SECURITY NOW!

Transcript of Episode #219

Badly Broken Browsing

Description: In preparation for episode #221's guest, John Graham-Cumming, who will take us on a detailed walk-through of the JavaScript language's security problems, this week Leo and Steve examine the sad and badly broken state of web browsing in general, and how we got to where we are.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-219.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-219-lq.mp3

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

Leo Laporte: Bandwidth for Security Now! is provided by AOL Music and Spinner.com, where you can get free MP3s, exclusive interviews, and more.

It's time for Security Now! with Steve Gibson, Episode 219 for October 22, 2009: Browser Scripting.

It's time for Security Now!, the show that covers all things security oriented. And Mr. Steve Gibson is here once again to terrify us with the bad news about security. Hey, Steve, how are you today?

Steve Gibson: Hey, Leo, it's great to be with you again, as always.

Leo: Thank you. Thank you. Now, we have a little programming change, don't we.

Steve: We have a little programming glitch. Yes. As our listeners know, we had talked about for the last couple weeks that we were going to have a rare guest appearance from John Graham-Cumming, whom you have known for years, and I have known. He's been a participant in the GRC newsgroups. We've referred to him recently a number of times because he recently wrote "The Geek Atlas," which is that terrific book that talks about 128 different locations all around the world where things of interest to geeks occurred.

Well, on September 27 he created a blog posting, which he sent me a link to, because he had just finished giving a presentation at the Virus Bulletin 2009 conference, where his presentation was titled "JavaScript Security." And of course now I think of that as the oxymoron to equal military intelligence, is to say "JavaScript Security." Anyway, it was titled "JavaScript Security: The Elephant Running in Your Browser." And so I was excited to have him join us this week to give us all the gory details, I mean, in detail about what's, I mean, fundamentally what are the problems with JavaScript relating to the security of web things.

Unfortunately, I got mail from him shortly before we began recording saying that he was just returning to the UK. He was actually here in the states yesterday, just returned to the UK. He learned just then of a death in his family. So he said, you know, "I can't do the podcast." And I wrote back immediately, and I said, "Well, of course not." So if he's around and his schedule permits in a couple weeks, I hope to have him do that.

However, there's a broader sort of overview that I wanted to give. I actually have a good friend of mine who's an ex-Microsoftie who was involved in the security model for the recent versions of IE, and we had some interchange about this topic. Which was, well, Loren was arguing, wait a minute, you know, is this really JavaScript's fault? Isn't this something bigger? And so I want to talk about with you, Leo, this bigger idea, that is, what's going on in general with the so-called Web wherever we are, 2.0, 2.1, moving forward? Is this ready for primetime? How is this model of the way servers and browsers are interacting today, how is it letting us down from a security standpoint? So we've got a lot to talk about. And then we'll still have John to come in and talk at the JavaScript level about this idea.

Leo: Yeah, that's going to be very, very interesting. He's a programmer. He writes a really excellent antispam program.

Steve: Well, he's done that. He did an implementation actually of the Perfect Paper Passwords system.

Leo: Oh, did he. Oh, that's neat.

Steve: Yeah. And he's, I mean, he's a coder. And a great guy. So, yeah, we will have him hopefully week after next, if his schedule permits. But he had to drop out of this one.

Leo: Fine, fine.

Steve: But we've got lots of news and errata and still some stuff to talk about.

Leo: Good. Well, what do you want to - you want to start with the errata?

Steve: Sure. First of all, this may not quite be ready for primetime because it didn't work for me. But we've spoken recently of Mozilla's move to begin taking responsibility for the state of plug-ins in the Firefox browser.

Leo: Right.

Steve: And we know that the first thing they did was they began warning people of a persistent problem that Adobe's been having with Flash. There's been vulnerabilities in Flash. For whatever reasons, the bad guys have been jumping on these Flash vulnerabilities very quickly and been quick to exploit them. So that meant that users staying current with the latest version of Flash was important. The problem is that there wasn't a mechanism in the plug-in model for notifying people when a newer version of Flash was available. So the browser, that is, the container of the plug-in, decided, okay, we're going to start taking some responsibility for this.

What they discovered when they launched an update to both the version 3.0 and the 3.5 browsers is that more than half of users of Firefox were running an obsolete, known insecure version that was known to have active exploits being pursued against it. So they thought, wow, this is a big deal. So they've decided, Mozilla has, to broaden their attack on being responsible for the things that they're running as plug-ins.

Now, right now there is a page at Mozilla.com that all of our listeners can go and try. I've heard that it's working, but it didn't work for me. I, well, first thing I had to turn NoScript on. I had to allow Mozilla.com to function. But it's Mozilla.com/plugincheck, all one word. And the page came up for me, but it said it had a problem and asked me to try back later. And it's been doing that now for the last day. So I don't know what's going on. This is me running Firefox, I can't remember if I'm at 3.5 on this main machine of mine or still on 3.0. I might still be on 3.0.13 I think is where we left off on the v3.0 train.

