "The .pst file containing all the email wouldn't copy. It returned the dreaded CRC check error. Was there a backup copy of the file? Of course not. Despair and gloom pervaded the establishment. My wife and I were helping our friend and her husband celebrate her retirement and New Year's Eve at her cottage deep in the country amidst the snowdrifts. Just the way of spending New Year's Eve that we all seek out, contemplating the loss of one's email archive stretching back many years. Happy New Year." He says, "You can guess the rest, of course. It may have been a cottage, but it had an Internet connection. So I was able to purchase and download a copy of SpinRite and mount it on a small USB drive that I happened to have in my bag. I've been SpinRiting my hard drives for years, but this was the first time I'd seen it actually find a problem." That's because he's been SpinRiting his drive for years. You know, we've talked about it before preemptively and as preventive maintenance.

He said, "...actually find a problem. DynaStat kicked in and worked away, converting dots" - oh, and says "...worked away and recovered most, not all, of the data. In other words, actually do something other than just plod through the sectors, converting dots to shaded rectangles. Very exciting. And as the New Year arrived and the champagne cork popped, SpinRite finished its work. Lo, the PST file now copied without trouble. My friend's retirement could begin. Thanks for a great product, and thanks to you and Leo for such a stimulating and informative webcast series."

Leo: Oh, isn't that nice.

Steve: Yup. Happy New Year.

Leo: Happy. You know, there's one question I want to ask you before we get to IE8, and it's off the cuff. I just noticed this, that April 1st is a special day for Conficker, and we don't - I don't think we know what Conficker is going to do on April 1st.

Steve: Ooh. So it's got that date built into it.

Leo: Yeah, apparently it does. And I just wondered if you knew anything about it or had anything to say about it because it's going to happen before our next episode.

Steve: Actually, no, it happens on our next episode. So...

Leo: We'll have to - we can talk about.

Steve: Oh, no, no, you're right. We're recording on the 1st.

Leo: Yeah, we record on the April 1st. And you'll hear us talk about it after the fact. I guess there's nothing much to say except that this would be a good time, if you've got...

Steve: So it's an April Fool's - Conficker knows about April Fool's.

Leo: You might want to scan your computer.

Steve: Oh, and speaking of which, Leo. When I scanned this laptop belonging to my friend, I used both AVG and avast!.

Leo: Both free.

Steve: And avast! found more...

Leo: Interesting.

Steve: ...than AVG, substantially more. That is, there were - it was the - I mentioned the spray, as I termed it, where the same agent had been encoded in a PDF. It had been scrambled in some JavaScript. It had been stuck into a Windows metafile. Those various ob- obscurations?

Leo: Yeah. Obfuscations?

Steve: Obfuscations, that's the word I was looking for. Those obfuscations eluded AVG. In both cases I set them up to scan slowly but surely, like take your time, do everything you want to. And so I did the avast! scan separately. And it found about 50 percent more than AVG did. So, I mean, that's anecdotal. It doesn't mean anything conclusively. But I thought our users would appreciate knowing that in this case avast! came out ahead. And, I mean, I'm glad to know that those other things that were missed by AVG were found by avast!.

Leo: Lately a lot of people have been saying that they prefer avast!. I've been hearing that a lot from people. I'll have to take another look at it. Because I think it comes and goes, you know, AVG was better for a while, and I think avast! is now. I still prefer ESET NOD32. But I'll send you - actually you can download a free copy. I'd be curious if you see anything different from that.

Steve: I'm going to run - I want to try the MSRT scan that we've talked about, the really deep deliberate scan. And I made several backups of her...

Leo: Oh, good. I was going to say, this is good, you can keep an image of her drive and use it as kind of a test bed for these guys.

Steve: I'll do that. I'll report next week.

Leo: Oh, good. Good, good, good. So let's get to the matter at hand: Internet Explorer 8.

Steve: Yes, well, this is the first major update since IE7, which happened in October of '06. So a little over, like, almost two and a half years we've been living with IE7. And in fact IE8 has been in beta for just about a year. And it's interesting, too. When I was thinking about this, I thought, you know, we didn't - on this show we didn't mention that the 20th Anniversary of the Web had just recently occurred, a week or two ago. The World Wide Web turned 20. At that time IE turns eight.

