Google's Chrome

Description: Steve and Leo examine Google's new "Chrome" web browser. Leo likes Chrome and attempts to defend it as being just a beta release; but, while Steve is impressed by the possibilities created by Chrome's underlying architecture, he is extremely unimpressed by its total lack of critically important security and privacy features.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-161.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-161-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 161 for September 11, 2008: Chrome. 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!, the show that answers your question, the vital question, "Help!"

Steve Gibson: Or the exclamation, I suppose.

Leo: Yeah, it's not a question, "Help!"

Steve: What to do with your Gibsonian reflex response.

Leo: That's, yes, the Gibsonian response, which we encourage you to have. That is something one of our viewers coined because anytime he sees something a little scary happen on his browser, he says, "I had a Gibsonian response." Little red lights flashed, sirens. Steve Gibson's here from GRC.com, the security guru. Hi, Steve.

Steve: Hello, Leo, great to be with you. We are airing this on the seventh anniversary of 9/11.

Leo: Oh, yeah.

Steve: September 11, so...

Leo: A very grave, serious anniversary, you're right.

Steve: Seven years, though, have already gone - we're getting old.

Leo: You know, 9/11 is one of those things, though, like the Kennedy assassination, and we're old enough to remember that, where you will always know where you were when you heard it.

Steve: Yup. In fact, I got a call from the FBI that morning and was asked to help out with some things they needed.

Leo: Oh, really. Oh, how interesting.

Steve: And the guy, my FBI guy called me and said, "You know what happened," I said, "Oh, yeah." You know, I had the TV turned on, and several people had called before saying, my god, turn on the television. So it's like, yeah, big deal. So, yeah, wow.

Leo: Yeah, it's certainly something to commemorate. And it changed the world forever. Certainly changed Americans' lives forever.

Steve: Yup.

Leo: Also the day after the Large Hadron Collider did not destroy the Earth.

Steve: That's a good thing. Assuming that our listeners - we're recording this on Wednesday...

Leo: If you're hearing this...

Steve: ...and the collider has just been turned on. Now, yeah, so assuming that this podcast is ever actually heard by any humans...

Leo: No, because they're not yet colliding, they're just testing. They're just running them around the track right now.

Steve: That's true.

Leo: No danger yet.

Steve: Of course, you know, the sky-is-falling people are saying that it's going to create a black hole that's going to suck the whole Earth into it. And but the good news is that small black holes evaporate quickly. And they may actually be, like, zipping around, you know, black holes can get caught by gravitational bodies. So we might have a few already inside the planet, just sort of zooming around our center of gravity. And, you know, nobody would really know it. It's not a big problem.

Leo: They asked Stephen Hawking. He said, oh, no, it's not a problem. But, see, I thought a black hole accretes very rapidly all the stuff around it because of its intense gravitational field.

Steve: Well, it does, except that there is also evaporation. And I used to know, I mean, I remember once I understood the physics of that. But it's, like, long since gone. But...

Leo: Right. Fascinating stuff.

Steve: But I believe Stephen because, after all, he is the person...

Leo: He seems to know.

Steve: ...that Hawking radiation was named after.

Leo: But, you know, I love it when they do big science like this. It's arguably the largest scientific experiment ever created by humans. Just exciting.

Steve: Oh, god, and Leo, when you - "Scientific American," earlier this year or late last year it might have been, had this fantastic spread that, like, with huge color photos of the various targeting systems like the endpoint where all of these high-energy photons end up going. And, I mean, it looks like a real starship. I mean, it's like - it looks like, literally, the engine room of a big Enterprise sort of warp drive. It's just phenomenal. And then in the photo they'll refer to the picture, like the guy on the scaffold. And you go, what? And then you look, and if you, like, zoom way in with your eye, you see this little person standing, like adjusting something in this massive thing surrounding him. It's just, ooh, I mean, it just gives me goose bumps. It is, like, it is as close to science fiction as science fact has come so far. It's just - it's exciting.

Leo: It's really exciting when we do stuff like that. It's just - makes you proud to be alive in an amazing era.

Steve: And it should be able to tell us, I mean, the whole point of this is by creating much higher energy collisions of particles, it will help to confirm existing theories and also raise questions that then the theoreticians will work on solving. So, I mean, basically it's all about allowing us to get a better sense for what it is that our fabric of reality is built from. How does it really work? Is it strings or loops or quarks or who knows?

Leo: We have a physicist who is a regular follower of our broadcasts. She's a professor at the University of Toronto of physics, Professor Peet. She's going to join us on the radio show on Sunday to talk about what it means and so forth.

Steve: Very neat.

Leo: And what the Higgs boson is and...

Steve: Will she be on for the whole three hours?

Leo: Oh, no no no, I don't think - well, who knows? If there's enough demand...

Steve: You going to start at the beginning?

Leo: We'll start at 11:30. So it's possible we could keep her for as long as people want to talk about it. I think this is the kind of thing it's important to talk about, you know? This is tech.

Steve: It is serious tech. It is mega tech.

Leo: So we're going to talk a little bit about mega tech. We're going to talk about the newest browser in the browser wars, a big shot from Google Chrome. And it's, I presume, a security angle; right?

Steve: Well, yes. That's, of course, that's the angle of our whole show. And, you know, we discussed it for the first time last week because it had been announced the day before we were recording. We record on Wednesdays for publication on Thursday. And Chrome was released on Tuesday of last week. And you and I immediately backed away from it due to the problems with the EULA, the End User License Agreement, which was ridiculous. And the good news is, so many people raised such a fuss that Google, with shocking speed, fixed it.

Leo: They said, whoops. They said, our bad, we didn't mean to - that was cut-and-paste. Now, I'm not sure if I believe that. But they backed off very quickly, yeah.

Steve: And I don't think I believe it, Leo. I mean, this thing is...

Leo: They have lawyers by the dozens. They can rewrite.

Steve: And this thing is two years in the making, the browser is. I have a lot to say about it, and none of it good. Well, not much of it good. I am very disappointed. I'll tell you why when we get into...

Leo: Good, I can't wait.

Steve: Yeah.

Leo: So, Steve, before we get into Chrome, which I'm very excited about, any updates - you know, it's funny, I booted up - I've been gone for a day. And I booted up, and all my Windows machines said we've got updates, we've got updates. So it must be a Patch Tuesday.