But Mozilla.com/plugincheck. Right now they're doing this as a you go to that page, and that page, with scripting, will interact with your version of Firefox, knowing what the latest versions of - I think they're like at 15 or 16 different plug-ins they're checking now, and they're going to be expanding that in the future. And so the way they're doing it now is you go to that page. Slated for v3.6, which I believe is due out next month, that is to say November 2009, slated for that version, that version will have this functionality integrated into it so that you will be shown on pages which use insecure or down-version plug-ins that that's the case. Somehow they will have a way of notifying users on the page that, oops, this page is using a plug-in for which there is a newer version. So that'll be moved into the browser. For the moment, you can go to Mozilla.com/plugincheck and check the versions of all your plug-ins.

Leo: Yeah, it's working for me. And furthermore, it did a really cool thing. I don't know if we talked about this last week. But when I ran it, it said, oh, the Microsoft .NET Framework is unsafe. We're removing - remember we talked about, a couple of months ago, about this plug-in.

Steve: Yeah. What was annoying people was that Microsoft had disabled the Remove button, so that it was - you could not remove it. And that was after surreptitiously sliding it in and not letting anyone know that it had happened. And yes, that's another item of news, I'm glad you brought it up, is that Mozilla has decided they're going to disable it because it has known insecurities, and they don't want it running in their browser.

Leo: Disabled it. And the interesting thing is, with the assent and approval of Microsoft. Because Microsoft put out a security bulletin saying we've got a problem here. And so, you know, I was very pleased. This is the second time now with the new Mozilla 3.5 that I've run it. The first time was after upgrading to Snow Leopard, and it said this is bad. This Flash is out of date and dangerous. It gave me a new one. And then just the other day I launched Mozilla, and it says, just so you know, we've disabled two Microsoft plug-ins because there's a severe exploit with these plug-ins. I think that's exactly, I mean, the browser is the first line of defense.

Steve: Yes. Exactly. It is becoming, and this is really what we're going to talk about today, it is becoming the new paradigm for the desktop, with this whole notion of web-based apps, data in the cloud, and the idea that you could, for example, go to any machine and login to Gmail, and there is a good working mail client running within a browser where the browser is the container. And so you're right, it's a little bit like the browser is becoming the operating system, and these are apps running in the operating system.

Leo: Mm-hmm, mm-hmm. So it's good. It's got to fix it. This kind of ties into our subject of the day, actually.

Steve: Yeah, it really does perfectly. So another little blurb popped up on my radar. We didn't have a ton of security news except that I thought our listeners would be interested in knowing there was an article both in USA Today and PC World covered a story that the scareware industry is becoming more aggressive now. There's a product which - well, "product" - badware which is calling itself Total Security 2009. And if you do something to get this onto your system by mistake, it now locks out every other application on your machine except Internet Explorer. So this is a Windows-based malware. And no matter what you try to do, if you try to do anything else, you get a pop-up with sort of a fake security scan telling you that your system is infected with viruses and malware and trojans and scary things. And then the only thing it allows you to do is to use IE to go to a site and purchase this thing for $79.95.

Leo: [Laughing]

Steve: When you purchase it for - oh, and then there's an extra $19, like, download insurance or something. It's like, oh, my goodness.

Leo: But, now, are you purchasing something really valuable, or are you purchasing a spyware?

Steve: You're - basically you are succumbing to extortion. You've already got...

Leo: Oh, I see.

Steve: No, this is just to get money.

Leo: It's a fix. Okay.

Steve: Yes, it is just to get money. So...

Leo: So it's a legitimate fix for a problem they caused.

Steve: Well, yes. Although it stays on your system. So it doesn't even...

Leo: Oh, please. It's not even a good fix.

Steve: It doesn't even remove itself. So but the idea is that it locks you out from doing anything else. You can't run antispyware programs.

Leo: Really.

Steve: You can't do, I mean, yeah. The only thing it lets you run is IE for the purpose of purchasing it. It then gives you, if your credit card transaction goes through for $79.95, then you get an unlock code which you can give it, which basically you've succumbed to the extortion. And then you can run other programs.

Leo: What do they call this virus?

Steve: It's called Total Security 2009.

Leo: Total insecurity.

Steve: Total nightmare. Yeah. And so it's interesting because...

Leo: So is this related to the Antivirus 2009 problem earlier?

Steve: It's the same genre. And we're seeing more of this. It's sort of a - it's using social engineering to convince people to some degree, I mean, apparently it says it's not safe to use anything on your machine, so we're not going to let you do that. You have to buy this. And so there, unfortunately, there is a cross-section of users in the PC community who, I mean, I've talked to friends who, you know, non-computer-savvy friends who say, yeah, I get this popup that says it scanned my computer, and I have viruses. It's like, oh, no no no no no.

Leo: Boy, that really is a - that is blackmail. That is...

Steve: It is. It's extortion.

Leo: You can't run any program until you pay them their $80.

Steve: Yup.

Leo: Or $19.95 for the premium support services.

Steve: Exactly.

Leo: Oh, that is - so, now, do you prevent yourself from getting it in the same way that you would any other virus or spyware? This is...

Steve: Yes. I mean, I'm sure that the good antimalware tools will quickly come up to speed. They'll hopefully see this coming in, block it from your computer, prevent you from getting this in the first place. But if you get yourself infected somehow, this is what it does. Basically it's pay us $80. And until you do, you cannot use your computer.