Leo: Well, actually that's clever.

Steve: So but actually not eight years, but at least eight...

Leo: Eight versions. I'm trying to think, let's see, I first - IE, because I remember I did an editorial on the site in 1995, when IE3 came out, saying watch out Netscape, Microsoft's here.

Steve: On the march.

Leo: On the march. And if I were you I would sell my stock. Which kind of irritated Marc Andreessen, as I remember. But it turned out to be right. So 3 came out 14 years ago.

Steve: Wow.

Leo: IE1, I don't know when it came out. But it must have been, I think - didn't they buy - they bought Spry's code. I can't remember whose code they bought. They started with a code base. It was either Mosaic or Spry's browser. Do you remember that?

Steve: I think I remember it being Spry, yes.

Leo: And that would have been - couldn't have been earlier than '93 or '94.

Steve: No.

Leo: So it's probably 15 years old, 16 years old.

Steve: Yeah, it's funny, I had an occasion to fire up Windows 98 the other day. This forthcoming DNS benchmark, which has revealed some really cool things, Leo, about, for example, routers you don't want to have doing your DNS proxying because, well, we learned that it's possible to crash them, but also they just tend to slow things down, and they're unreliable as a DNS proxy. But we'll be talking about that when I talk about the benchmark. But it was because there was some - I think there was something, oh, I know what it was. I had, in the intervening years since I've been programming '98, I had changed the way some of my Windows API code works. And this benchmark is heavily multithreaded, and there's some parameter changes between XP and the NT-flavor OSes and the older 95/98, so that this thing wasn't working on 98. So I fired up 98, installed it in a VM so that I could contain it and work with it. I had the most interesting feeling, though, using it. And that was, you know, for all of the movement that Microsoft has made all this noise about, really not that much has changed.

Leo: Yeah.

Steve: I mean, you look at 98, it's like, oh, everything's sort of in the same place.

Leo: Kind of familiar.

Steve: The way I remembered it. And it was like, wow, how long ago was that, and why does it not seem that different from XP at the moment, which is where I still am. I'm not over on Vista. Where I guess things really have begun to look a lot different.

Leo: Vista and then 7 are very, very different. But one of the things that makes Microsoft successful and one of the things that's always been a benchmark for them is downward compatibility, supporting legacy. So they don't, because business users are their primary market, they really don't want to change too much from version to version because they don't want to have to do a lot of retraining. By the way, I found a page on Microsoft's site written by Sandi Hardmeier called "The History of Internet Explorer." They bought Spyglass's code from Mosaic.

Steve: Spyglass, that was it.

Leo: In 1995 they licensed the source code from Mosaic to Microsoft. The first version of Internet Explorer was not released with Windows 95, but came out later with the Plus pack.

Steve: That's right.

Leo: And then they put out something called the Internet Jumpstart Kit, and then the Internet Connection Wizard. So it is - actually it's only about 14 years old.

Steve: Wow.

Leo: Just so you know.

Steve: Well, so we've got a new IE8, and I want to talk about the things our listener base cares about. I did hear you and Paul talking about, from a feature standpoint, the web slices, which are like little mini pages that IE will automatically poll on remote servers, looking for any changes, and then alert you to those, and various other sort of UI things. But of course my focus is, okay, what kind of a job have they done from a security standpoint? And, you know, security and privacy.

It's worth mentioning that, unfortunately, it is still the slowest browser among the top five on the 'Net. Chrome comes in as the fastest in running the SunSpider JavaScript benchmarks; Firefox in number two place; Safari, surprisingly, in number three; and Opera in number four position; and IE8, number five. Now, Microsoft makes a bunch of noise about how fast it is and that it's the fastest. It turns out that that's - apparently it's in their testing a little bit faster than something else, not in script performance but in dumb page rendering, which that's valuable, but we're becoming so script happy these days that JavaScript rendering speed is important. Chrome just apparently is way faster than the rest of the pack, really. Firefox is 59 percent faster than IE8.

Leo: I should point out that there's a Firefox 3.1 data that is considerably faster than 3.

Steve: Oh, good.

Leo: Yeah. So they're paying attention to this. And Safari 4, which is also in beta, is paying attention to this, and the new WebKit is. So I think they're all in the pack. You know, one of the things Paul Thurrott says is, yeah, IE8 is, what did he say, 50 percent slower. But it's all in milliseconds we're measuring this, remember. It's pretty fast.