Steve: It was, yes. Yesterday was a Patch Tuesday, and it was an important one. In fact, well, there were four major Windows components that all had patches - Windows Office, Media Player, and Media Encoder. The Office vulnerabilities were significant because there was a new component that was added in Windows XP. All versions of Windows from the very first version 1 had something called GDI, the Graphics Device Interface. GDI, along with user and kernel, are like the three main pillars of Windows. And of course the whole point of Windows is that it's a graphical environment for...

Leo: Does every - all calls, all graphics calls go through GDI?

Steve: Yes, yes. GDI is the - well, yes, all graphics calls do. There are non-graphics calls like memory allocation and things that don't involve graphics. But, yeah, it is, it's where all the graphics system is located. And Microsoft added something called GDI+, sort of an additional next chunk of - it's another DLL library of subroutines. Well, there were four, I'm sorry, five vulnerabilities in GDI+. And the reason these are of concern is that these are image-rendering vulnerabilities. And images, of course, are what web pages display. So people who understand what the vulnerabilities are, it's one of those where, you know, email that is running in the IE viewer, so displaying email that displays an image or using Outlook with the IE viewer or going to a website with IE or even non-IE, any browser that is going to be rendering those images will typically be using this GDI library. So anyway, very important, as always, it's like it's never not important for people to make sure that they've got these most recent patches for Windows, this being, you know, just having passed another second Tuesday of the month. Also the news about Wells Fargo login continues.

Leo: Just to update you, this was an email we got two episodes ago from somebody saying, hey, it's weird, it truncates my password, doesn't use any - what is it, eight characters it uses? And then...

Steve: Well, yeah. The first report we heard was that extra characters were ignored. Now, I'm not sure if - no one has, like, done an experiment or reported it that says, look, this is how many it uses. We do know that you can put superfluous characters on the end that are completely wrong, just random, and you still get to log in. Then the second report we heard was that not only is the password, the tail of the password superfluous, it doesn't matter, but the password is non-case sensitive, which dramatically reduces the security, but in the name of making sure users are able to log on. The problem is, when you do that, you're helping the bad guys to log on, as well. Anyway, I got another report from someone who, after hearing these two, decided, okay, I'm going to play with this myself. So he reports that, not only is the password not case sensitive, neither is the username.

Leo: Oh, man. It's getting worse and worse and worse.

Steve: So none of this is case sensitive. And that would have had to have been deliberate on the part of the programmers because you would need to deliberately remove the case before you stored it.

Leo: Strip it out, yeah.

Steve: Yes. You would, like, make everything lowercase or uppercase, one way or the other. And then you'd have to do the same conversion every time you did a comparison. So it's not a natural thing for something to be not case sensitive. It is an unnatural thing. I mean, you'd go to some effort in order to make that happen. So anyway, that little tidbit...

Leo: And you would do that because you would like the users to not have to - to make it easier, as usual, the tradeoff between security and convenience. So if they enter it with a capital "L" for Leo or a lowercase "l," it doesn't matter.

Steve: I know. And...

Leo: It does make sense for the password, but I guess you'd probably have some - okay, I'm going to be stereotype here...

Steve: And it's not like you're logging into TWiT or Twitter or something.

Leo: This is your bank account.

Steve: This is your, exactly, this is...

Leo: But they're worried that some unsophisticated user will type the password with uppercase and lowercase, not realizing it makes any difference, so they just make it easier. They don't want the support calls.

Steve: And we don't know what the history is. It may well be that the programmers originally implemented it in a fully case-sensitive fashion, and they got so many redundant calls saying, hey, can't log in, that management said, okay, we've got to make this easier. This is ridiculous. Let's, you know, people are not remembering the case of their password. And so they just, presumably, removed it. I got a kick out of something that happened, well, a kick only because I'm not a user of Trend Micro's AV. Last week Trend Micro, the update early last week misidentified a collection of Windows XP and Vista core OS files, quarantined them, and removed them.

Leo: Ho. Which means it broke the system.

Steve: It hosed people. There are still people who have lost XP, who cannot get back to XP. Even going into safe mode doesn't help you because it's some core files that are necessary for safe mode. And it's not the first time this has happened with Trend. It also did happen to Symantec a few years ago. So, I mean, this is sort of the dark side of the heuristic pattern matching is - you've got to wonder, too, how they missed this. I mean, they run this on their own machines. Or somehow was it maybe a foreign language version matched and the language they were testing on didn't or something. But it's, like, really bad when your AV - it's like an autoimmune disease, I guess. I mean, your AV decides you're evil and quarantines...

Leo: Boy, that's a [indiscernible] description.

Steve: ...the OS from itself.

Leo: It is like an autoimmune, isn't it.

Steve: Yeah, that's where your immune system goes after yourself instead of - yeah, so not good. And I did want to mention also I got news from my friends at Golden Bow, who are the publishers of Vopt, which is one of my two favorite defraggers. Vopt I really like, which has always been at major version 8. I think it's been at 8.1 for a while. They released version 9, which has some Vista enhancements. It's been - it's redesigned, and it's very nice. So that and PerfectDisk are my two favorite optimizers. They're enough different that I like to use them both sort of for - Vopt is very fast and sort of does a nice, quick, very graphical, you can really see what's going on, defrag. And PerfectDisk is able to defrag the files that are in use, that is, the page table, hibernation file, directories, basically the system things that normal defragging won't do. You're able to say "defrag at boot," and then when you restart the machine it jumps in before Windows gets going and defragments all of those core things that don't tend to fragment by themselves, so you don't have to do it very often, but it's just nice to have something that'll, like, set that up once for you when you're setting up a new machine. So...

Leo: I'll tell you how old that is. I remember Jerry Pournelle recommending Vopt, that's where I first heard about it, in his users column, Chaos Manor, in Byte magazine. It's probably 15 years ago, a long time.

Steve: Yup. Golden Bow's been around a long time. They're a good company, nice technology. And I was just - there hadn't been much action or motion with Vopt for a long time. So I was sort of wondering, well, I guess it's sort of not going to be changing. But I got the news last week that it had gone to version 9. And so I just wanted to point that out to people because I've mentioned it before. I know that there are listeners of Security Now! who have adopted Vopt, and so I wanted to make sure they knew there was a new one.