Leo: Wow.

Steve: So watch out for that one. If our listeners, I mean, our listeners are probably savvy enough not to fall into this trap. But they may have family and friends that are not listening to this podcast, so...

Leo: Right. Well, I know I'll get calls on the radio show. Oh, I'll be hearing about that one.

Steve: Total Security 2009 is anything but.

Leo: Many of my listeners got bit by the Antivirus 2009. So this is just, yeah.

Steve: Right. Yeah, it's exactly - it's the same genre. And it's interesting, though. Again, it's sort of, I mean, it's not using any social engineering that any of us, any of Security Now! listeners would fall for. But it's just confusing enough that it raises that doubt. It's not just bringing up a big skull-and-crossbones and saying, hah hah hah, you must pay. It's like, oh, we're trying to help you. We're going to help you get these bad things off your computer. So, yeah, thanks.

So our good friend Bruce Schneier, whom I refer to often, a security guru and cryptographer, had an interesting blog posting on October 19, 2009, which was a reaction to the mega Patch Tuesday that we talked about last Tuesday. I mean, we talked about in our last week's podcast because it was just the previous Tuesday, which as we know is the biggest patch event in Microsoft's history. It's the largest number of fixes in one one-month period. And Bruce coined a term that I liked in his blog posting. He called this the "patch treadmill."

And there were two paragraphs that I wanted to quote from Bruce's blog posting because I thought they were really apropos. He said, "Patching is essentially an impossible problem. A patch needs to be incredibly well tested. It has to work without tweaking on every configuration of the software out there. And for security reasons it needs to be pushed out to users within days or hours, if possible. These two requirements are mutually contradictory. You can't have a piece of software that is both well tested and quickly written."

Leo: Yup.

Steve: Which I thought is, I mean, it's exactly right. I grumble at Microsoft taking longer than it seems that they should when a known problem is hanging out there, flapping in the breeze, being exploited, and we're complaining that there's no fix for it yet, week after week after week. Yet look at the spread of platforms they have and the possibility of side effects.

And so the second quote from Bruce's blog posting, he says, "The real lesson is that the patch treadmill doesn't work, and it hasn't for years. This cycle of finding security holes and rushing to patch them before the bad guys exploit those vulnerabilities is expensive, inefficient, and incomplete. We need to design security into our systems right from the beginning." This is something that we're going to be talking about in the show's content here coming up because, I mean, this is key to the problem we have today. So Bruce says, "We need to design security into our systems right from the beginning. We need assurance. We need security engineers involved in systems design. This process won't prevent every vulnerability. But it's much more secure, and cheaper, than the patch treadmill we're all on right now."

Leo: Hmm. Interesting.

Steve: So from his standpoint, he sees what we experience from the outside, which is that security is still not being baked in. Security is an afterthought.

Leo: You're saying measure twice, cut once.

Steve: Well, yes.

Leo: Do it right first.

Steve: Exactly. And I've talked often about why it is fundamentally difficult to do security. It's the weakest link in the chain model. And I used this analogy just last week, where if you have a chain of links, every single one of them must be strong because it just takes one of those to be a problem, and that creates an exploitation. Whereas the chain works, and most people stop as soon as the chain is a chain. As soon as everything, you know, you pull one end, and the other end moves along, it's like, oh, look, our program is running. The system works. And it's time to ship it because they're always under the gun and late. But that doesn't mean that it's going to work when it's being challenged by somebody actively being bad. And that really - it's a different way of looking at it. And as Bruce says, it requires that security be taken to a level of seriousness, I mean, baked in, that still doesn't exist today. It's just not the way we're doing things.

Leo: Yeah. Well, you've got all sorts of issues with legacy compatibility, which is inherently a problem. It's going to keep you from doing the right thing in terms of security.

Steve: Yup. That's a very good point. You're...

Leo: You'd almost have to start from scratch; right?

Steve: You're often making compromises because you can't - and this is what's been, I mean, really Microsoft's claim to fame has been upward compatibility, or backward compatibility. As they're moving forward, they're still keeping all this old stuff alive. And even to the fact where, for example, with Windows 7, which is being released, what is it, tomorrow?

Leo: Yup.

Steve: As we're recording this?

Leo: Today as the show comes out, yeah. We're doing a big party tomorrow, yeah.

Steve: Yeah, Windows 7 is being released. And controversially, they've dropped some compatibility with the past, so they're having to put a virtual machine in, in order to run an older version of Windows for things that require - it's Windows XP, right, that they're having to allow you to run in Windows 7 in a VM.

Leo: Yes. Yeah.

Steve: And people, of course, complain like there's no tomorrow if their particular widget is not compatible with some future version of Windows. Often it's like, wait a minute, we don't have the source code anymore. We can't recompile it for the new version. That's gone. We needed to be compatible. So it really is a challenge.

So some interesting errata. I wanted to note that PayPal has fixed the bug that I discovered and other of our listeners have since confirmed, in their eBay payment system. Remember that I called it the dongle bypass bug.

Leo: Yeah, right.

