SECURITY NOW!

Transcript of Episode #332

Listener Feedback #133

Description: Steve and Tom discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-332.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-332-lq.mp3

TOM MERRITT: This is Security Now! with Steve Gibson, Episode 332, recorded December 21st, 2011: Your questions, Steve's answers, #133.

It's time for Security Now!, the show that keeps you safe and secure on the Internet. Well, at least tries to. As safe and secure as you could be. And of course the star of the show, Mr. Steve Gibson is here, the man who makes ShieldsUP!, SpinRite, and so many other great things come to life. I'm Tom Merritt, filling in for Leo Laporte, who is on holiday break. But he'll be back next week. Welcome, Steve. How's it going, man?

Steve Gibson: Hey, Tom. Great to be with you again. You seem to be doing the Q&As with me. Every other week you're jumping in to...

TOM: Yeah, it has worked out that way. I'm the December Q&A guy. I'm looking forward to that. I like the Q&As. You get a lot of samples of lots of different stuff. It's really fun. Let's start off with our Adobe Watch. What's the latest?

Steve: Well, this week, unlike last week, I don't know if you were aware, but so much happened week before last that last week's podcast had so much security news that we didn't even try to get any of, like, our regular, like, tutorial or explanatory or whatever topical content in. This week we don't have that much. So we've got a nice Q&A, but fortunately not that much happened.

Adobe Watch has us keeping our eye on the two zero-day Flash vulnerabilities which surfaced last week. They were discovered by a Russian security firm who has demonstrated them, is selling fixes for them to their own customers, but is not disclosing to Adobe what they have found, saying that, well, Adobe's not paying us, so we're not telling them. So...

TOM: Now, this is the opposite of what we usually run into, which is a researcher letting everyone in the world know to help make it safe. They're saying, you know what, we're not telling a soul.

Steve: Well, and they're - exactly. So their game here is that they're saying, hey, our clients pay us to protect them, and we're protecting them against something that we know about, and we can demo it, but we're not going to tell Adobe. So the concern is that the bad guys will be able to reverse-engineer the protection, figure out what's wrong, and exploit it. And Adobe, who hasn't been informed, won't be able to do anything about it. So we're sort of in a holding pattern here. We know that these are in Flash. We know that you can invoke Flash visiting a website or opening a PDF for some bizarre reason. Flash is supported by PDF because those are Adobe formats. And so we're just - there's been no news on that horizon. So we're kind of keeping an eye on that.

The good news is that, in response to an emergency problem in the versions 9 and 10 of Adobe Reader and Acrobat, as we have been expecting, Adobe did update v9 of Reader and Acrobat to fix the problems which had been, again, another zero-day problem which they learned about a few weeks ago. It is contained by their sandbox, which was put into place with v10. So even though v10 of Reader and Acrobat also has this problem - I think they're at 10.1.1 at the moment - they're not going to update that in a big hurry because this exploit can't get out of their sandbox. So this has been an example of the sandboxing technology doing a good thing. We wish that it didn't have the vulnerability in the first place, but at least as far as they know it can't get loose from that.

I got a kick out of the SANS Institute, SANS Security Institute. One of their editors, Tom Liston, who is a senior security consultant and malware analyst for InGuardians, he's a handler for SANS Institute's Internet Storm Center, and also the co-author of the book "Counter Hack Reloaded." He said, of all this, he said about the Reader and Acrobat problem, he says, "Isn't it about time that we drove a stake through the heart of PDF and started over? This time, let's not include stupid cruft like JavaScript, Flash and Universal 3D in a 'DOCUMENT' format."

TOM: Oh, hear, hear.

Steve: Yeah, I mean, it's just crazy to have, I mean, so many problems have been a consequence of the PDF document format supporting executable content, which is of course Flash, which is interpreted and has had a history of problems, and JavaScript, which has all kinds of exploits being made possible.

TOM: Now, do we need to start over? Or can we just take that stuff out? I mean, because I know some of the alternate readers are more secure because they just ignore that aspect of PDF.

Steve: Yeah. And, I mean, he's sort of tongue-in-cheek. He knows we're not going to scrap PDF. I mean, PDF is the standard interchange format now for page format of documents. It's not going anywhere. But you're absolutely right. One of the things that we have often promoted on this podcast is people going in and disabling things like JavaScript and Flash support in Acrobat and Reader. There's just no reason to have it. The problem is it's all on by default. What would be really nice is if it was off by default, and then in those rare instances where a document actually needs JavaScript or Flash - and I'm sure there are some vertical corporate applications where there's, like, within a narrow range, it makes sense to have this.

But most of us are just looking at static pages. And yet we've got the vulnerability of an interpreter, a PDF document interpreter that will do vastly more than we want. And anyone who's been listening to this podcast for more than a couple years already gets it, that even if you think those extra features are secure, you're more secure to turn them off. It's just the target surface, you want to minimize the size of the target service. So having fewer things on always makes you more secure.

TOM: If it's not there, it can't be hacked.

Steve: Yeah.

TOM: That's why I used to unplug the phone line from my computer when I wasn't - when I didn't need it, obviously. It's like, well, nobody's going to get into it if it's off and it's unplugged from the Internet.

Steve: I remember when Microsoft was bragging about the security level of NT. They were - I don't think - I think it was maybe called "S3" or "C3," I think it was C3 was a government spec for security. And they were saying that their new Windows NT - this is when, of course, it was new - new Windows NT 3.1 operating system was C3 secure. The problem was that one of the requirements of C3 security is that it's sitting in a room all by itself with nothing connected to it. So it never was actually C3, not unless, I mean, not if you had it networked and connected to the Internet, god help you, and so forth. So it's like, I don't think that quite qualifies.

TOM: And I'll be honest, I haven't had Acrobat Reader on a computer in years. I just keep it off. There's plenty of other ways to read PDFs, one of them being Chrome. We got a security update for Chrome to talk about. Of course it does it quietly.