Leo: Yeah, that's a good...

Steve: And then I promised last week that I would share a short little SpinRite blurb with our listeners about SpinRite saving 200 kittens. It turns out that was a little misquote. But, well, but not much. The subject line of this email is "SpinRite Saved 200 Hungry Cats." And so the author, Marius, says, "Hi, Steve. Hi, Leo. I want to give some feedback for the fabulous SpinRite. I'm working in an animal shelter. We have got a special database to control the feeding and to control food orders automatically. During the weekend our computer broke down, and we were unable to determine whether there had already been food orders for all the animals. Because of the fact that we're very low on money these days, a double order was impossible. After I asked some technically skilled guys, my friend Paul told me that there's SpinRite. The order was no problem because your site is designed very well. After I purchased SpinRite and got it instantly, I was able to recover all the data on the computer, and I saw that we had not placed the food order. I was able to complete everything, then purchased a new hard drive as a precaution. 200 hungry cats and dogs are thanking you, Steve and Leo, and so do I. SpinRite saved these animals" - oh, okay - "saved these animals, and I'm very happy to announce that I'll try to listen to Security Now! from now on, too. But I'm not a technical guy. Thanks for this brilliant program in the name of the hungry animals. Yours, Marius."

Leo: The hungry animals say, "Thank you, Steve." Hungry animals.

Steve: The hungry animals thank us for SpinRite, yes.

Leo: That's great. That's great. Chrome is a good name. You know, I was thinking about the choice of names.

Steve: You know where the name comes from; right?

Leo: No.

Steve: "Chrome" is the jargon which is used by browser designers to refer to all of the UI outside of the page.

Leo: How interesting.

Steve: So they refer to that as the "chrome" on the browser.

Leo: Right, that makes sense.

Steve: Like the skin.

Leo: And by the way, this is a very chrome-free browser. So it's kind of ironic.

Steve: It is. It's minimal. It's minimal chrome, exactly.

Leo: Yeah, yeah.

Steve: Well, and that's one of the things I like about it. We were talking just the other day that I like small devices. I've got this little OQO, which is a cute little handheld ultra-mobile Windows machine. The screen is 800x480, so I don't have lots of screen pixels to waste on superfluous UI. And so running full screen in the browser, and a browser that isn't taking up a lot of the screen, is really nice. But where, you know, we talked about the EULA, and then I was aware a couple days later that Google had fixed the EULA. It's like, okay, well, that's good. And I had mentioned to you that prior to the podcast starting I was in the process of installing Chrome in a VM, in a VMware virtual machine, just to give it a place to live so I could watch it and not have to install it on my main system and then remove it with all of the wear and tear that creates. Well, but I didn't really take any action until - that is, you know, further action with Chrome. And with the EULA being the way it was, that of course put me off of it completely, though they have fixed that.

But I happened to go to one of my pages which is not yet public. It's the whole cookie region that I've been working on, which I suspended work on while I'm working now on this very comprehensive DNS profiling facility, which I expect to be announcing in two weeks. And so anyway, I went to one of my cookie pages. And this is a page which is basically advocating for third-party cookies being disabled by default. The only browser that does that in the entire industry, and this is inclusive of Chrome now, is Safari. Safari has cookies disabled by default. And on this page I show, of all the visitors who come to GRC, how many people have cookies enabled. And it's a huge number, I mean, a huge percentage. It's like 80-some percent, I think. And then I show the power of default settings by showing what Safari's setting is. And it's always been down in the low, like, just a little over 10 percent.

But when I happened to go to that page - oh, and this is all real-time statistics that update continuously. Every Sunday night the prior week's summary is made current so that I'm able to see changes over time and not just accrue forever. So I'm able to see, like, we're always looking at what the last week's stats are. Well, suddenly it was - Safari was showing as 54 point something percent. And it's like, whoa, wait a minute, that can't be. Nothing has changed in Safari. And then I immediately clicked on what it was because I remembered that Chrome was based on WebKit, which is the same open

source HTML rendering system that Safari is based on. So my hunch was that my cookie tracking system was misrecognizing new Chrome users as Safari users.

Leo: Oh, interesting, huh.

Steve: And that since Chrome had third-party cookies enabled by default, I was suddenly believing that Safari had gone bad. And but the fact that the number was so big shocked me. It's like, wait a minute, people are really using Chrome? And so then I went over to my demographics stats page, which is much more comprehensive. And sure enough, suddenly I have a big - I have a pie chart there that shows the various percentage of browsers of visitors coming to GRC. And everyone, all of our listeners will know about this as soon as I get these pages finished. I don't want to talk about it too much, I mean, I don't want to go into detail about all the other things that are there because they're not complete, and we end up with people saying, hey, wait a minute, I clicked this link and it says there's, you know, I got a 404. It's like, yes, that's just a placeholder for me.

So anyway, the point is that I was quite surprised by the rate of Chrome adoption. And I thought, okay, if that's the case, then we need to talk about it because there are some things interesting about Chrome, lots of interesting and intriguing good design decisions, or potentially good, from a security standpoint; but some things that are also very annoying to me. So I did some research, and it turns out that in the first 24 hours of Chrome's release it hit 1 percent Internet penetration, that is, 1 percent of Internet users were giving Chrome a try. And that peaked about three days later at 1.57 percent in one stat that I saw. So obviously it didn't take over. But it did, you know, there were a lot of people using it and, apparently, going to GRC to see what we thought of Chrome. To give people some sense of the way the demographics are breaking down right now, IE is holding about 70, 71 percent.

Leo: You just sold a copy of SpinRite, I hear.

Steve: I thought I'd muted that.

Leo: No, I like it. You should never mute that.

Steve: Oh, really?

Leo: I love it. That yabba-dabba-do is a little - Steve has all these sounds that he normally mutes in the background. That means, what, that's a license to SpinRite; yeah?

Steve: That's someone's credit card cleared. Because I have, as they're moving through the eCommerce pages, where you fill out the form, and then you submit that, and you verify before you commit, I have, like, a cash register sound, kaching-kaching, kaching-kaching. And then when the actual credit card transaction occurs, I have this Fred Flintstone yabba-dabba-do.