Steve: Where if you were paying for something in eBay, and you went to PayPal to do that, you would give it your regular credential, you'd give it the password that matches your email address. Then it would prompt you for your dongle information. And what I discovered purely by mistake was if you, instead of giving it, you hit the back button, it takes you back to that login that you had just left, but with you logged in this time. Not even - it's grayed out. You're not even able to put that data in again. And it says you're already logged in, click below to proceed. So when you click that, it jumps you over the whole dongle question, and you're right in without using your multifactor authentication device. So it was sometime last week that I was purchasing some vintage computer stuff on eBay...

Leo: Again? We've got to cut you off.

Steve: It's bad. The problem is I've got searches now that are, you know, I've got my little search spiders out on eBay. And every morning it's like, oh, look what we found for you.

Leo: There's new stuff.

Steve: It's like, oh, I have to...

Leo: Most people are buying new gear, Steve.

Steve: I have to have one of those.

Leo: Most people say, oh, there's new Macs out. They're not saying, oh - they're saying Windows 7. They're not saying, oh, look, here's something 30 years old.

Steve: Well, as a matter of fact, what I purchased was the original source code listing for the TECO editor in PDP-8 source code because there's no better way to learn a language like PDP-8 assembly language...

Leo: Interesting. Interesting.

Steve: ...than to read what an expert in that language has done. I mean, I could, over time, if I, like, was coding a ton, I would end up developing some of my own tricks and approaches. But an expert coder already knows that. And so when I saw that this listing was made available, it's like, oh, I would love to read that.

Leo: Now, who made it available? Was it the guy who wrote it, or...

Steve: It was just - it was a copy that was - in fact...

Leo: Somebody just had, huh?

Steve: ...the person selling it knew, he himself printed it out in the basement of Georgia Tech on a chain printer or something. And then it was interesting because I had some correspondence with this person's wife, who explained to me that - because we were negotiating the shipping cost because I said I'm not in a big hurry to get it. It's been sitting on a shelf for 30 years. I don't mind if we use snail mail to get it to me.

Leo: And how big is it?

Steve: It was about, from the picture, it looked like it was about a two-inches-thick listing. And so anyway, she said that she had received, after the auction closed, she received email from a museum asking whether the purchaser, that is in this case me, would be willing to donate it to the museum.

Leo: No.

Steve: And so, well, after I've read it, you know...

Leo: Oh, maybe, yeah, sure, why not.

Steve: I'm not going to key it in. So I don't need to have it forever. And I certainly don't want it to wind up in a dumpster and being landfill. So I wrote back and said yeah. And so she gave me all the museum contact information. And I'll put a note, sticky note on the listing. And they can have it when I'm through reading it.

Leo: That's fantastic.

Steve: So I thought that was a kick. And I did want to note, you probably saw that the Kindle price has dropped.

Leo: Yes. I did see that.

Steve: Down to $259.

Leo: And they added an international radio into it.

Steve: Yes, so...

Leo: And Barnes & Noble is selling one.

Steve: There's a lot of these.

Leo: Yeah, yeah.

Steve: Yes, Barnes & Noble, they call theirs The Nook. It's like, okay, I guess that's instead of Book, it's Nook.

Leo: What you really don't want to say is the Nook eBook Reader because...

Steve: The Nook eBook Reader, no.

Leo: ...that's not good.

Steve: And it's a wacky thing. It's got a dual - the Barnes & Noble has a dual screen. The upper portion is our standard eInk display that everybody's pretty much using, Sony and all the Kindles and now Barnes & Noble. But then they've got a lower color LCD which is a touchscreen. And so it's like, okay, well, that's interesting. So and they say, like, you display your photos and things. So you can - it's sort of supposed to be sort of a dual purpose, I guess. And Best Buy and Verizon are getting into the business. IREX, a spinoff from Philips, has announced. Plastic Logic will have theirs shown at CES, where I think you're going to be this year, aren't you?

Leo: Yes, we're going to cover the show, yeah.

Steve: So maybe if you have a chance, it'd be interesting to see what you think of their reader.

Leo: Oh, we will, don't worry. That's for sure, yeah.

Steve: And then...

Leo: You should come out. Be part of it.

Steve: I'll think about that. That would be fun.

Leo: I mean, there's no COMDEX anymore. This is the closest thing we've got to a gathering of the tribe.

Steve: It's definitely that. And I wanted to ask you, Leo, Audible being a sponsor of ours, I'm getting ready to try walking on the wild side.

Leo: Not audio books.

Steve: I am.

Leo: Oh, my god, Steve. Be still my heart.

Steve: Well, because I have to read a couple books that are not available on the Kindle. Actually I'm going to reread one of Bruce Schneier's books, "Practical Cryptography."

Leo: I have that. It's a great book, yeah.

Steve: It's a fantastic book. And I'm just - I'm going to read it cover to cover as I begin to get my sleeves rolled up and to plow into CryptoLink. I thought, oh, just going to read it again, just to sort of brush up. But that means that I can't be reading it on my stair climber as I do now where I'm reading Kindle book, and I synchronize my Kindle DX, which is the large screen, which I have rubber-banded to the stair climber's control head. So I thought, well, okay, I ought to try an audiobook when I'm on my stair climber. So I wanted to ask you, given no other consideration except convenience, like remembering where you left off, not losing where you left off, being able to back up a little bit easily and so forth, what's the best device for reading...