Steve: And the fact is your local rendering time is much less significant than your roundtrip packet travel time. So it's like, yeah, okay, you can demonstrate this. But in terms of the user experience, when I was using IE8 to poke at it, it seemed very snappy to me. And that was even then in a VM, in a VMware virtual machine running XP. It's like, okay, this is - it was working well except that I was able to crash it repeatedly, which we'll talk about in a second. So one of the things that I saw, that I heard you and Paul talk about, is the so-called "compatibility view."

Leo: Yes.

Steve: I was nervous about IE8 and when it was going to matter on the Internet because my script-free menuing system at GRC had been broken under all of the betas. And so I was thinking, okay, I'm going to have to go in and do something. It had a weird effect where the menu items were spaced out by, like, a blank line of blackness. And it was like, okay. And I had seen that on a couple browsers during the development of the menuing system, which tended to be highly browser specific because browsers are still, you know, there is no standard. I mean, I'm really glad that at least Microsoft has made so much noise about IE8 being more standards compliant than any of their previous browsers because I had to do a bunch of things under specific versions, prior versions of Internet Explorer in order to make them work the same way that Netscape and Opera and Safari worked. So this is generally a good thing.

The way it works is interesting, too, because I'm sure you know from having spoken to Paul that Microsoft has broken many websites, sort of like my menuing system, which had adapted themselves to the fact that prior versions of IE were not very standards compliant. But the good news is that whatever it was that was broken for me, that was broken with GRC's menuing system under the betas of IE8, they got fixed. And I checked, it's not because Microsoft special-cased GRC.com. It's that it was a problem which they fixed, and so it was fixed naturally. And I did find one strange little rendering anomaly when I was checking IE8's cookie handling, which is still broken, as was IE7. It turns out you're unable to block all third-party cookies, even if you tell it that's what you want, which has been persistent...

Leo: You'd think by now they would have fixed that.

Steve: I know. Well, I haven't made a big bunch of noise about it. And in fact my planned noisemaking has been delayed by this work on DNS because one of the things that I'll be doing is really drawing attention to the fact that no versions of IE allow you to block third-party cookies.

Leo: Remember that Firefox said we can't do it anyway, so remember they took it out for a while?

Steve: Yeah.

Leo: Saying because it's broken or something. So maybe that's Microsoft's point of view, too, is...

Steve: Well, no, this is - the way this is broken is different. What happened with Firefox was they took it out, and it was my cookie pages, which are soon to be public, made them put the switch back in.

Leo: Aha. Good for you.

Steve: Yeah, because they knew that people were going to - you had to go through that weird about:config and then bring up that whole page of stuff, and then type in c-o-o-k to find only the entries about cookies, and then go change some random, I mean, it would have been a real pain for people to fix this. But we're going to shine a bright light on this. And it turns out that IE is among the most broken of the browsers in terms of cookie handling. But anyway, I did see a rendering anomaly which I was able to fix by putting it into compatibility mode. What compatibility mode does is it causes you to fall back to the IE7 rendering engine, which is the non-standards, or less standards compliant, I don't have any idea how standards compliant IE8 is. They say they passed the Acid2 test. Does that matter, Leo?

Leo: It is a compatibility test. It's a very difficult test, and a lot of - no browser, to my knowledge, does it a hundred percent. So, yeah, it's important. It's a CSS test, so it is - I think there's an Acid3 now.

Steve: Well, I'll be interested to find out what this one little rendering deal I saw was because it's - I have used a lot of CSS in my newer pages. And so something's strange. So I'll track that down. But...

Leo: It's done by the Web Standards Project. So, I mean, it is, it's the one thing I know of that you can really test...