Leo: It's not merely celebratory. You probably also can use it diagnostically because if you hear a lot of kaching-ching-chings, but you don't hear a yabba-dabba-do, if you start hearing little issues like that, that probably has some value.

Steve: Oh, absolutely. Yes. I mean, it does. There is - oh, and I've got - there are other sounds that it makes. Basically I set up a custom UDP client and server. And every two seconds my client pings a custom server at GRC's facility at Level 3 to request an update on all kinds of stats. So a whole stats package comes back that allows me to monitor incoming and outgoing bandwidth and other things that are happening, including the status of our eCommerce system. So...

Leo: Anyway, I'm sorry, Fred distracted me, and I'm easily distracted. Let's get back to Chrome.

Steve: Okay.

Leo: I'm actually going to load my statistics pages because I use Google Analytics on a number of pages. You know, we get a much more geeky audience. So our Chrome adoption rate is going to be much higher than the average, I would imagine.

Steve: Right. IE currently has about 71 percent market share. Firefox is at 20.

Leo: This is not your server. This is global.

Steve: No, this is global. These are stats people from...

Leo: It's reversed on my server. It's exactly the opposite.

Steve: Well, and actually at GRC it's very much similar to that. Firefox is about half. And I think it slightly edges out IE. We still get a lot of IE. But really a disproportionate share compared to the Internet in general, which is not surprising because Firefox users, I mean, NoScript is super popular, which is what I keep preaching, is that JavaScript is not safe. And so, yes, it's useful. But it's like radio, it's bad. And so you have to have it sometimes, but you don't have to have it all the time.

Leo: You also get probably a lot of business users buying SpinRite or going to ShieldsUP!, and that may skew you a little bit more towards IE than, for instance, TWiT.

Steve: Oh, that's a good point, too, yeah. I don't really know the demographic of the ShieldsUP! users. But so IE at 71; Firefox at 20; Safari, Apple's browser, and this combined Windows and Mac, is at somewhere between 6.1 and 6.3, depending upon who you ask. And Opera, surprisingly, is as low as 0.75.

Leo: You want to hear my numbers?

Steve: Yeah.

Leo: For TWiT.tv. And again, a geeky audience, right, so it's going to be a little different. Firefox 60 percent; IE 20 percent; Safari 14 percent...

Steve: Mac, of course, yeah.

Leo: Yeah. Chrome, 2.41 percent.

Steve: Wow.

Leo: And this is in the last, looks like the last - since August 10th, so the last month, 30 days. So if I actually -if I go since Chrome came out, let me just look at the week, it's going to be much higher Chrome percentage. And then Opera at 2.27 percent. So it's interesting, the disparity, really. I'm just - I'm curious. Let me just look at the last, say, when did Chrome come out, the 2nd; right?

Steve: Yes, Tuesday before last.

Leo: Right. Let me go the 2nd through the 10th and see what Chrome is.

Steve: Chrome has fallen, by the way.

Leo: Oh, really. Yeah, it's 8.8 percent in the last week for me.

Steve: Wow.

Leo: And you know who it took market share from? Firefox. Firefox down 5 percent; IE only down about a point and a half.

Steve: Well, now, that actually speaks to some of the points that I'm going to be raising because I've - well, and I want to just finish, that 'Net-wide, Chrome peaked at 1.57 Internet-wide and then began to drop and is now down to, at last note, 0.9 percent. So there were a lot of people who gave it a test drive, who thought, oh, I want to see what Google has done.

Leo: Sure, sure.

Steve: And this is my main complaint is that, as the famous old expression is, you only get one chance to make a first impression. And I sort of wonder who Chrome is targeted at because it was clear to me that it would be Firefox users who were - that is to say, those who are, were first of all, willing to move from IE. There's been a lot of conversation over the week about Web 2.0 and AJAX application handling because one of Chrome's main features is that they say that it has an extremely strong, very fast, brand new JavaScript engine, their own JavaScript engine, V8, made by some guys, I think a team in Denmark, as I recall. And sure enough, if you benchmark their JavaScript versus others, theirs wins. There are JavaScript benchmarking suites and sites. And Chrome does win. However, in overall page-loading performance, it is not speedier, for example, than Firefox or Opera. So that's a problem.

Now, one reason is, one of the benefits of Chrome is that they are launching - and I've checked a lot of this out now. They really are launching an entirely separate process, a Windows process for every page. So there is process creation overhead with creating a new page. It's not bad. But it's two things. It does take some time, and it does take some memory. At the moment, Chrome is a bigger memory hog even than IE8, which is now in Beta 2, and IE8 has been criticized as being a memory hog. There was one reviewer who opened a standard 10-page set of tabs and, whereas IE8 consumed - are you sitting down, Leo?

Leo: Yeah.

Steve: 324MB to open those. Chrome was a little more than that.

Leo: Yeah, but everybody has several gigs. I mean, come on, that's not...

[Talking simultaneously]

Leo: ...point out that when you're testing beta software, frequently there's code, as you know, left in beta software that takes more memory. Beta software is not tuned for memory usage yet, or speed.

Steve: Well, okay. Maybe.

Leo: They might even have the symbol tables in there and stuff. I mean, there's all sorts of stuff that could be still in there.

Steve: It's not in there.

Leo: Oh, okay, all right.

Steve: I looked. I think that what we are going to have to accept is that we're moving to a next generation of browser.

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

Steve: I think that IE8 and Chrome are both aiming, I mean, certainly this is where Microsoft's direction is, and we know that's where Google's direction is, they are aiming at the browser becoming the OS.

Leo: They're, well, they're an application platform at least. I don't know, I don't think you'll be deleting files and moving files via Chrome. But it's an application platform, for sure.

Steve: I wouldn't be surprised if someone does some wacky [indiscernible]...

Leo: Plug-in for file management?

Steve: Okay. But in any event, what I mean, and I don't mean the OS in that sense, I mean as where you run applications.

Leo: Yeah, an application platform, right.