Leo: Well, you already have a Kindle. I mean, the Kindle will do it. You can just put them on the Kindle. And that might be convenient because then you've kind of got it both ways. You know, Amazon owns Audible. I really had hoped that by now they would have synched the two, so if you had the book on the Kindle, and you had the audio book, that you could, like, it would highlight it as you're listening to it.

Steve: Boy.

Leo: And you could, like, have - wouldn't that be nice?

Steve: That'd be nice, but tricky because you'd have to have a control channel of some sort.

Leo: It needs to have an index; yeah.

Steve: Yeah, in the audio.

Leo: Probably not going to happen.

Steve: Yeah.

Leo: Anyway, but Audible does use a proprietary format that is designed to support those features - the bookmarking, the chaptering and all of that stuff. So it's an MP3 wrapped in this .aa format. And that's why not just any device supports it. You have to have a device that supports Audible. I think, given what Apple's done with the interface, an iPod Touch would probably be the best. For instance, they have visual scrubbing. So you can put your finger on - you're listening to the book. You can put your finger on a dot and scrub forward or backward. And the farther your finger is down the page, the slower the scrubbing is. So you have a lot of granularity. They also have a 30-second rewind. And I find that the most useful with books because sometimes you're doing, you know, you're listening to a book, and your attention wanders. You got pulled over or something. And then you just press the 30 second, 30 second, 30 second, it jumps back 30 seconds at a time.

Steve: Oh, okay. And I happen to have, wouldn't you know it, an iPod Touch, so that's perfect.

Leo: Oh, perfect. Yeah, update it with the latest 3.0 software, which I think will cost you some money if you haven't updated it. Like five bucks or something. And then...

Steve: I think I did when 3.0 happened.

Leo: Then you're golden. That I think is the best experience. It's not great if you're running or something because you have to use the screen to control the book or the music. But perfect on a treadmill or a bike, anywhere you could prop it in front of you because then you have easy access to those controls. It's just the screen gives you more capabilities than just a click wheel would. And I don't know, I haven't tried it on a Kindle, but I can't imagine it has much of an interface at all.

Steve: Yeah, I mean, that was my reaction when you mentioned it because I know the Kindle of course does MP3 stuff. And the Kindle is a...

Leo: It's an Audible device, yeah.

Steve: ...is an Audible appliance, okay.

Leo: As is the Zune, as is, I mean, pretty much everything. But I think the iPod is the best. You already have a Touch, you're gold, you're good.

Steve: Yeah.

Leo: That's the way to go.

Steve: Okay, cool. Well, and I do have a fun and always different SpinRite story. This one was - the subject was "SpinRite 6 Saves My Bacon." A person wrote to us whose name is Wray Buck. And he said, "I used earlier versions of SpinRite way back when a large PC hard drive was measured in megabytes rather than gigabytes. I lost track of my floppy with the program on it, and SpinRite receded into dim memory. Then recently one of my computers abruptly refused to boot, looping unmercifully on the failed boot, choose safe boot, normal boot, et cetera."

Leo: Oh, I hate that.

Steve: "I finally slowed the boot down by getting into the BIOS edit, enough to see a fleeting screen error 1720, imminent hard drive failure warning. The BIOS setup had a self-test that confirmed that my boot drive fails the test and recommended replacement. But I needed my data. The manufacturer's and Microsoft's websites were not particularly helpful. I was not even able to boot from the WinXP install disk. From the dim recesses of my memory I knew I had at one time used software that would repair and/or move data from bad locations to good. I Googled my mind and came up with..."

Leo: [Laughing] Oh, if only I could Google my mind.

Steve: "I Googled my mind and came up with Gibson something."

Leo: Gibson.

Steve: "On my remaining good computer I Googled the Internet for 'Gibson' and found again Gibson Research and SpinRite. It didn't take me long to decide to purchase v6 and make a CD for the sick computer. Level 2 didn't find any problems. And there was no change in symptoms. So I just kept increasing the level of SpinRite and attempting reboot. Finally, at Level 5" - we're at Level 5 - "an unrecovered sector appeared. After waiting for the process to complete, reboot finally opened Windows XP. I then had it do chkdsk, and it found some orphaned segments and deleted some files from the table. But in any event, I now have hope of recovering nearly all the data and programs on that hard drive. And I have SpinRite to thank."

Leo: That's a nice story.

Steve: So it was a great story.

Leo: That's a great story.

Steve: And I thank him for sending it to us.

Leo: So we're going to talk about browser scripting. I guess kind of a setup for Paul.

Steve: Yeah, we're going to, exactly, set things up for John in two weeks.

Leo: For John, yeah.

Steve: We're going to talk about sort of the problem with the way we're doing things today.

Leo: Which is - so it's not just scripting.

Steve: It's not just scripting. It's bigger than that. We'll talk about it.

Leo: So, Steve, let's talk browser scripting.