Steve: Well, yes. Somewhere along the way, Chrome did update itself once again. Google paid out $6,000 total for the respective discoverers of the various flaws which this latest update fixed. And what dovetails nicely on that is that Microsoft has seen the light and announced that they, too, starting next year, starting in 2012, will be adding automatic background updating to Internet Explorer. They've been actually waging a campaign that we've talked about a couple times on the podcast to try to get people to stop using IE6. And there is some strong corporate support still, I mean, insecure as IE6 is, because Microsoft began to break compatibility as they went to IE7, and there are - I remember that we've had listeners telling us that they would like to leave IE6, but they've got huge applications that were written specifically to IE6 features which are not portable to later versions of IE, which is, oh, goodness.

I mean, so I guess if you just used IE, if you locked it down and used it only for those things, the problem is IE doesn't like to coexist with other versions of IE, so you're almost forced to use a third-party, which is actually a good thing, a more secure third-party browser for your Internet stuff, and then just use IE as an application platform where you have no choice. Microsoft has said that they will be, by default, because, I mean, their goal is to corral everyone and bring them current as they move forward to their later versions of IE. So it will be an opt-out automatic update, meaning there will be a means for turning that off for users who specifically don't want it, and if you had ever said "no thanks" to updates in the past, then this thing won't sneak up on you. It'll stay disabled.

TOM: Yeah. If you have automatic updates off now, you won't be forced into this. But if you have automatic updates on now, this is going to be part of them. Is that right?

Steve: Well, if you didn't decline in the past an offered update to IE, then it will now just not even - it won't be in your face. It won't ask you. It'll be like Chrome is with Google, where it'll just be keeping itself current in a much less obvious fashion. Because, you know, I mean, we all know that browsers are the application platforms of tomorrow. We're seeing everything going cloud and distributed. We like the idea of seamless access to cloud-based applications on various devices. So Microsoft's working towards that same model. They said, and I don't quite get what their rollout schedule is, it won't hit us in the U.S. immediately. They said they're going to roll it out in Australia and Brazil first at the beginning of 2012, I guess to sort of see how it goes and sort of beta test it in those two lucky...

TOM: Yeah, it's an interesting pick, Australia and Brazil, two opposite sides of the globe, southern hemisphere.

Steve: And maybe they're doing an alphabetical - maybe alphabetical order by country name.

TOM: Yeah, maybe it is.

Steve: Starting with A and B.

TOM: Where's Austria, then?

Steve: Yeah, well, yeah, true. Maybe that's next.

TOM: You know what's interesting about this, I remember when they tried to make updating to the next version of the browser automatic several years ago, and there was a huge outcry because we were not accustomed to being pushed. And Microsoft forcing you, like don't you dare force me into upgrading. And there were all the people, like you say, who use IE6 because it only works with their custom applications, and IE7 wouldn't work that way. It was this huge outcry.

But now, years later, we've gotten used to Chrome. We've got now Firefox is moving towards the same thing. And we'll talk about that in a second. But we're all so accustomed to it that it's being welcomed more, especially because they're doing it in a way that allows you to turn it off, if you want to.

Steve: And if we go even further back in our Wayback time machine, remember that when Microsoft first introduced the whole concept for Windows of automatic updating, people freaked out.

TOM: Oh, yeah, definitely, uh-huh.

Steve: I mean, suddenly we liked the idea of having control. We just received service packs from time to time to fix a lot of things. And Microsoft began saying, oh, no, instead of coming to us, we're going to come to you. And, oh, all of the old-school gurus just had fits about that.

TOM: Well, so many of those updates had broken things in the past that I think we were all burned. And I'll be honest, still to this day on my Windows machines I let it notify me, and then I say, okay, I'm ready. You can update.

Steve: Yes. Well, and there is nothing more annoying than waking up a machine and having everything you were doing gone, and then discovering that it updated and rebooted because the update needed a reboot.

TOM: "Windows Updates have been applied."

Steve: Yeah. Microsoft has said that they are going to provide three days' notice of intent to reboot your machine to give you time to save things and shut things down gracefully. So, yes, thanks so much. And...

TOM: Also if you're on - I was going to mention, if you're on XP, you'll only get moved up to Internet Explorer 8, not Internet Explorer 9, I believe.

Steve: Correct.

TOM: Because 9 doesn't work on XP.

Steve: Correct. And you mentioned, and you're right, that Mozilla - now, okay. Mozilla has said they're going to do it, too. Now, here's what gets me. Someone, I saw somebody tweet something, asking me, "Steve, what do you think about Firefox v9?" And it's like, oh, is that where we are? Okay, good luck with that. I'm still at 3. And I just did receive a notice that I have a new version of 3.6.x is available. But I see now in this announcement of Mozilla's intent, they're planning to add automatic updates, background updates to Firefox v12 on April 24th of 2012.

Which says that this other thing that's been annoying people is that Firefox has gone from really slow, painfully slow updates, which frankly people were liking a lot, that they weren't - it wasn't this crazy update festival all the time. So suddenly now we're - it's like I'm already hearing about 9. 8 just happened. Somewhere between now and April 24th they're going to have to do a 10 and 11 and then a 12. So, okay.

TOM: Yeah. I think what they did is they just changed the numbers. Instead of .0 or .1, they just said, well, we're just going to call the next one 5 and then 6 and then 7.

Steve: We're going to move the decimal point three places to the right and call them major versions. It's like, eh, well...

TOM: And Firefox right now does a sort of an automatic update, but you have to restart the browser. And I guess what's going to happen April 24th, if I read this right, it'll work like Chrome, where you just never really know that it's being updated.

Steve: Yeah. Which would be nice. And it will require some plumbing underneath, behind the scenes, in order to make that work correctly. So, yeah.

TOM: All right. We've been talking about this a lot on Tech News Today, the Stop Online Piracy Act, HR 3261. Of course the latest is that they haven't passed it out of committee, thank goodness.

Steve: Right, right. Again, I got a kick out of one of the editors of the SANS Institute newsletter, in this case William Hugh Murray. He's an executive consultant and trainer in Information Assurance and associate professor at the Naval Postgraduate School. And about this he said, "On December 15, the managers of the bill published amendments intended to respond to the criticism" which the bill immediately received from the industry. He said, "The amendments said, in effect, that the remainder of the bill should not be interpreted as written English..."

TOM: What?

Steve: "...that it was not intended to do what it does." He said, "Drafting legislation is difficult, even when one's intentions are honest. When it is drafted by an interested party, bent on disclaiming its interest, it becomes nigh impossible."