Steve: Well, so that's a good thing. And I'm glad they're finally doing it. And they had to bite the bullet in order to make IE8 standards compliant because, as we've just been saying, they've broken thousands of web pages on the 'Net. And so what they have is they have a built-in list of known incompatible web domains. And when you go there it automatically drops your IE8 back down to use the IE7 renderer. In addition, there's a little button, showing like a cracked page button, which you're able to toggle at will on whatever site you're at. So if you went to a site that looked like stuff was not looking the way you'd expect it to, you can just press this little button, and it drops it from IE8 into IE7 mode and then refreshes the page, which will probably cause the page to look correctly. The nice thing is that the browser then remembers that that domain needs, apparently, to be rendered in IE7 mode, and that's a sticky setting. And I found myself thinking, oh, why couldn't they just do this with scripting? I mean, okay, here they're breaking pages, and then you push the button to fix it. Well, that's the same as turning off scripting.

Leo: Sure, sure.

Steve: And you push the button to fix the page.

Leo: Right.

Steve: So it's like, okay, well, that's all I would ask for in an IE. Maybe we'll get one one day. But so I'm still over in Firefox mode with the NoScript add-on because it allows me to do that.

Leo: Somehow I doubt that's ever going to happen.

Steve: I know. I don't think so. Not from a mainstream browser. But they have done one amazing thing that I will get to here. One of the things that they have done is they have enhanced the Delete Browsing History. You are now able to surface a whole bunch of buttons on their little toolbar. So, for example, Delete Browsing History, you're able to say I want to add that to my toolbar. What they've done, though, is that you can optionally accept, that is, make an exception for any of the sites which are in your favorites. They've renamed their Links is now Favorites. So they sort of merged the terms. So what they used to call Links is now - everything is just called Favorites. And so you can optionally cause any sites that you have in your Favorites tree to retain browsing history; whereas Delete Browsing History then gives you some granularity on what kind of things you want to delete - cookies, past history, form content, and a bunch of different things. You're able to turn those on. So they've made that very nice, which is good from a privacy standpoint.

Of course the popular feature is the so-called - they call it In Private browsing, which it's funny, as I was reading some reviews and getting some more background, I saw one writer referring to it, it's like "a.k.a. Porn Mode," as he called it. And essentially what this does is this causes the browser not to write anything permanently to the system, to keep it all internally while you're doing browsing. So when you click that button - and it's easy to, again, make a little button, or you can find it in the tool menu, when you click it, it essentially opens - it clones the session, opens a new window that very clearly labels itself as In Private.

And as they say, what happens in Vegas, stays in Vegas. Well, what happens in this window stays in this window. No trace of any sort is left behind. And in my testing I verified that. I could not, like, this is not super deep, I'm absolutely sure. But all the things that I did, watching my system very carefully, especially playing with cookies to see whether the leakage that Microsoft has was leaking out of that, and they weren't. So it really does look like they've got good containment using this "In Private" browsing mode.

Okay, now, the thing that they did that I am more excited about than anything else is something that they call In Private filtering. In Private filtering, I'm surprised they did this. It's not on by default, so you'll have to turn it on by default. And I should have said already, I'm not advising anyone use IE8 yet. The good news is Microsoft's not pushing it. They're not, I mean, literally pushing it. It's not part of Windows Update or Microsoft Update. I'm hoping they wait awhile before they do that because, well, most users, typical users won't know about it until it arrives automatically, until Microsoft decides, okay, it's time for us to push this out to everyone.

The reason I'm not suggesting that people use it is that it's a browser. You never want to use the initial release of a major update of a browser. And it's already been hacked. The first security vulnerability has already been found. Proof-of-concept code was demonstrated. I don't know if that code is on the 'Net. But I do know that Microsoft has been informed. They have repeated the problem, and they've acknowledged it. So now they're in their standard, oh, well, we're examining this, and we'll let you know what happens. But so we already have the first security vulnerability in IE8.

So there's no hurry to update to it. There are, I mean, I like this very much as an improvement over IE7. So when it's matured enough, when it's stabilized, I mean, again, we're going to be finding problems with it, I'm sure. But then we're still finding problems

with IE7, so it's not like that's any big change. But there are some features that I think really make this worthwhile. This In Private filtering is top on my list of what I love. If you turn it on - and it's not on by default. But if you turn it on, the browser, IE7, running in both In Private mode and not - so this In Private filtering is different than In Private browsing. So this is the normal default browsing behavior. It looks at third-party content as you browse the web. And if it sees that you are going to multiple sites, and those sites are receiving - you're receiving the same kind of third-party content from the same third parties, at some point of multiple hits it blocks it automatically. You choose how many sites, how many times you have to encounter it before the block occurs.