Steve: So, well, the whole web, the way the web is working - I was at Starbucks this morning when they opened at 5:00 a.m. And they always ask me how my day is going, which I think is funny because it hasn't really yet. Nobody else is awake except the people that had to be there at Starbucks at 4:30 to get the store open for 5:00, and me. But I said, well, it's podcast day, being Wednesday, when we record this. And the manager, who's being shared between two stores so he doesn't really know a lot about me, as much as I'm a regular there, he said, "Oh, what's the podcast about?" And I told him it was about Internet security-related topics.

Anyway, the gal who was busy stocking the carbohydrate bar that they have there said that her computer had to be completely reset, scraped and scrubbed and reinstalled, because she went to a sewing site, a sewing website that she'd been going to for a long time, and it infected her computer, and it no longer worked, and she lost everything. But she guesses that's just sort of the way it goes. And...

Leo: I think a lot of people are very fatalistic now about this stuff.

Steve: Yeah.

Leo: It's like, what can you do?

Steve: Yeah. Well, I mean, but it strikes me as so sad that it's just like, oh, you just sort of shrug. I mean, you're right. There is nothing they can do. Most people who will fix a computer, they say, oh, well, you know, it's not worth our time trying to figure out what happened, we'll just reformat it, you know. Do you have your original install disks, and we'll just set it up for you again. So it's sad that people are fatalistic about it. And I explained to her, I said, well, you know, it's not that the sewing site that you went to is evil at all. It's that they're not security experts.

And unfortunately, to create a sophisticated website - I mean, who knows, I don't know the details of the site. But it probably has, like, online forums, and you can join their community, and you're posting things. And, I mean, all of this fancy, next-generation activity that is web based, based on the browser and a remote server, I mean, it's what people want to do. We know pretty much it's the future, that we're moving to the cloud. We are moving to browser-based apps of one sort or another. We have, as we were talking about earlier in the show, plug-ins which facilitate much more rich experiences than you're able to get back in the pre-interactive model.

The problem is that it is difficult to create a site, that is, for amateurs to create a site. And in fact there's a commercial running right now that I get a kick out of. In fact, it captures my attention so much, it's one of those where I don't know what it is they're advertising. And there's a series of vignettes. And the one that captures my attention is a - it looks like a store owner and his wife are - because there's sort of a counter and customers in the background. And they're in the foreground. And he looks up from a big 500-page book, and he's flipping the pages, and he says, "We're doing our own website."

Leo: [Laughing] Uh-oh.

Steve: And wife is sort of, like...

Leo: Uh-oh.

Steve: Wife is rolling her eyes around, kind of like shaking her head a little bit, it's like, oh, my god, we have no idea what we're doing. And he's flipping pages and, you know, we're going to do it ourselves. And it reminded me, and this topic reminds me, of the comment that an ex-employee computer developer of mine in the early days of Gibson Research said. And I've shared that before on the show. It's when Microsoft came down from Redmond, the product manager Nevet Basker showed me the pre-release version 1.0 of Visual Basic. And here was this toolkit, I mean, Bill Budge on Apple II created the pinball construction set, where you just sort of dragged and dropped elements of a pinball arcade machine on the screen, and it was alive. And it just blew everyone away when he had created this, like this pinball, visual pinball editor.

And essentially that's what Microsoft did programming Windows. You had a palette of buttons and dropdowns and list boxes and edit controls. And you just dragged these things onto this empty application window and set them up visually the way you wanted to. And then you went behind the window and wrote little scriptlets for each of the different controls and hooked them together that way. And before you'd know it, you had a running application.

Anyway, so Millard, seeing this, we were sort of - we got the whole presentation from the product manager. And I said, "So what do you guys think about this? I think this is going to change everything." And he sort of had his head in his hands. And he says, "Ooohhh."

Leo: This changes everything just like adding fonts, giving people the chance to use fonts changed everything in desktop publishing.

Steve: Exactly. Who's going to control the colors? He put his head in his hands, he says, "This makes it way too easy for anyone to program." And so really that's where we are right now with the state of the art in web stuff. I mean, if you think about it, we really are still in the hacking stage. We're inventing one language after another, one acronym after another. I mean, you've got PHP hooked to SQL, and then you've got AJAX and you've got all of this stuff. And there's no, like, right way to do it. And then you mix that in with prepackaged open source things where you sort of grab this and add it to your server and glue it in. And meanwhile the husband's flipping through the pages, trying to figure out, okay, how do we do commerce? It's like, oh, my god.

And is it any surprise that, again, we have to understand that bad guys have an intention that is completely contrary to the rest of us. They're looking for opportunity rather than what the creators are looking for success. They just want it to work. The guy creating his first website is struggling to make it work. So once it sort of does, there's this huge temptation to publish it, to make it live. Oh, look. And then to check in every few minutes to see if anyone has gone to the website yet. Do we have any - how many members do we have in our forum? And oh, look, the forum's working. It's like, yes. But doing this correctly, doing it securely is amazingly difficult.

And so it's no surprise that the well-meaning sewing website put a bunch of this stuff together using toolkits or maybe some prepackaged design-your-own-site. And before they knew it, some bad guy realized, oh, look, they've got an old version of WordPress that they're using, and we're able to exploit a known cross-site scripting vulnerability in that in order to inject a malicious script into the content such that when people who have some unpatched browsers come by, we'll be able to run our script on their browser. And before you know it, Total Security 2009...