TOM: And there was a great section in one of these amendments, and I think it's the amendment he's referring to, where it said, "Nothing in this bill should be interpreted to break the way the domain name system works; and, if so, then it should be ignored." I looked at that and said, great, the entire bill can be ignored because everything they're recommending breaks the domain name system.

Steve: That's exactly right. This new replacement starts out, the first clause is that nothing here should be interpreted as foreclosing any free speech rights. And the second part is, exactly as you said, and if this breaks the DNS system, then we didn't mean to do that, so ignore that part.

TOM: Yeah.

Steve: And then they go about explaining how the bill does exactly those two things. So, crazy.

TOM: Prior restraint, and breaking DNSSEC.

Steve: Exactly. The problem is, I mean, from my technical standpoint, ignoring the social and constitutional and just sort of the emotional aspect, from a purely technology standpoint, what they're trying to do doesn't work. And we have example after example of example of the fact that it cannot work. What they're trying to do is blacklisting. And we have a long history of failed attempts at blacklisting on the Internet. Famously, spammers are a persistent problem.

TOM: Right. None of us have any spam anymore because everybody's been blacklisted.

Steve: Exactly. Wasn't that a great solution. You just blacklist those particular pesky spammers, and they can't send you spam anymore. Well, we know that doesn't work because all they have to do is change their identity and their location, or their apparent identity and apparent location, and, whoa, they're able to send spam again. The point is that the fundamental architecture of the Internet is to permit publishing by default. And any person can get, in the case of domain names, any person can get any not previously registered domain name from any registrar, set up a website anywhere in the world, using any ISP that they want. And, by default, anybody anywhere can access it, if they know its name.

So, I mean, it's very much like sort of the old-school way that firewalls were originally created. The first firewalls had all their ports open by default. And then, if there was, like, some service that you were running inside your network that you did not want anyone outside to access, you would block that port. So the default was open, and then you made exceptions to close ports. Well, everyone quickly found out that was a bad idea because somebody inside the network would fire up some new service and start offering something, and then people outside were able to access it until they were blocked. So now we have firewall technology. I mean, everyone knows you block everything by default, and then you selectively permit those things that you know you need.

TOM: Don't let Congress hear that, Steve.

Steve: Well, and see, that's just it. It can work in a controlled, constrained environment. There's no way to do this across the Internet. There just - there isn't. And so my concern about this whole SOPA mess, aside from all of the other non-technical aspects, technically you can't blacklist. We quoted someone a few weeks ago saying that - it was a quote that I really liked - the Internet was designed to route around censorship. I mean, it is censorship-resistant, I mean, robustly so. And so the problem would be, if we ask ISPs to block all of these following bad domains, the counterfeiting purse people will simply create some new domains.

TOM: Yeah.

Steve: You know, different names. And then we'll add those to the blacklist. And then they'll move again to different domains, and we'll add those. Before you know it, there'll be this massive list of domain names that needs to be checked. And most of them won't have anything there anymore, but they'll still be in the list. I mean, it's just a technical catastrophe. I mean, essentially, the people that are trying to make this happen, the good news is they don't understand the technology, and that's what has stopped them now because a lot of people who do have said we're moving towards unspoofable DNS with DNS security, DNSSEC. And this breaks DNS security. And suddenly all of the Congress people go, whoa, what, what, what?

TOM: Well, no, Steve, I heard - the head of the MPAA told me, told everyone that those fears are overblown. And obviously the head of the MPAA knows more about DNSSEC than the dozen or so Internet engineers who work on it every day who signed a letter saying the opposite.

Steve: Isn't that Christopher Dodd, now, by the way?

TOM: Yeah, it is Christopher Dodd, correct.

Steve: Oh, you know, okay [laughing].

TOM: I don't - and here's the thing. I don't want to minimize the challenge that the industry faces in trying to protect their intellectual property. There is a right to protect copyright.

Steve: Yup.

TOM: However, it's being overblown, A, how much of a danger it is, and how damaging piracy has been to the economics. And so we have this high-pitched rhetoric where I think the industry is feeling like, okay, we've got this Internet full of hackers, both white hat and black hat. And all they do is like to come up with ways around everything we try. We tried to get them with DRM, and we tried to track their IP addresses, and we tried this, and we tried that, and we can't stop them because the Internet's full of people who could figure out how to get around stuff. So let's just get them off the Internet.

And it turns out, you know what, you can't do that because they are people who like to hack around whatever obstacle you throw in their way. You have to come up with a more sociological situation, a situation like the music industry has sort of stumbled into where you say, you know what, instead of just trying to slam piracy, let's give people a better option where they're willing to pay money. And it's certainly hasn't solved everything for the music industry, but people are paying money for digital music, something if you had told the music industry this would happen in 2001, they would have told you you were crazy.

Steve: Yeah. Well, and I keep harkening back to the conniption that the motion picture industry had with the advent of consumer VCRs. They absolutely tried to prevent the VHS and Betamax from ever happening because they said it would be the end of the movie business. Well...

TOM: There's a great "20/20" that's kicking around, I think on YouTube, where I think it's Jack Valenti, maybe, talking in exactly the same terms that they talk today about the VCR and what it would do to the industry if it was allowed to exist. Didn't happen.

Steve: No, no.

TOM: All right. Well, we can't move on to a happier - well, I guess it's sort of happy. Depends on how you look at it. Carrier IQ is sort of - the story's sort of winding down. But the carriers are backing away, essentially.

Steve: Well, yeah. We've already covered this through a couple weeks. I didn't want to spend much time on it except that we had talked, and Wired magazine carried an interesting story that I got a kick out of. The headline was "Mobile Carriers Claim Consumer Consent to Carrier IQ Spying." And reading just the first two paragraphs from Wired's article, they said, "According to mobile phone makers and carriers, Americans consented to secretly installed software on 150 million mobile phones that logs what apps they use, what websites they visit and who they communicate with. Sprint, AT&T, HTC and Samsung told Sen. Al Franken..."

TOM: My friend.

Steve: "...last Thursday that their end-user licensing agreements," the EULAs that we're all so fond of reading, "those pages of fine print you sign when you get a new cell phone authorize them to use Carrier IQ software to monitor app deployment, battery life, phone CPU output and data and cell-site connectivity. The companies' statements, released by Franken, are a good roadmap to how the companies will fight federal privacy lawsuits already brought by consumers over the secret software." And this dovetails nicely into, as I was saying to Leo last week, he often reminds people that I'm credited with coining the term "spyware" because I found this Aureate spyware...