I wish it would let you set it lower than three. But three is not bad. You can choose between three and 30, and the default is 10. So if you turn it on, a privacy-conscious person will probably crank it down to three. And I experimented with this. I turned it on, set it to three, and then I went around to places I figured were going to be giving me junk. You know, MSNBC, Wall Street Journal, CNBC, CNN, Disney. I just chose a whole bunch of sort of messy third-party junk coming at you from all directions sites. And sure enough, I quickly accumulated a bunch of debris.

There was one called 2mdn.net, which is owned by DoubleClick, which of course is owned by Google. On many sites there was something called flashwrite_1_2.js. Okay, well, we know what that is. That's doubtless a technology to create persistent tracking by writing cookies into flash cookies. And this is a little .js JavaScript that is running in browsers. So after having encountered it three times on different sites, IE stopped requesting it. It started blocking it, all by itself. I ran across two things from GoogleSyndication.com: render_ads.js and show_ads.js. DoubleClick.net had something called test_domain.js. I remember dissecting that some time ago and seeing that it was basically DoubleClick probing the settings in your browser to learn about it. That's why it's called test_domain. And then it was sending information back. So again, blocked after having encountered it for the third time. GoogleAnalytics.com was running ga.js, obviously "ga" for Google Analytics. And Quantserve.com was running quant.js. And this is just - this I was able to cause to happen in the course of about four minutes.

So this is a very cool thing. And what I like about it is it actually shows some innovation from Microsoft, which we rarely see, in this space especially since they seem so determined to be Luddites in terms of browser technology. Their theory is that, because pages are now often deliberately mixing content, the so-called "mashup" pages where, I mean, for example, you go to MySpace or Facebook or something, and there can be applets which are scripting, which are part of the page being sourced from another server. Well, the question is, is that bad? Is that privacy impinging? Or is that something that you want?

And so Microsoft's concept is, okay, if we set that to 10, so that you would have to encounter the same thing from the same source in 10 different domains, well, the idea is that's unlikely to happen for something that's, like, an add-on to Facebook or MySpace or something. Typically only that domain, MySpace, would be sourcing a so-called "mashup add-in" in the form of some scriptable agent from one other given site. So it allows that, even if you've got this thing cranked all the way as tight as you can to only - to block after three different events. So it would allow it by default. But things that are truly tracking sorts of things, like all these DoubleClick events and Google Analytics and Quantserve, for better or for worse, those that are being sourced, spread across the web, and they are for the purpose of tracking, IE will adaptively block those. Which I think is spectacular.

Leo: So it sounds like you think this is a good, secure update.

Steve: Well, I think that this is a - I would call this a welcome feature. So that's the In Private filtering feature of IE8. Now, I'm not leaving Firefox. But IE still has a 65-plus percent market share. So more than two thirds of the world are going to be using IE8. Now, unfortunately this is turned off by default. But for people who for whatever reason want to stay with IE8, it's easy to turn this on and to crank it up to maximum intolerance, which is to say set it to three repetitions. And then it's also kind of fun, the reason I know all these things are being blocked is that there is a nice user interface where you're able to see that.

And if you decided, hey, you know, I want Google Analytics, that's something I don't want my use of the Internet to block, you're able to go in and not default block, but to choose from this growing list of things it finds. You can say I want to allow ga.js, and Google Analytics will be allowed to run as you roam the Internet. And you might want to say I want Google's ads. So you can turn on render_ads and show_ads to turn that system back on. So, I mean, they've really done a very nice job. But you are also able to say block by default after you enable it, which is not enabled by default. So that's a good thing.

Now, they have an adaptive heuristic reputation-based approach also. They have something called Smart Screen Filter. This is a whole bunch of new terminology that over time we'll become familiar with. But their Smart Screen Filter gives you on-the-fly site warnings based on Microsoft's own reputation database. There's a local cache that grows in your browser of known okay sites. So, like, because generally users are going to many of the same sites all the time. So if your browser doesn't know for sure that some domain is all right, then it'll ask Microsoft, hey, do we know anything about this? If it's known to be a disreputable site, you get, I mean, the whole world turns red in front of you. You just about fall off your chair. There's no way to miss this now. The whole background goes red, and a pop-up comes up and says, eh, this would be really unhealthy if you go here. Otherwise, as you roam around, your browser will learn that Microsoft thinks most sites are okay, and you won't be seeing this. So it won't false-positive. But it's another nice layer of warning to help prevent people from going to sites that are known not to be safe.