Steve: Right now we run applications on top of the OS. And clearly Microsoft and Google are both aiming toward this whole, always connected, we rent your applications to you, and you're going to be running them in the browser. So a strong JavaScript interpreter, and in fact Chrome apparently goes further. They do some sort of byte code compilation. They say they're compiling into real machine language. So it's probably, I mean, there's been a lot of work done in virtual machine architectures over the years. And there are systems where they will compile on the fly, the first time they run across byte code they compile it in a just-in-time fashion into real machine language; and then next loop-through, next time they execute it, it's much faster. You still have an intermediate language translation overhead and intermediate language sort of expression overhead as opposed to something where a compiler is able to crank on it for some length of time to produce natively optimized code. So it's never going to be as fast. But it is acceptably fast. And we have machines getting much faster. And to your point about how much memory these systems have today, I mean, you're certainly right, Leo. So what if it takes a third of a gig? I will say that I completely crashed Chrome running it in a 256MB virtual machine.

Leo: Oh, my, yes. So, but I think that that's the way, that's the trend of all software, and certainly all application platforms and OSes. You assume more memory space.

Steve: However, it crashed. I mean, it didn't hang.

Leo: That's not good, yeah.

Steve: It just disappeared off the screen, and then it would not restart because...

Leo: Now, I'm wondering how much RAM does Word take up, or Excel take up? When you're running a native application, it takes up a lot of memory, too.

Steve: I don't think they take up...

Leo: About 300 megs.

Steve: 300 megs is a huge amount of memory.

Leo: You're biased because SpinRite runs in, like, 20K. So you...

Steve: I'm just saying that it is going to have a problem on lean machines. There are 500MB machines that people are using today because once upon a time half a gig was a lot of memory.

Leo: Well, and I also want to point out, I'm looking in the chatroom, there are people who have 20 tabs, there's a guy who says I usually have 20 tabs open, 12 tabs times 3 rows, 15 to 25 tabs. There are people whose workflow has a lot of processes running in their browser.

Steve: Okay, so, now, the reason that Google has done this is twofold. They recognize that if a browser is going to be an enterprise-ready tool, that is, if literally, if you would be using it as your word processor, then you can't be 15 pages into creating a document and have some other tab that you briefly switched over to to do something hang your whole browser because you've got 15 pages of work in one of these tabs. So, and frankly, when this thing just disappeared from my screen yesterday, I wasn't very impressed with its collision-handling capabilities. But, again, it is beta. We recognize it's beta.

So the idea, though, is by launching separate processes, they keep them independent. And Google's focus from the beginning has been that these things, that individual processes run in separate tabs so that, if one dies, it's just like an app dying in Windows. An application dies, and of course that happens, or locks up and, you know, happens from time to time, especially if they're poorly written, you just - you close it or kill it, using Task Manager if you have to. But inherently you've got your other applications are unaffected. Similarly, the other tabs in Chrome would be unaffected. So there's that.

Also Google makes the point that there is inherent memory fragmentation, it's known as "heap fragmentation," within the context of a process. So within a single process one of the things that happens is there's all kinds of memory continually being allocated and deallocated. As you surf around, and a page is loaded, the page contains all kinds of GIF and PNG and Flash and all kinds of other images. Well, those all acquire memory from the process, within that process's space, while you're looking at the page. You then go to another page, and those chunks are freed.

Well, all these chunks are different sizes. And so what happens is the operating system searches for a free space large enough to fulfill a requirement, and it sticks something in there. Then, for example, say something else comes along that's smaller. Well, so it fits it into a smaller space. Then something else is removed. It is exactly analogous to fragmentation of a hard drive. When you think about it, the reason hard drives fragment is that new files are added, file sizes change, files are deleted, an old version is turned into a .sav and a new version is created. So there's constant churn on the hard drive. And all users are familiar with the way their hard drive looks when they view it in a good defragger. It's just all chewed up. It's all fragmented.

Well, the same thing happens to memory. What happens over time is - and in fact heavy users of Firefox are familiar with this phenomenon because it's something that has afflicted Firefox to somewhat greater degree for whatever reason, just architecturally, than IE, is Firefox will start getting really slow. And you'll have to literally shut it down and restart it in order to, like, get it going at normal speed again. And that's due to fragmentation. So...

Leo: Modern operating systems, memory managers handle that. They make sure you don't get fragmentation. Why is it these browsers can't do that?

Steve: Well, modern operating systems actually don't.

Leo: They don't?

Steve: Well, no. The containment of this is per process. And so it's the process that has the fragmentation.

Leo: So the application, or the page, has to handle that. Or the JavaScript or something.

Steve: Well, what - the advantage of this per-process model in Chrome, and I have to - I should mention that IE has gone to the same thing. IE8 is also a process per page, for many of the same reasons.

Leo: Oh, interesting, yeah.

Steve: So we have that in IE8 without having to go to Chrome for it. The point is that, by having individual pages be processes, you get the robustness of them not crashing each other, hopefully, unless the whole browser crashes, as mine did yesterday. But it also means that when you leave a tab or close a tab, that process, even though there might have been fragmentation within it, all of the memory is released because, for example, the heap structure is a per-process heap. So it's per process allocation that this is being done. Essentially it means that the fragmentation that you will have is per tab rather than per browser. And so just closing a tab which is becoming a problem, if you happen to be, like, surfing in one tab all day long, which it sounds like most people aren't doing, they're jumping around between tabs, and tabs have a life of some length of time much less than the time they're using the browser, so...

Leo: So an operating system is kind of at the mercy of the application that's running. If an application has memory leaks, or it doesn't release memory properly, then it can't help the fragmentation.

Steve: Correct. And in fact there is this notion in modern high-level languages like JavaScript...

Leo: Garbage collection, yeah.

Steve: ...there is something, I was just going to say, the garbage collector. Again, Google designed it so that they have a more - they're able to have a more aggressive garbage collector in their JavaScript engine than other JavaScripts are able to because theirs is able to track the usage of pointers which point to these temporary objects with a finer degree of precision, essentially, than other JavaScript engines. And the last benefit is security. By running pages in their own process, you get the benefit that the OS already brings to interprocess isolation. Now, that's sort of an oxymoron, as we know, because interprocess isolation could be and should be arguably much better under Windows than it currently is. There is not sufficient interprocess isolation.