TOM: I remember that.

Steve: ...on my machine back in the day. I mean, this was this advertising spyware. And their defense was that, in the contracts that they made with the freeware carriers of this spyware, so that you downloaded freeware, installed it, and along with it came this spyware. And this was - it was a way of advertising enabling freeware in order to kick back a percentage to the freeware makers. And the model never worked. The whole thing just collapsed. But this was installed in tens of millions of people's machines, and they told their freeware authors, do not remove this when the user removes your freeware because other freeware may have since been installed that also so uses it. And so there'll only be one instance of our spyware, and all the freeware is able to use it.

So there was this amazing hue and cry when it was revealed that there was this spyware technology that had been installed in everyone's machine. I created a little Opt-Out was the name of my own little remover to take this stuff out of people's machines. And their defense was that, exactly like this Carrier IQ situation, it's like, whoa, it's in the fine print, literally in the fine print. And it's like, sorry, that just doesn't keep people from being really upset when they find out that this was the way this software is behaving.

TOM: Well, and you see the legal arm saying one thing. And at the same time you see Sprint pulling it off of millions of their mobile phones. So this is bad news for Carrier IQ.

Which I really, honestly believe was not trying to be up to no good.

Steve: No, I...

TOM: I think they got caught in a sea change of writing software for a platform in the '90s and having it still working on a platform now in 2012 almost. There's an entirely different set of assumptions about what you're getting into. When I've got a little flip phone that all it does is make calls and send some text messages, that Carrier IQ diagnostic software is not nearly as burdensome and dangerous as it is on a smartphone, where I've got all my financial information and apps and all my contacts and all of that.

Steve: Well, and it has evolved. I mean, certainly, if it's monitoring app usage, their argument is that some apps drain batteries. And so they would like to be able to - they're not able, the carrier doesn't know all the things that a user has installed. Yet the carrier is who gets called and complained to when the battery only lasts two hours. So, I mean, so defending them, they have a strong case, I think, to make to say, look, we need to be able to know what's running, what percentage of the time it's running, what percentage of the CPU it's using, what percentage of the battery it's draining, and be able to pull that intelligence up on our tech support employee screen when someone calls and says their phone's dying after a couple hours. So, yeah, I mean, I can see the need for that.

I mean, I don't think there's a - there's not a good solution to this, unfortunately, because users are just going to use their phone, and no one is ever going to read the fine print, and this stuff is just going to be there. So I think ultimately it has to kind of get out into the world that this is what our smartphones do, and you have a choice of not using the smartphone, or maybe using one that has this stuff removed or disabled, or maybe there will ultimately be some sort of, it's not on by default, but if you have a problem then you contact the carrier. They say, okay, look. We're going to turn this on so that we can diagnose the problem. Call us back tomorrow and we'll see what we learned.

TOM: Well, you know what...

Steve: That might have been a better way to handle it.

TOM: That's the way Mark the Spot works in iOS now. AT&T uses Carrier IQ and Mark the Spot on other platforms. But on iOS it doesn't. What it does is, it has you download an app that you launch when you have a problem, and then it captures the state. Now, it's not going to be as comprehensive as Carrier IQ running constantly in the background, but it does give you the control over when it grabs everything.

I think something like that is really all that Carrier IQ needed to do, is give you an alert when you first buy the phone, saying, hey, we want to have the software running, collecting diagnostic information. Click here to find out all the things that it collects. Do you want it to run? If yes, click here; if no, here. And then, like you say, if you did click no, you could always choose to turn it back on if you're having problems. Just give me the control over it and let me know what it's doing, and I'm fine with it.

Steve: Yup.

TOM: All right. A couple of miscellaneous things here. What's this about "briefly stalled sales"?

Steve: Yeah. I mentioned this to Leo. I followed through with switching my SSL certificates throughout the entire site from VeriSign over to DigiCert. And the experience was spectacular. I am so glad to be with DigiCert now. I mean, I'm saving money. I switched up to EV certs, so I have those. They give me protection of my root domain, GRC.com, in addition to three other subdomains, so like www is just part of the package. And I'll also be doing media.grc.com for our media server. And my goal is to move the entire site to SSL always, you know, HTTPS Everywhere mode, which is the direction I'm heading. But I also wanted to do it with EV certs.

The problem was that something bad happened a day or two after we switched. And, for example, last Sunday - Sunday. Yeah, yeah. Sunday a week ago? No. Just, yeah, yeah, Sunday a week ago our sales stalled. I mean, we hadn't had a lower number of SpinRite sales, like, ever. And it's like, what the heck? And so I checked the server. I was trying to see if there was a problem, if there was, like, some - we weren't processing financial transactions or whatever.

Anyway, what was interesting was that a frequent listener to the podcast who goes by "Dr. Mom" in the chatroom, whose actual first name is Liz, sent me an email saying, hey, guess what, Steve, my organization thinks GRC is evil and has blacklisted you, and we can't get to your site now. And I was like, oh, my goodness. Well, turns out that - I asked her to track down what was going on. They use an automated, software-based technology from a company called Websense. And Websense briefly, they fixed the problem, or it fixed itself. I don't know if they've got someone who listens to the podcast and heard me.

But they noticed that the Certificate Authority that signed GRC's certificates changed. And of course that is the No. 1 thing that you would expect to see happen if there was a man-in-the-middle attack or a DNS spoofing attack or something that would be taking you to a pseudo GRC site and, over a secure connection, would be presenting you with a bogus certificate that would almost by necessity be signed by someone other than the previous certificate signer. So, unfortunately, it was a brief and short-lived false positive alert because in fact, for all good reasons, we did have the people signing our security certificates change, and I'm really happy that happened. So anyway, the problem only persisted for a day or two, and everything's back to normal.

TOM: Thanks to Dr. Mom.

Steve: Yeah.

TOM: By the way, her first name's Lil. She wanted me to...

Steve: Oh, Lil, sorry.

TOM: ...make sure - Lillian. Thank you, Lillian. All right. I love this last one here because I'm a sucker for a good math joke. But Steve, why is it that all these programmers I know always confuse Halloween and Christmas?