Leo: [Evil laughter]

Steve: ...is installed on their machine.

Leo: Happy Halloween.

Steve: I mean, this is how it happens.

Leo: Yeah.

Steve: And so...

Leo: Now, people are going to accuse you of elitism. They're going to say, well, yes, the programmers want to keep it to themselves. But there is a skill set here.

Steve: Yes. You know, doctors have to prove...

Leo: Yeah, good point.

Steve: ...that they know how to fix people, or that they've studied the bones of the body, and they've put in their time before they're allowed to touch you. And lawyers have to pass the bar. They've got to go through, I mean, and here I am, across from UCI, hanging out at a Starbucks which is set up like a library, we've talked about it before, how I've spent days there working on code. And it's full of students, and I see the LSAT books and the MSAT books. And we happen to have, like, a huge medical student community. So I listen to them quizzing each other with flashcards and all this, and what they go through.

And there's nothing like that for any of this, for computer programming, for anything relating to something as crucial as the security associated with a website that is asking you for your credit card and your information. We can assume, and lord knows we've beat this to a pulp, the security of getting your data, your credit card information to the server in a way that prevents it from being eavesdropped on, with talking about SSL and the browser model and all that, as we have for the prior two weeks. But now it's sitting on the server. Nothing regulates or requires or specifies how that's handled.

And it's one of the reasons I didn't - I just didn't feel comfortable when I was creating GRC's eCommerce system to buy something off the shelf. First of all, I wanted to write my own. I wanted the experience of it. But I'm acutely aware of all of the different types of things that can go wrong. And so for example I chose a database where nothing written on the hard drive is ever in the clear. That's absolutely secure. There is AES encryption, actually I think it's Blowfish, I think it's Bruce's encryption that...

Leo: Bruce wrote Blowfish? Wow.

Steve: I hope I'm not wrong. I think he wrote - there's Blowfish and Twofish. And I think Bruce wrote Blowfish, if memory serves. So...

Leo: Yes. Designed by Bruce Schneier as a drop-in replacement for DES or IDEA.

Steve: Yeah, and it's a fantastic cipher which has withstood the tests of time. I mean, it's absolutely great. And I'm using large blocks and large keys and doing everything right. And the key is not on the disk. I went through all kinds of things because I wanted mine to work right. But I went to tremendous lengths, knowing how important it was to me and to our customers that their data be safe. And unfortunately security is, in most situations, an afterthought. And it's not something that we can afford to have as an afterthought. So I totally get what you mean, Leo, about the elitist approach. But at some point this has to change. And frankly, I don't see how it's going to, unless it's unfortunately like onerous regulations of some kind where...

Leo: Do you think a certification, like, I mean, there are security certifications; aren't there?

Steve: Certainly. Various sorts exist. But then what would the model be? So we have security certifications. So would it be that, like, you can't...

Leo: You're not allowed to write secure software? No, I think the deal maybe is not that you're not allowed, but that if you're a certified security professional or certified security coder, that there's a certification on your software, and that that may be somewhere publicly visible. You know, this is - I don't know. It's just setting up more bureaucracy. But it is something we need.

Steve: Well, and it's like - another thing that I get a kick out of. You go to these sites, and they have that Hacker Safe seal on them.

Leo: Yeah, that's bogus.

Steve: Exactly.

Leo: That's just a money-making...

Steve: It means nothing about the security of the...

Leo: Well, I don't know, they test it somehow or something. But really it's basically - it's my understanding that you're just buying - you buy this badge because it makes your users feel better.

Steve: Well, or it might be, like if I were in the bogus security business, I would have ShieldsUP! going out and testing people's websites. I'd be doing port scans...

Leo: Certified by ShieldsUP!.

Steve: Yeah, exactly. And I'd have revenue stream that I don't have now. I could do it trivially. But I'm not going to because it doesn't mean anything to the user about the security of the server, I mean, about what happens to that data after it lands at the other end. And is there a way for bad guys to get in? We've talked about using SQL in the background for the database and how it's possible to enumerate the fieldnames in SQL through an insecure browser application and literally dump out the database and do this all remotely. I mean, these are things that actually do happen.

And so my sense is that we're still - we're in the pioneering stage. We're hacking around with different solutions. Yet the world didn't wait. The world said, oh, great, let's use this stuff. Even though it's really not ready for primetime. And there's no control over how the system functions. It's like, oh, it works? Let's make it public. Let's start taking credit card numbers. Let's start, you know, let's get going with commerce. And I don't know how this ever changes. But as you said, users are becoming now just abused. They've been beaten up. And it's like, oh, well, I went to do something on the Internet, and I got infected with Total Security 2009. Now I had to pay them $79.95 in order to get my computer back. And it does happen.

Leo: Somebody in our chatroom is pointing out that the credit card industry does have such a security standard. It's called the PCI Security Standards. It's PCISecurityStandards.org. And they do, it's interesting, they do training for merchants and the general public on maintaining security. I mean, it's not really for programmers. But it's for anybody who takes online payments.

Steve: Yeah, and unfortunately it is virtually useless.

Leo: Really.