And Google makes a point of talking about how add-ons to Chrome can weaken the interprocess or, in this case, the intertab isolation and also the isolation of the tab with the OS. Google is deliberately working to sandbox the operation of the pages running in the browser. They have a model where you're either user or sandbox. We could think of it a little bit like NAT routers. We know how, for example, the big, bad Internet is outside of our NAT router, and we don't allow unsolicited traffic into our protected local network. Well, similarly, the model that Google has adopted is sort of like a NAT wrapped around individual browser pages where the page is unable to make an unsolicited access, an unsolicited request outside of itself. It's only the privileged OS on the outside, the user space, that is able to communicate inward. And the app is only able to respond to external requests. It's not able to initiate any communication itself. So that's, to the degree that that succeeds, that's a nice model.

My problem with the browser is that it is, well, to say it is feature-lean is an understatement. And this is where I wonder who they're trying to sell this to. I don't mean "sell" literally, because it's free. But we know that Firefox users love the features of Firefox which IE lacks, and IE is slow in adopting these things. Like, oh, gee, tabs, for example. But also simple security features. For example, okay, get this. Chrome, like all contemporary browsers, offers to save your passwords. And you can turn that off, but it's on by default. The problem is, it will also show your passwords. But there is no provision for a password to protect the passwords. Meaning that anyone can sit down at your Chrome browser, I mean, other than you - your kids, a coworker, anyone - and look at all of your passwords, and which displays all of your usernames and passwords in the clear, and write them down. There is no provision for protecting that. Plus, for example, in Firefox you're able to create - and Opera - to create a master password which will protect access to those.

Leo: You know, it's funny, I noticed that. My, what do you call it, the Gibson alarm went off...

Steve: A Gibsonian response.

Leo: Yeah. I noticed that it was saving my passwords, but it didn't ask me for a password to protect it. And I was wondering how they store it. So they store it in the clear?

Steve: Well, it's you click a button to say "Show Passwords." And...

Leo: I guess it would have to. If you don't give a password, how else are they going to do it, yeah.

Steve: Yeah. Well, so, okay. So there's that. And absolutely no scripting management of any kind. You can't turn it off. I mean, even IE lets you turn it off. Even, I mean, and Firefox, and Opera, I mean, everybody...

Leo: Well, remember, though, this browser is designed for JavaScript. I think one of the ways I use it, I don't use it as a day-to-day browser. What I've done is that I've taken, like, Gmail and made that be a separate application running in Chrome on my desktop. And again, that's not safe if it's saving the Gmail password. But at least, I mean, you know, that's kind of how I'm using it. I'm not using it to browse randomly. And I suspect that's the intent; right?

Steve: So I recognize that they wrote Chrome to have an application for running JavaScript. But again, who is their customer? Because it is a huge benefit for people running Firefox. And as I said, even IE you're able to do, like, per-site handling in IE and in Firefox and in Opera. There is zero per-site features in Chrome. There is nowhere in there can you say I want to whitelist a site or blacklist a site. There is no provision for that kind of granularity. And the cookie handling could not be weaker in terms of privacy. Now, we know that, you know, they bought DoubleClick, the king of third-party cookies. So that's a bit of a concern. You've got three settings for cookies, which is wide open or completely closed, which we know is just impractical, you just can't do anything with the 'Net that way. But no whitelisting. You can't say "closed except for these sites." I mean, again, even IE, the least privacy-concerned browser, supports that.

Leo: How is its third-party cookie handling?

Steve: Well, it's bad. That's the third setting is restrict - quote, "Restrict how third-party cookies can be used." Well, no one's really even sure what that means...

Leo: Right, right.

Steve: ...in the first place. But we do know that, unfortunately, and maybe this is a consequence of their WebKit heritage, they are equally bad as Safari in that they block, when you turn on "Restricting third-party cookies," it blocks them coming in, but not going out. Which means that you have this problem with what's called "cross-context

leakage," meaning that if you were to go to PayPal and click on a link at PayPal, since PayPal loops you through DoubleClick, your browser visits DoubleClick, it's there in a first-party context because it actually pulled up a DoubleClick page through a redirect. That allows DoubleClick to put a cookie on your browser in a first-party context. Then it bounces you back to PayPal. Now, wherever else you go, not PayPal but anywhere that is serving DoubleClick ads, because a DoubleClick cookie snuck into your browser, slipping through in a first-party context, even though you said I want to block third-party cookies, it's sending them out.

Leo: Now, a couple of people in the chatroom saying, well, Steve, you're being unfair because this is version 1.0, don't compare this to Firefox.

Steve: And I said you only get one chance to make a first impression.

Leo: Well, and I'd also point out it's version 1.0, but you are competing against version 3.0 of Firefox and version 8 of Internet Explorer.

Steve: I see. And Google knows nothing about browsers. Google has never seen a browser before. They don't know how they work. They've never seen Firefox or Opera or IE or Safari. These are newbies over there at Google who really don't understand the way the web works.

Leo: Obviously not. So you're right, they should have known better, yes.

Steve: It's nuts. I mean, it is nuts, Leo. And if nothing else, look at the adoption rate. Almost, well, 1.57, 1.6 percent people used it. And I and a lot of other people said, okay, well, no thank you. I'm not using something that is by default storing the passwords I use for logging on and giving me no ability to protect that storage from somebody who might have access to my browser at any time in the future. I mean, that's crazy. It's just crazy.

Also no provision in cookie handling for distinguishing between session and permanent cookies. Even IE, again, you're able to say, look, I don't mind session cookies, that is, cookies that are persistent only while I'm using the browser, as long as you throw them all away at the end. Other browsers provide that. No provision for handling sites individually. I mean, I truly - I don't get what they're thinking, who they're aiming this at because IE users, who we might say, okay, are just not going to move away, and they're not clued in to security and privacy, so they just stay with IE, well, they're not apt to use some other browser. They're not going to move from IE. People who do, do for a reason, because they want these additional features. And Chrome doesn't have any of them. I mean, any of them. It just boggles my mind. Oh, yeah, I just - and no scripting management, weak cookie handling, I don't know, I'm just...

Leo: Well, I mean, obviously...

Steve: Oh oh, oh, oh, and they call that thing at the top the "Omnibox"?

Leo: Yeah?

Steve: I call it "Omnispy."

Leo: Why is that?

Steve: It is a real-time keystroke logger.