Steve: Well, this is something that always surfaces, every season. I see these either in the mailbag or now in my Twitter stream. And several people tweeted this. I just thought I would share it with all of our listeners because those who enjoy, as you said, math, will get a kick out of it. And this is one of those things, it's like, okay. Someone clever thought of this, and it's of course correct. And the reason those two holidays get confused, apparently, in some programmers' minds is that 25dec, d-e-c, that is to say, decimal, equals 31oct, which is to say, octal. And sure enough, that's the case. Two times 10 is 20, plus five gives us 25 in decimal, and three times 8 plus one gives us 25 in octal. So, sure enough.

TOM: Somebody working in octal one day just had that brainstorm and said, wait a minute, Halloween is Christmas. Everything's crazy.

Steve: Well, and I had - I got a nice note from a Richard Shepherd dated the 17th of this month. And the subject was "YAST," Y-A-S-T, Yet Another SpinRite Testimonial. It's a little quickie. He said - but this is something I don't think we've ever talked about before. He said, "I remotely connected to a client's domain today to take control of a PC there and burn our site-licensed ISO of SpinRite at the client's office that is 72 miles away from me. I walked the client through rebooting to the SpinRite CD and starting SpinRite at Level 2. And, well, this email exchange is all you need to know. I get all the credit for your great work." And then actually he says, "I hope your EV Cert/SpinRite sales issue has been resolved." And indeed, as we know, it has. And then he signed it, "Big Fan, Rick Shepherd." So, Rick, thanks very much for sharing your SpinRite success with me.

TOM: Shall we get into some questions, Mr. Gibson?

Steve: Absolutely.

TOM: This is Listener Feedback #133. We'll start off with Bruno Miranda in Portugal, who solved the mystery of his router's login failure. He says: Hello, Steve and Tom. Wow. I actually got in an email. I have just won one of those battles against those little things that we wouldn't normally suspect of, and almost out of despair call it broken logic. Suddenly one day I discovered that I couldn't log into my router, a cheap but interesting Vodafone Sharing Dock. It wasn't recognizing my password. I was surfing the web, everything else was okay, but I just couldn't log into the router. I rebooted, restarted, reset, powered the router off and back on again, cursed at it, yelled at it, all to no avail. Had I been hacked and my router stolen from me? I even upgraded, then downgraded the firmware. Still nothing. After a full factory reset, it wasn't even accepting its default password. Then I tried my tablet, and it was working fine. But the laptop wasn't. And I knew the password. I knew that I knew the password. Was the router broken?

So I took a last deep breath, multi-booted my Linux machine into Windows, and it was working. It wasn't the laptop's hardware. I returned to Linux Mint, installed another web browser, and it was working! Only two chances left: Broken router or something in Firefox. I went around Firefox's configurations, and yes, I had changed something some time ago: I had activated the Do Not Track (DNT) header. After unchecking the box, I typed in my password, and Shazaam. That was it. Of course there's no need for or worry about my own router tracking me. This seems to be one of those little broken compatibilities that test our nerves. I wanted to share my interesting adventures with your listeners. Thank you so much for the great show and all the energy both of you put into it! Security Now! is listened to on this side of the Atlantic.

Steve: Now, that's really odd, and I did want...

TOM: What is it doing that?

Steve: Yeah. The only thing that the Do Not Track header does is add a "DNT: 1" for Do Not Track. Basically it's just making - your browser adds that one line to what's called the "query headers," the list of things that are being sent out when your browser is asking for a page. And normally, essentially, the router looks like a web server, so your browser is querying the web server in your router for a page. And it's just - it's bizarre to me that the addition of a header, which it almost certainly wouldn't know about, would cause a login failure. I mean, the only behavior of turning Firefox's Do Not Track header on should be to add that to the query. It shouldn't prevent, for example, cookies.

Now, the only thing I could think is that there's some interaction or maybe something else in his browser was seeing the Do Not Track header and was, for example, doing something with cookies because I could imagine that, if you were blocking cookies, that could cause a login problem. But I just can't see that the Do Not Track header by itself could. But I thought I would share this just in case anybody else had a router that was acting in the same way. Turning on Do Not Track is something that we would be promoting for people. So if it's causing a side effect in some bizarre cases, that's certainly worth knowing.

TOM: Rckgift in the chatroom speculates maybe the router was using that code for something, and the router had been created before Do Not Track was implemented?

Steve: It's the only thing I can imagine. But except that, well, or maybe a bug in the router's web server. Essentially, the router wouldn't be able to induce your browser to generate a DNT header. And if it's named - if it was naming a cookie DNT, then the header would actually be cookie:dnt=, so that would be semantically parsed differently than dnt: and then a one or...

TOM: You know, chetpot has an interesting speculation. What if the admin CGI script is being taken from an array, and the added header changes the array stack?

Steve: Again, it would be, I mean, again, that's another possibility.

TOM: Intriguing, yeah.

Steve: But requiring that a browser have exactly a certain set of headers, that's a problem, too. In fact, one of the ways that browsers can be identified is the sequence of the headers that they generate because different families of browsers emit their query headers in a different order. And so I remember at one point, I think it was when I was working on the browser identification for the CSS script-free menuing system on GRC, I was looking at how can I determine which browser is which? And without scripting, you can't really take advantage of header sequence. But I do remember noting that one of the things that some servers were doing is looking at the sequence of headers as a means of disambiguating browser families. So, you know, again, that's hard to see that would be the cause. But still, something certainly kind of freaky.

TOM: Yeah. All right, Question #2 from Notre Poubelle in Vancouver, Canada, asking about an iOS battery management app. He says: I've seen an app called "Battery Boost Magic" in the iOS App Store. Could an application actually help battery life? Wouldn't this be managed by the OS? I can see how an application that uses heavy resources could kill battery life, but to improve it? I've seen lots of reviews on the web, and they're generally extremely positive, but I can't see how this thing would work. Assuming it does work, is there any possible negative long-term effects to using something like this?