Now, we know how I feel about ActiveX. ActiveX is, like, the worst idea that ever happened. It's right up there, it is, it's just a horror. I mean, look at all the problems that we have with ActiveX. Basically it's DLLs for the web, which says, oh, yeah, let's - without asking the user we're going to download and run a DLL. Well, in IE7 we finally got "ask the user." That was that little bar that you see, the little yellow bar at the top that sort of drops down and says, this site is trying to run an ActiveX control. And most of us see that when we do a fresh install on a system because we'll go to a site that wants to run Flash, for example, the Flash Player, which so many sites are now using. So it's like, yeah, it's fine, install the Flash Player.

Well, what's interesting is there's more granularity now. Microsoft allows you to allow ActiveX controls to run only on specific sites. So, for example, as I was doing this it immediately wanted to install Flash Player. When I looked in the permissions, and it's like, oh, do you want to allow this to be run on all sites, or only this site? So there's per site granularity, and there's also now per user granularity. So you don't have to globally permit everybody on a computer to run something. You're able to say only allow myself to run it, but not others. So that's nice.

They've also got a really enhanced UI for managing add-ons which I really appreciate. It used to be that you sort of got a rather terse list of things, sort of like Microsoft was thinking in IE7, they were thinking, well, I guess we really have to show these to people, although we'd rather that they just left it all alone. Now there's a whole Explorer user interface with categories on the left and lots of information. You're able to right-click and look at properties to see where this add-on lives, when it was installed, what the status is. And in fact they also show you how long ago it was activated to give you some ability to understand why something is so slow all of a sudden. Because it might be that an add-on which is able to insert itself into the whole UI experience with the browser, it might be poorly written or be having problems and causing your browser to have various slowdown problems.

One of the other things that they've done that I appreciate is they highlight the domain name. So if you put in, for example, www.GRC.com slash anything, everything except GRC.com is light gray, and GRC.com stays black. Or Microsoft.com, or Windows, or Leoville, I mean, whatever. The browser recognizes the domain name and highlights that in the URL, which has the effect of helping, again, to prevent people from being fooled by domains which are compound, where for example it'll say PayPal.com.something or other, and then .evildomain.ru, where people will look, and they'll see PayPal.com and go, oh, good, I'm on PayPal. When in fact that's four layers of subdomain underneath evildomain.ru. So the browser isn't fooled, of course. But people can be visually fooled.

So what IE8 would do is it would render everything except evildomain.ru in light gray. Evildomain.ru would be made black. And so your eye just automatically goes there. And that's, again, I'm liking all of this. It's like Microsoft has really sat down and said, okay, here are the problems people are having. And these are not just with their browser. This is browsing in general. It was not designed for safety, unfortunately. Safety and security wasn't even a consideration when this was all being originally created. So it's nice that they've done that.

Also, all of the toolbars, any toolbars that you load into IE, or which load on you, because it's so often the case now that you download software, and if you're not really paying attention, oh, yes, install the Google Toolbar will be...

Leo: Yeah, I hate that. I hate that when they do that.

Steve: Oh, it's so annoying.

Leo: So frustrating. You have to really watch closely. A lot of people do that now.

Steve: Yeah. The good news is there is now a regular little X, red X Close button to the far left of every IE toolbar. And just for the heck of it, I did install the Google Toolbar, wondering if that was a per toolbar thing or not. And it's not. No toolbar has control over it. So every toolbar gets it. And so it's easy to just say, whoops, I don't want that. You just click on the little Close button. That pops up a dialogue that then allows you to determine how sticky you want this to be, to disable it and any of the components that it invokes, as well. So that was a really nice addition.

So, oh, and big deal, in IE8, unlike IE7, under Vista, and Windows 7 as well, DEP, the Data Execution Prevention, is finally enabled by default. And that's a wonderful improvement. Microsoft is slowly creeping this stuff forward as they gain experience with

it. So IE7 under Vista has the option of turning on Data Execution Prevention, which is a substantial benefit on modern processors. That uses the so-called "NX," the No Execute bit. We've talked about it extensively in the past on Security Now!. And it goes a long way to preventing buffer overrun-style mistakes, the idea being that, well, and the idea being that you don't want data to be executable.