Steve: I have not talked about it before because the stories were sort of dry and boring, and I didn't know that anyone would really be interested, although we are sort of on that topic today. But many of the instances of massive credit card loss are from PCI-certified sites.

Leo: Oh, well.

Steve: So, I mean, it's one of those certifi- it's what you'd expect. It's a nice - it's another stamp or seal. But in practice there's no enforcement behind it.

Leo: It's run by the credit card companies themselves.

Steve: Yeah, in order to make people feel better about it.

Leo: Feel better. Ah, well. Nice try.

Steve: Yeah. I mean, it's a bunch of bureaucracy. And it's like, okay, fine, so we have that, thank you very much.

Leo: It might be a step in the right direction. But...

Steve: It's beginning to be, and maybe it demonstrates some of the will. The problem is that, again, there's this disconnect. It's actually doing it is so difficult that in practice it doesn't get done.

Leo: Yeah.

Steve: So on that happy note...

Leo: [Laughing] So much for that.

Steve: ...we will have a Q&A next week and then be joined, I'm presuming - if not, then we'll get John as soon as we can because I'm really interested to hear him, not in overview mode, but in painful detail mode, okay, here's what it means to use JavaScript itself. Not generic scripting, but this specific language, in detail. Because that's going to give us a much better sense for this.

Leo: And if you want to get your question answered next week, go to GRC.com, that's Steve's site, Gibson Research Corporation, GRC.com/feedback and leave a question for Steve. There's a great security forum there, too. John Graham-Cumming and others are there answering questions and talking about these issues. Steve's got a lot of great stuff there, including the must-have security tool, ShieldsUP!. Make sure your site is ShieldsUP! certified. No, see, it doesn't work. It just doesn't work.

Steve: [Laughing] Make sure your computer is, at least.

Leo: Yeah, at least your computer. Go to - oh, and all sorts of great stuff. Including, last but not least, SpinRite, the world's best hard drive maintenance and recovery utility. Let's make sure Steve goes into retirement with a little bit of cash in his pocket. Because I'll be honest, Steve. Solid-state drives are coming on strong, and you don't - you can't use SpinRite on them.

Steve: I know. I know. As a matter of fact, I have a - I purchased a 64GB Single-Level Cell, SLC, the expensive kind, SSD. It cost me $650.

Leo: [Whistling] Was that an Intel, the X25, or...

Steve: This was not. This was Transcend.

Leo: Oh, yeah.

Steve: It's a brand that I like.

Leo: Yup.

Steve: And I had coffee with my operations gal, Sue. And I brought it with me. And I said, Sue, I want you to understand, this is why you're going to be hearing me doing a lot of work on CryptoLink.

Leo: You've got to find the next product because I think within five years you're not going to - well, maybe not. I don't know. But just this stuff is coming on fast.

Steve: It's a circuit board with chips. And we know what circuit boards with chips cost. They cost $12. You know? I mean, that's all there is to it. And these things are so expensive now because they can get the money for it. They're recouping their investment. The hard drive market is so mature. You look at a hard drive that's, like, $50, and you think, how can they make this thing for $50? I mean, it's got moving parts and bearings and a gazillion little screws. It's got super smooth plated platters and heads that are flying low over the surface. And, I mean, a motor that's unbelievable technology. And for $50. And then here I'm holding this circuit board that's got nothing on it, that they're currently getting $650 for. But we know that that's going to be - it's going to be nothing.

In fact, the model's going to change, Leo. In the future laptops will be like iPods. There won't be like any kind of a hard drive removable thing because the connectors will be more expensive than the storage itself. So it'll just be - there'll be a processor integrated onto the motherboard. There'll be the various I/O. And there'll be X amount of nonvolatile storage. It'll be 64, 128, 256, however many gigs you want to buy. It'll just be part of the unit, the way the memory is part of an iPod. And that's where we're headed. And I think we've got plenty of years left. Drives won't disappear overnight. But yes, I'm definitely aware of the fact that 20 years from now I don't think SpinRite will be selling the way it was 20 years ago.

Leo: Yeah. That's okay.

Steve: Yeah.

Leo: You have a second act.

Steve: I do indeed. It's going to be a good one.

Leo: Yup. All right. Thank you, Steve Gibson. Everybody should go to GRC.com. Also 16KB versions there of the show, the shrunk-down ones. And transcripts, thanks to Elaine, for people who like to read along as they listen. See, you do it. The Kindle may not, but you do it. We thank you all for being here, and we invite you to watch, if you want, live. We do this show every Wednesday at 2:00 p.m. Eastern time, 11:00 a.m. Pacific, that's 1800 UTC if you want to watch at live.twit.tv.

And as I mentioned, we're moving towards offering video downloads of all our shows, plus putting them on platforms like the Roku box, the Popcorn player, the Palm Pre, the iPhone, just everywhere. The idea is, if you want TWiT, and you've got a device of some kind, whether it's a big screen or a portable, you should be able to get TWiT with a click of the button or a touch of the fingertip. So watch for more details on that at our regular site, TWiT.tv. We're actually moving very quickly to put video up on that site so you can start watching it right there. Steve, thank you so much.

Steve: Always a pleasure, Leo. Talk to next week for Q&A, and then onward into the future.