Leo: So here's the deal on that, just to explain. As you type in a URL or a search term, it will supply - it goes out to, by the way, not necessarily to Google, whoever your search engine of choice is, and gets - kind of prefills it with suggestions. Firefox has been doing this for a while. You consider that keystroke logging.

Steve: Well, I was curious how it worked. So I turned on a packet capture. I fired up Wireshark, turned it on, and then, as I typed keys into the Omnispy box at the top of Chrome, as I began to, it initiated a connection to Google, and every single key I typed in, it sent that keystroke back to Google. And it's like, again...

Leo: Well, that's how it works, right, it's telling - it's sending the keys - Firefox does the same thing. It sends the keystroke to Google. Google then provides completion in real time from that keystroke, or those series of keystrokes.

Steve: Right.

Leo: I mean, it's not like you're entering a password there.

Steve: Well, I just wanted people to be aware...

Leo: And, by the way, you can turn that off. [Indiscernible] you can turn that off.

Steve: You can turn it off, but it's on by default. And maybe it's convenient. Many people have said they're a little unnerved by having a single box instead of a URL and a search area separately. I sort of like the idea from a conserving space. And it's like, okay, I'm not too worried. But again, people need to understand that what they type in there, even when they're typing in a URL, certainly it's the case that when you go to Google and you enter a search phrase into Google's page, obviously they know what you've entered. This moves that boundary all the way up to your keyboard, when you're typing even a URL you know. So if you type in a URL you know, that you would like not to be watched typing - now, you do have the advantage, however, of using the Incognito window, which is a nice feature of Chrome, where that feature is not available, and what you do in that window stays in that window. No cookies are written permanently, no caching is made permanently. So it's a simple way of doing something, you know, the example they give, Google gives, is buying a secret present for someone, and so your spouse won't look at

your cache of your browser, if they're apt to do that, or look at your history and see what sites you've been at. So none of that is saved. People out on the 'Net are calling that the "porn window" because it doesn't maintain any history of what you've done. So that's a nice feature. And that is also a feature in IE8. So IE8 will have something...

Leo: A porn window, yeah.

Steve: Can't remember what they call it.

Leo: Private browsing, private searching, probably something like that.

Steve: They've coined a nice term for it. But now I have to say one of the cool things that I like is the notion of dragging tabs between windows. For people who are browser-centric, and it really sounds like you've got some people, for example, you were talking about it, who have 30 tabs open in three rows, these are browser-centric people. I know that sometimes I'll have an IE window open with a bunch of tabs, and I'd like to, like, keep a couple of them. The idea of being able to drag them into a different browser instance, literally dragging tabs across browser windows, and then close the one that I no longer care about any of the tabs that are left, I think that's a cool feature. And someone's getting it. Is it - either Firefox, oh, I think it's Beta 2 of Firefox 3 is adding that kind of cross-window tab handling, which will be a nice thing.

So the thing I like about it more than anything else is I like the reloading your page little worm, the little worm turning thing. I dislike...

Leo: I don't even remember that.

Steve: Oh, it's a cute little thing. I'm annoyed when the page is still loading indication is not really clear. And I used to like it in the old IE where it was the spinning globe. You could easily see that the globe was still spinning, and so you could be doing something else waiting for the page to get finished. And then in Vista and/slash IE7 they've made it just that little glint that sort of moves around in a circle. Well, in Chrome you've got almost - it's almost a 180-degree of a circle, sort of like it looks like a little worm which is, like, spinning around. And it's interesting because it goes backward slowly when it's looking up the IP of the site, until the page begins to load. And then it starts running forward again. So that's my favorite feature. Other than that, I'm not very impressed.

Leo: Well, let's summarize both the security and the usability flaws of Chrome in just a second.

Steve: Oh, oh, oh. And they've already had problems, which we'll talk about.

Leo: All right. And the problems people are...

Steve: Security problems.

Leo: Security issues that are coming up.

Steve: Yes, already, in less than a week. Okay. While we're on...

Leo: So security issues, as well, now, for this thing?

Steve: Yeah, yeah. While we're on science fiction, though, if listeners are sure they will not read the book, then there is a Pak Protector entry in Wikipedia - Pak Protector. You might have fun going and looking at it.

Leo: But don't do it if you're going to read the book.

Steve: Yes. It is a spoiler. It will completely spoil the bok because, like many of Niven's things, it's one of the reasons I really like the way Larry writes, is there is a - you have no idea what's going on, even though you think you do. It is a total surprise. And the revelation of the reality of what's happening is, I mean, it's the reason you read the book. So do not, do not Google...

Leo: Don't spoil it.

Steve: ...anything about "Protector" if you think you might be interested. I recommend the book. Again, I own the paperback...

Leo: Here, I'll read you the summary. "Phssthpok the Pak had been traveling for most of his thirty-two thousand years. His mission: save, develop, and protect the group of Pak breeders sent out into space some two and a half million years before...

"Brennan was a Belter" - already I'm confused - "the product of a fiercely independent, somewhat anarchic society living in, on, and around an outer asteroid belt. The Belters were rebels, one and all, and Brennan was a smuggler. The Belt worlds had been tracking the Pak ship for days - Brennan figured to meet that ship first...

"He was never seen again, at least not by those alive at the time." And if that's not enough to get you going...

Steve: And again, it is just - it is a fun - again, I own the paperback. It's not very thick, so I don't think it's - I know it's not a big book. But it is...

Leo: It's a seven-hour read. That's a fairly normal-sized book. That's not too small. Oh, I'm putting it on my list right now. I'm just...

Steve: Really, it's good, Leo.

Leo: I love Larry Niven. I loved Ringworld. The whole Ringworld saga is just so inspiring and exciting. I'm adding it right now. You see, this is so cool. So I've got a credit, I just check it right here, and [indiscernible], it's going to download right now. I'll have it on my iPod for walking home tonight.

Steve: Okay. Second topic on the science fiction front is last night a new series aired which was really fun. It's called "Fringe."

Leo: I saw a big billboard for it.

Steve: It's J.J. Abrams' new series. You know he's working on the next Star Trek movie that we're going to have, that's going to come out next summer. He of course is behind "Lost." He was behind "Alias" with Jennifer Garner. And a couple other successful series. This is very X-Files-like. And I loved it. It is re-airing - the reason I bring it up is it is re-airing on Sunday. It's on Fox. So anyone who missed and think they might enjoy an X-Files-like sci-fi, I was just very impressed with the show. I thought it was tremendous. And of course...