Steve: So I took a look at what the app was because I completely agreed with his assumptions about what limitations an app running in iOS would have. And looking carefully at what their claims were, I'd have to come to the conclusion that their claims were a little overblown. They were hyping what this thing was able to do more than their technology would warrant. What it appears that it does have to offer, which iOS doesn't, is very sensitive measuring of the amount of current that is being drawn, or the high-resolution look at the current charge state of the phone. And so over time, by looking at that, the app would be able to see the rate at which the phone was draining because the features which seemed strongest that this thing was offering was a projection of how much time you had left on the battery when you were doing different things.

So this app was running, is passively looking at the rate at which the battery is discharging based on a much higher resolution readout of the amount of charge in the battery, and then it's able to do probably a straight-line prediction of when the battery will hit zero, essentially, and tell you, oh, you've got seven hours using this app and two hours using this app and so forth. So it does look to me like it's stretching what it's able to do. Essentially, it's a sophisticated battery meter and really doesn't look like it's anything more than that. And they've been clever with what they're doing with it. But they are sort of overselling it.

TOM: Battery meter/placebo effect is what it sounds like to me. All right. Ranget in Syria wonders about remote attacks on home computers: I like your podcast a lot, and I'm a weekly listener for almost a year. Damn, I wish I knew of your podcast earlier. Anyway, thanks for the amazing podcast. As for my question, let's say a hacker got a hold of your IP address, and your home network is behind a hardware firewall, a router. What can he do in order to hack the network? Are we safe behind our routers? Or are hackers able to gain access remotely to our network by probing the firewall with some of their gadgets? And what can we do in order to protect against such attacks? So, yeah, how do we harden our own firewalls?

Steve: Yeah. When I encountered this, I thought, well, this is sort of a basic question, but basic is also good because some things have been changing in our computers in the last few years that are worth noting. The other day I was setting up a new machine and was curious what exceptions had been made through the Windows - I was setting up a Windows machine and was curious what exceptions had been made through the Windows firewall. And I was disturbed to see how many different apps and services had registered themselves to receive incoming traffic through the firewall. Meaning they were opening ports through the software firewall in Windows to make themselves available for incoming traffic.

Now, that's different than opening ports out in the hardware firewall, the router, as he mentions. Except that Universal Plug and Play, UPnP, explicitly allows this. That is, it is designed, the reason it was created was that consumers were installing routers for their security and for the features that they afforded. But that was blocking software features from being able to receive incoming traffic.

So Universal Plug and Play was created as a means to allow machines inside the network to talk to the router, which would be advertising its UPnP services and selectively open ports through the router, essentially violating its security. Leo and I have often, through the years, suggested to people that, if you do not need, you don't know you need Universal Plug and Play, then you really want to disable that in the router. A place, for example, where you do need it is by default Xbox wants to open a bunch of ports.

Now, what you can do is disable Universal Plug and Play and then manually open those ports yourself so that you retain control over what your router's doing and have those ports sent only to the X-box. If you have Universal Plug and Play enabled, any machine in your network can open ports through your router. And when I look at the number of openings in the typical Windows firewall now, it's a lot less secure than we wish it was.

TOM: All right. On to Question #4. Jamie Hunt in Darby, England, wonders whether Steve is an open source publisher without knowing it. He says: Hey, Steve. I might be missing something here, and I'd love to know it if I am; but aren't all of your tools, which you write in assembly language, inherently open source, since they can be relatively easily disassembled?

Take, for example, your DNS Benchmarking tool: If I download a copy of this, I can open this with my favorite disassembler (PE Explorer), and within seconds I am looking at all of your source code just as you wrote it! If you wrote these tools in C++, then I wouldn't have your C++ source code, I would have the compiled assembly language produced from the source code so they remain relatively closed source. But since your tools are written in assembly language, the code is the same; right? I have a feeling that I am missing something, but I can't see where.

Steve: Well, it's funny because there's been - I sort of smiled and chuckled when I saw this because a topic that comes up every so often in GRC's newsgroups is people saying, hey, why don't you release the source of these freeware that you create because, after all, it's free.

TOM: It's free, right, yeah.

Steve: So why not let us see your mojo and magic and how you're doing this?

TOM: Make a speech and beer.

Steve: [Laughing] Exactly. And then, if I don't respond immediately to that posting, if I don't get around to it, somebody will weigh in and say, well, you know, Steve writes everything in assembly language, so just disassemble the executable if you want the source code. Now, the fact is, if anyone has seen my source code, they'll know, and sometimes I'll settle the argument by posting a screenshot from my editor showing what mind looks like because mine is heavily indented, heavily commented, beautiful variable names that are long and descriptive, I mean, it almost reads like English.

I also use all of the Microsoft MASM conditional flow tools - if, then, else, while, do. All of those map down into single instructions. So I'm really writing, I'm writing assembly language, but it's really pretty and much easier to read than the stuff you often see posted on, like, random hacker sites, where it's just a string of opcodes running down the left-hand margin of the page. That is what you get if you disassemble my code, is a string of opcodes running down the left-hand margin of the page. And you don't get nice variable names which are multiword and descriptive when I create them. All you get is an address of something. And of course you get no comments. Those are all stripped out as part of the assembly process, as well.

So there's a big difference between what I produce and what you get if you disassemble the post-assembly code. But to answer the question which actually Jamie didn't ask, but I'll answer because it's the one that is posed so often in the newsgroups, the reason I don't offer my source is it would make it extremely easy for someone to clone my apps and then post them on the Internet and have them masquerading as mine. And it's not that I would mind if they identically cloned them because, you know, that's the same as just rehosting my EXEs. But they could also make them evil. They could have the DNS Benchmark doing something behind your back that you don't know. It would look like a really tasty tool, even if they didn't say it was from me. If it was a really nice benchmarking tool, lots of people would want to use it. But if they made it also evil at the same time, then they would be suckering people into using something that they didn't know was being bad for them.

And of course there's lots of other things that do that already. I just don't want to contribute to it. And I don't see any benefit to me in releasing it as open source. I like the fact that my stuff is sort of uniquely small and special. And you come to GRC.com if you want to get it.

TOM: It's open ugly source, is what you're saying.

Steve: [Laughing]

TOM: All right. Question #5, Sami Lehtinen - and I apologize if I'm mispronouncing your name - from Helsinki, Finland makes a GREAT observation about dangerously leaky "hardware" firewalls. He says: I wanted to warn people about potential problems with regular home routers such as the more expensive and fancy firewall routers that are very configurable. That configurability can backfire nastily. This kind of plays into what we were talking about earlier.