And so for example we've recently had these problems with PDF files and with image files, JPGs, for example, that are leveraging the rendering engine of the image, or the page has a problem. So essentially the data space is executed. So people are able to put code in an image and cause it to run. Well, not if you've got Data Execution Prevention enabled. The problem is it's disabled by default in IE7. It is enabled by default in IE8. And that is a huge win for long-term browser security. So that's - we don't get it under XP. We have to wait for Vista. But of course a lot of the world is either on Vista or getting ready to move to Windows 7. So that's going to be another really big deal.

Now, in addition to saying don't use IE8 because it's new, I have to say I would be skeptical about it because it's so crashable. During my brief testing of IE8, because I'm not living there at all, I crashed it a bunch of times. In fact, I can't get it to display The Wall Street Journal WSJ.com site, and multiple pages there, deliberately. I wanted to play around with its tab grouping features, where if you open a tab from another one, like you hold Control down when you click, that says don't switch this page to that URL, open another page. Well, IE claims as a feature that it opens the new tab immediately to the right of the current one, which it does, and that it calls those "similar tabs," and it colors them in order to visually group them. Well, I wasn't really able to get very far with that test because on the third one that I opened it just completely crashed the browser.

Now, the browser has got anti-crash protection. One of the features from a user standpoint is that they're saying that they are - that individual tabs are running in their own processes. So if a tab crashes, then it only crashes that one tab. I saw the browser trying to do that. I got a little popup notice, a little balloon that said this tab crashed. Actually I wrote down what it says. It says, quote, "This tab has been recovered," unquote. The second line: "A problem with this web page caused Internet Explorer to close and reopen the tab." Unfortunately, it tried. I don't know if it got in an endless crash loop or what. But it never came out of that condition. The processor showed 100 percent CPU utilization. And the whole UI was destroyed. I forced it to die. And then when it came back up it tried to reload. It asked me if I wanted to reload all the tabs that I had. So they've got that sort of like crash recovery stuff. But when I said yes, it all crashed again.

So it's like, okay, I don't think we're quite ready to have everyone in the world be using this. I like the fact that you can reopen a tab that you closed by mistake. I sometimes click Close on a tab I didn't mean to. And it's like, ooh, shoot. And Firefox allows me to do that. IE has that now, too. And they say that they've got really fancy zooming, which I haven't had any experience yet with. But apparently you're able to adaptively zoom a page, which would be nice because one of the machines I use has an 800 pixel horizontal resolution, and sometimes I'm scrolling from side to side a lot. Apparently this is designed to prevent that from happening, if you want to zoom in, or if you've got a reduced-resolution page. So lots of good things.

And lastly, they've got some very nice support for development. They've got a built-in set of development tools which, for example, allows you to obviously view the page source. We've had that from the dawn of the Internet. But it's really nicely formatted now. And you're also able to browse around in the so-called Document Object Model. And so they have a built-in DOM viewer that allows you, as a web page coder, to look at the page from that standpoint. There are third-party tools that allow that. And Microsoft has

even had some of their own add-ons. But normally they are, well, they've never been built in before. They are in IE8.

So there's the whole IE8 story. There's a couple things about it that I think they've really done a good job with. I mean, in general they're moving this forward. They've still got some - they've obviously got some problems. But I really very much like this In Private filtering notion, the idea that, adaptively, if they see you encountering the same add-on script in multiple sites, they will adaptively shut it down to prevent you from being tracked, which is very cool. They've made it easy to flush your history. And this In Private operation where you're able to - the so-called In Private browsing, where you're able to open up a window that retains no memory at all of what you do, those are all very cool features. And a lot better control over ActiveX, although we still have ActiveX. We're suffering with the never-ending problem of that security.

Leo: Yeah, yeah. Well, you can't - they'll never get rid of ActiveX. Too many things rely on it.