Leo: "Fringe."

Steve: "Fringe" is the name. And of course we have "The Sarah Connor Chronicles" has restarted also. Its first episode was on Tuesday, the second season of that journey with Terminator mythology. So that was neat.

Leo: So let's talk about some of the flaws people have discovered.

Steve: Well, yes. I was smiling to myself about our listener whose question we read last week when she asked, hey, Chrome is new, and I listen to you guys, so I've learned that you can't ever claim anything about security preemptively. How long should I wait before I trust it? And I grinned because there were already problems found. I mean, immediately. Several bad ones. There was a couple - there was a way that a Java JAR file could be downloaded and executed without users' intervention. Bad. And there were some - a buffer overflow found in misformed URLs. And a little bit annoyingly, some other problems that they have fixed but refuse to document. And that's of a little concern because it's an open source project, and we would expect them to be not hiding what it is that they're doing. But in this case they were not being forthcoming with what things they fixed. I mean, the good news is they fixed them quickly. Chrome does keep a part of itself running all the time, even if you're not using the browser. And every few hours it phones home to see whether there's anything important has happened. And now...

Leo: Now, it's getting phishing site information.

Steve: Yes, it is doing that. Both phishing and malware are coming in on the fly.

Leo: Malware search strings, not malware itself.

Steve: Right, right, right, right, right.

Leo: Let's not imply that there's malware being imported here.

Steve: Yes. It's acquiring phishing and malware site lists, essentially. And so it uses that to protect people, bringing up a big, wait a minute, this is a known malware site, are you sure you want to go here warning message if you attempt that. Anyway, so the takeaway is that it's brand new software. It's going to have problems. I like the architecture. I like the potential of the architecture from a security standpoint. I think we have to acknowledge that browsers are getting bigger. IE8 is going to be big. Chrome is big. And I don't expect to see them shrink. So it's just they're going to be RAM-hungry things that are running applications in themselves, rather than applications all running separately.

Leo: Right, right. And so in summary, Chrome is underfeatured. Its privacy controls leave much to be desired. Doesn't offer...

Steve: There are none.

Leo: There are none.

Steve: Yeah. It just doesn't have any. They just forgot that somehow.

Leo: Left that out. Well, I mean, their business is advertising. I'm maybe not surprised. Furthermore, there are security issues, potential security issues. On the other hand, it's speedy and lightweight and, you know, I'm pretty much sticking with it as a way to run Google's applications.

Steve: Well, and certainly that is one of their targets. Now, you might argue that add-ons are the way that these missing features could be produced. And certainly it is Firefox add-ons, for example, NoScript and others with really nice ad-blocking features and so forth, which are very popular among users. So you could say, okay, well, Google has said that they're going to be making an API available for add-ons. Unfortunately, they've also explained that add-ons will have the problem, or the capability, of being able to breach the containment of the Window tabs. So to the degree that they're able to create containment, the add-ons are powerful enough to cross that boundary.

So I would argue that it makes much more sense, if you really care about security - and nothing Google has done so far really demonstrates to me they care about security or privacy - if they do, give us all the features in the native browser so that we don't need to add potentially insecure or security-violating add-ons in order to make up for what the basic browser doesn't have. And it's not like they have to mess up the UI a lot. Have an advanced line on a menu somewhere that most people won't bother going to, but which people like myself and you, Leo, and Firefox users would find everything that they want

hidden in the advanced line of a menu option. I mean, it's not hard. It's just missing completely.

Leo: Yeah, yeah. Well, there you go. That's kind of a manifesto to Google to make your browser better.

Steve: Yeah. I'm just - I'm unimpressed. Again, I don't know who they're aiming it at because, as you said, they borrowed market share from Firefox, and then they quickly gave a lot of it back because Firefox users must have just said, wow, I can't do anything with this. I don't have any of...

Leo: Yeah, I think last week everybody tried it, you know, all the geeks tried it. I doubt very many people are using it as their sole browser anymore. Certainly not after listening to this. And especially since there are many good quality choices that give you much more security. It's not like you need this browser.

Steve: Well, exactly. I mean, Firefox has a huge market share. It's half of the people who come to GRC. It's more than half of the people that go to TWiT world and Leoville and all of your domains, Leo. And so clearly that's a mature solution which also has a really, really strong - I can't think of the term.

Leo: Security model or...

Steve: Ecosystem is what I was looking for.

Leo: Ecosystem, yeah.

Steve: it's got a huge ecosystem and add-on feature set that lets people really make the browser work the way they want it to.

Leo: Right. Yeah. No, I'm sticking with Firefox. I'm using it right now. And on both Mac and Windows that's what I use. Although I have to say I'm happy with IE7, too. And I'll look at IE8, depending on what you say.

Steve: How it comes along.

Leo: How it comes along. Steve Gibson is the host and majordomo of GRC.com, a great site for your security needs, for ShieldsUP!, lots of great utilities. Of course the fantastic SpinRite, the world's best disk maintenance and recovery utility, a must-have for everyone. GRC.com. When you get there you'll find 16KB versions of this show for quick download, if you don't mind a little audio quality loss. You'll also find transcripts which have actually no audio quality but are much easier to understand sometimes. A lot of people read along while they listen. And Steve's show notes, too.

That's all at GRC.com. Next week, a question-and-answer session.

Steve: Yes, so I wanted to remind our users, GRC.com/feedback will take you to a web page where there's no scripting required, and you're able to send questions and comments and thoughts to me, which I will peruse prior to and while I'm preparing next week's Q&A stuff.

Leo: Very good.

Steve: And the week after, we're going to do one of our deep propellerhead shows.

Leo: Oh, I love those.

Steve: We're going to do DNSSEC, the languishing but clearly important DNS security spec and model, and talk about exactly how it is and how it works. Probably by that time I will have my DNS work finished. And one of the things it will show you is whether your ISP's DNS servers are supporting right now DNS security.

Leo: Ah.

Steve: And lots of other cool things, too, Leo.

Leo: Very good. Thank you, Steve Gibson. We'll catch you on the flip-flop. Take care. Have a great week.

Steve: Talk to you then.

Leo: See you next time on Security Now!.