Steve: Yes.

TOM: While the router is booting - it's quite a long process - parts of the system start with default configuration, like the switch portion. This causes all LAN, WAN and DMZ ports to be completely bridged for about one minute. After that, normal NAT/SPI, DHCP, et cetera, function returns.

As far as I can tell, that's a very serious security issue. 60 seconds is more than enough for automated attacks to get through, even if somebody would claim it's just a short moment. And this is not just one case. I have noticed similar functionality in other products like this earlier from the same manufacturer. I assume the basic system they're using is flawed. It shouldn't start networking before everything else is ready.

It's very easy to notice this functionality when configuring the firewall because, if you run ipconfig/renew after reboot, it's trivial to get a public IP from the ISP's DHCP pool and use the Internet for about one minute. After that one minute the network stops working until you again renew the lease, and then you'll get the IP address from the local LAN DHCP pool, as expected.

Steve: Well, this is a fantastic observation, and I'm not at all surprised this is going on. But it's something that had never occurred to me before. Many of the fancier, higher end routers are based on Linux, and they've got a fundamental networking architecture which is supported at the low-level OS level. But then they layer on many more features which run as independent processes and, for example, hook into the network in order to add filtering and NAT routing functionality and so forth. But without those things running, that is, before they hook into the network layer, you have a generic bridging router with none of the security features enabled.

So this is a very real problem. What, I mean, the takeaway from this actually is to - what I would do is, and I'm probably going to do it from now on, I don't reboot my router very often, but I would disconnect my LAN side connection for a couple minutes until the router comes up and it settles down, and then bring my local network up inside. What he was saying, just to clarify, and this is one way to test this, he was saying that shortly after rebooting the router, if he then - he was using the Windows command, "ipconfig /renew," which tells Windows to go send out a query for its auto configuration, the DHCP, Dynamic Host Configuration Protocol, send out a query to get an IP.

What he discovered was that, if you do this shortly after the router comes up, you are actually connected directly out to the public Internet. And traffic is flowing both ways. You have a simple, non-NATed bridge to your network. So you send out a DHCP query, it goes to your ISP, not to your router. Which means you will get back a public routable IP, the one that would normally be acquired by your own router. You would obtain that. And your system would be on the Internet during that time. Eventually, the router's own

DHCP server comes up, and its interception technology, NAT and so forth, comes up, the stateful packet inspection and all that. Then you get normal routing functions.

But what he observed, and this doesn't surprise me, but it's certainly something to be aware of, is that with a router which is actually probably Linux-based OS, it's going to take a while to get itself going. We know that these are not fast processors. They're little, cheesy, I mean, they're slow, barely enough to handle the normal traffic that you have through the router, and they're cutting costs every way they can.

So minimizing the complexity and the speed of the processors is one of the things that they do. So what that means is that it's fine once it gets going, but it really takes it a while to come up and get going. And during that time, you could actually have zero protection. I think that's really interesting.

TOM: So you could also just keep all your computers unconnected to the router during setup. But it seems simpler to just pull that connection to the Internet out because then you can make sure that your computers are getting assigned and everything.

Steve: Well, yes. The problem with that - I mean, yes. That's the - you have one connection to pull if you pull the WAN side. The problem then is that your router won't have been able to obtain, when it booted, a public IP. And so you'd have to give it a kick or wait for it to go ask again or do something. What I was wondering was whether you could run ShieldsUP! during that time. But the problem is you would, if you got a public IP - you have to have an IP in order to run ShieldsUP!. If you get a public IP anyway, then you know you've got a problem. So, I mean, you know that you've got no protection from the Internet during that window.

Now, this makes me glad that all of our personal computers now have their own software firewalls, also, because that's going to give you some protection. But, boy, this does say that you don't want to absolutely depend upon the software firewall in your machine. I'm sorry. You don't want to depend upon the hardware firewall offered by the router because it's transient. It's not present for a while when you're restarting your router. So what's safest, although it's not just a single plug, if you've got a router that also is a switch, you'd have to, like, pull all of the connections from it while it comes back up, wait for it to settle down, and then plug things back in again. But, wow, that's really a great observation.

TOM: Yeah. Question #6 from David in Chicago. He needs to know how to disable Windows Safe Boot mode. And he's got a funny reason why. He says: My kid gets around the Windows parenting filter that I put in place by booting into safe mode. Do you know a way to disable that? This goes to what we were talking about earlier. Whenever you make a blacklist, people find a way around it. Is there a way to turn off safe mode, though?

Steve: Wasn't that - first of all, I got a big kick out of the question. And it's probably, behind the scenes at his kid's school, they're all talking to each other, and they have figured out this is the way you get around what Mom and Dad have done to the computer is you boot into Windows Safe Mode. So I poked around to see whether there was a way around it. Some crazy guy is suggesting that you can hex edit the ntldr.sys file, which is...

TOM: Wow. That's hardcore.

Steve: ...a core component of Windows. Do not do that. You really don't - it's version dependent, and it's search for a certain pattern, and it's like, oh, goodness. I mean, now all these components are signed. That would break the signature for the signed driver files, so you don't want to do that. I did find somebody who is selling something. If you Google, just the phrase with no spaces, "nosafemode," you Google that, the first hit that Google brings up is a page ending in that dot html. And that appears to be a respectable piece of software which you could install which will, specifically for this purpose, disable Windows safe boot mode. It is available, I think it was a 30-day trial. So you could try it, see if it does what you want, and then buy it if it works.

So I did find that. But I just got a kick out of the question and wanted to share it with our listeners and offer that little, although I can't vouch for the app at all because I have not tried it, it looks like it's reputable and would do the trick.

TOM: Now, a bunch of people in the chatroom are suggesting putting a password on the BIOS. That way he can't reboot without knowing the BIOS password.

Steve: That's good. So he would have to have his parent then enter that and then supervise the escorting into Windows normally. That may not work with the way his family is structured, you know, Junior coming home in the afternoons and wanting to use the computer before Mom and Dad are home and so forth.

TOM: Depends, that's true.

Steve: Very clever.