Steve: Yup, yup. And as you say, they will never get rid of scripting completely. So it'll probably be Firefox. I mean, again, you can do what I used to do when I was under IE, which is you're able to use the Trusted Zone to enable scripting, and let the Internet Zone have scripting disabled. So you can get some of the effect of Firefox. But we've got Firefox. And Firefox has a mature ecosystem of add-ons. It's doing much more for you, I think, than IE is. And it's still, Firefox without question is still, in my opinion, the more secure browser.

Leo: But as you point out, IE is the default browser for the world. So as Microsoft goes, so goes Internet security. So I'm glad they're at least paying a little attention to it.

Steve: Right. And so ultimately, when they end up moving this to Windows Update so that everyone starts receiving it automatically and updating themselves, all the 7s will update to 8s. And to the degree that the default settings are useful, and I think these default settings, there's more attention to not letting users, not letting inattentive users get fooled. This will move the security bar further along and in general be a good thing. And there are some features that it would be nice to see Firefox steal. I mean, this adaptive website tracking elimination, that's a very cool thing. I like that a lot. I'd add that to Firefox in a heartbeat.

Leo: I bet somewhere there's a button that you could change it from three to one or, you know.

Steve: Yeah.

Leo: So that it doesn't wait for three tries to turn it off.

Steve: Yeah. In fact I did try to go down below. Of course it stops at three.

Leo: [Indiscernible] somewhere, yeah. I bet there's somewhere, some setting. We'll find out when it comes out. I've been using 8 on Windows 7 for some time, but that was kind of a prerelease. And now it's out for everything but Windows 7, actually.

Steve: And again, no hurry to jump to it. It crashes on the Wall Street Journal website.

Leo: That's kind of hard to believe. That's just hard to believe.

Steve: Already it's been hacked. There's a first vulnerability. I mean, again, there just isn't - there's nothing so compelling about it that I would think anyone would have to jump to it. I'm going to wait for it to be pushed onto my system. And I've got it running in a virtual machine, so I can go visit it if I ever need to.

Leo: I don't think they'll push it. I remember when IE7 came out it was almost - it wasn't even like a forced update or a critical update. It was just you should really use the new 7.

Steve: Right.

Leo: And they'll probably just do the same thing there.

Steve: Right. In the meantime, I think everybody who's listening here is probably happy with Firefox. And I think they should be.

Leo: You bet. All right, my friend. Thank you very much. A great subject, and one everyone needs to know about. If you want to read as Steve talks, you know we have transcripts thanks to Elaine. She writes everything down. And Steve puts that on his page, GRC.com. You can find all the show notes, 16KB versions of the show, and Elaine's transcriptions there. And while you're there, check out SpinRite, the world's best disk recovery and maintenance utility.

Steve: Yay.

Leo: It's a must-have. I didn't hear any yabba-dabba-dos. You turn those off now?

Steve: Yeah, 'cause I think they're just a distraction, so.

Leo: We're going to - I've been inspired by you. I want to make a device that will pop my ball if somebody donates a thousand dollars to TWiT. So we're going to work on that.

Steve: You want to be careful who you say that to, Leo.

Leo: My, you know, the blue ball I sit on.

Steve: Pop your blue ball. That's much better.

Leo: And I'm going to have a Nerf gun that's aimed at my forehead. And if you pay, you know, $10 it'll shoot an arrow at me. I figure I'm going to take this yabba-dabba-do thing to the next level.

Steve: Maybe we could get some sort of a robot arm where it'll throw a shoe at you.

Leo: There you go.

Steve: Agh.

Leo: We have a guy, I mean, there's a guy who's an expert in robotics is going to build some stuff.

Steve: Cool.

Leo: And we get a ping, we could set it up to get a ping whenever there's a donation. So we'll see. GRC.com, that's the place to go for SpinRite. Oh, and don't forget ShieldsUP! and all those great free security utilities.

Steve: And more stuff coming soon.

Leo: Yeah, I can't wait, I can't wait. Thanks, Steve. We'll see you again next week for Security Now!.

Steve: Thanks, Leo. We'll do a Q&A, and I will remind our listeners, please send me your questions, thoughts, and comments: GRC.com/feedback. I go through all of that when I'm preparing for the Q&A episodes every other week, and read as many and answer as many as I can. And we do a great show with those. So GRC.com/feedback.

Leo: Fantastic. Thank you, Steve Gibson. We'll see you next time on Security Now!.