TOM: Kid's going to get a boot disk of some sort anyway. It's going to be an arms race. That's what I think. Jim Hyslop in Toronto remembers that Lucille Ball explained bandwidth. He says: I have an analogy to share and a question to ask: Listening to the most recent Q&A, it occurred to me that a better analogy for bandwidth is a conveyor belt. You put your packets on the conveyor belt, and they get whisked off to their destination. The conveyor belt moves at a constant speed, so the limitation is not how fast the data moves, but rather how much data you can put on the conveyor belt at any given moment. If you have a lot of people trying to put data on the conveyor belt at the same time, some of it has to wait until there is room. The classic "I Love Lucy" chocolate factory sketch is a perfect illustration of, not only bandwidth, but also how routers can drop packets when they get too busy..." because she drops the chocolate all over the floor.

Secondly, I want to cover an extension of one listener's question about how to get people to understand security. Your virtual-to-physical security analogy is great, but I sometimes run into people whose attitude is "Why would anybody want to break into MY computer/website/whatever?" Do you have any suggestions on what to say to those people?

Steve: Okay. So first of all, I assume that our listenership has seen that episode. I mean, it is one of the classic...

TOM: Go seek it out, if you haven't. You can find it online, actually. "I Love Lucy" is pretty easy to find legally online.

Steve: Yes. It is a spectacular piece of comedy. And but mostly, his analogy is great. I love the analogy of a conveyor belt because we all like to have visual aids. And for our listeners who are trying to explain stuff to other people, this is perfect because the idea being that packets are like blocks, essentially, and this conveyor belt is moving along, this imaginary conveyor belt, at a certain rate.

And so the idea is that that is the shared broadband that all of the subscribers on a leg of the ISP's network share. And so the idea being that you're given a percentage of the conveyor belt's capacity, and you put packets on, along with everybody else putting their packets on. Some people get a bigger percentage; some people get a lesser percentage. But the actual rate at which the individual packet moves is shared by all users and the same. What differs is how often you're able to put your packet onto the conveyor belt, sharing the space with everybody else. So I love the analogy a lot.

TOM: Now, if I have this right, is the speed of light the conveyor belt speed?

Steve: Actually, no, because that would be the case if we were actually - if we weren't modulating. We're actually...

TOM: Okay, yeah, that makes sense.

Steve: We're modulating the data onto a carrier. And so it's substantially slower than that. The carrier speed is the speed of light, but the data carried by the carrier being modulated is a lot slower.

TOM: All right. Let's...

Steve: Anyway, great analogy. And Part 2 was...

TOM: Oh, right, right, the virtual-to-physical security. Why would anyone want to hack into MY website, Steve?

Steve: Yes. And that is a great question. And it is the defense that people who want to be lazy about their own security use, is nobody cares about me. The question is, I would - I think, again, trying to relate this to people who are resistant, ask them if they think viruses care who they are. Viruses don't. Viruses are agnostic to who you are. They just want to infect everybody they can. Email spam carrying infected links don't care who you are. These bad guys want to get their malware into everybody's machine. They don't care who you are. They would like to set up a bot trojan in your machine and use it to attack others. They would like to install Zeus into your machine, Zeus being the very successful, distressingly successful banking trojan, in which case they don't care who you are as long as you've got money in your bank account, which they would be happy to help you drain.

So you get Zeus installed in your machine, you're anonymous to them. But this thing watches you log into your Bank of America website, present you with a fake page showing the balance you expect, while behind the scenes it sends your money off to Russia. So absolutely, just in the same way that viruses don't care, none of this stuff cares who you are. It's just happy to have your money.

TOM: Yeah. The answer, the short answer is the reason they care about whatever it is you've got is because you have processing power and a connection to the Internet. And they could use that to take all kinds of stuff from you and other people, essentially without your knowledge.

Steve: And you may have a bank account. And they'd be happy to help you empty that.

TOM: Question #8 from Mark Wonsil in Royal Oak, Michigan points us to a very cool animated CAPTCHA. He says: I hadn't seen this before, but maybe you had, an animated CAPTCHA. I wonder if this defeats some of the image recognition software like Google Goggles - for now. And there's an example at MPESupportGroup.com. So essentially it's a normal-looking CAPTCHA, but it ripples. It's like an animated GIF.

Steve: It's very clever. And I wanted to share this with our listeners. We've talked about CAPTCHAs at length. So it's the contact form, as you said, Tom, MPESupportGroup.com/contact-us.html. And I commend it to our listeners to take a look at it. Essentially, it uses the fact that our brain is able to integrate an image over time, so that, if we watch this thing rippling, we can read it. But it's because we're seeing it stretched out over time. There's a numeral - actually, I guess it's going to be different for everybody, so the one that I saw will not be what everybody sees, obviously. But in the one I saw there was a numeric digit on the end that happened to be a digit "5." And it was actually sort of sliding under a fold in this ripple-y fabric sort of animation, so that you could see that it was a five.

But the point is that it would take some extreme intelligence on the part of software, first of all, to realize this is a multi-image, probably a GIF, an animated GIF image, and then to look at every separate frame. No single frame contains the CAPTCHA. It's only over time that your brain reassembles this into what this waving flag, sort of a printed waving flag is. Anyway, that's very clever, and something I had never seen before that I wanted to share with our listeners. So thank you, Mark, for pointing it out to us.

TOM: Yeah. And Burke, are you able to get my screen, or - oh, never mind. It doesn't look - I didn't have a number in mine, Steve.

Steve: Okay.

TOM: It was just "RWWU." But you could never have captured any single frame and seen all of the letters. That's...

Steve: Exactly.

TOM: It's that rippling, that folding that you're talking about. So a machine is not going to ever see all of it unless it was smart enough to be able to integrate the way our minds do. But that's a much taller order.

Steve: Yeah, and it's not just like sort of revealing something static over time.

TOM: Right.

Steve: Because that would be easy to sort of programmatically fix. These things are sliding under ripples and under folds. And I think it's very clever. I don't know where it came from. But I'm sure looking at the page source you could probably figure out where they were getting their CAPTCHA technology because to me this looks like it would slow things down, probably for quite a while.

TOM: All right. Just three more, no, my math's wrong, four more. Question #9 from Rob in Las Cruces, wondering about SpinRite and hard drive cloning: I manage a help desk where we see our share of failed hard drives. Most data is backed up, so I'm not usually too concerned with bringing a dead hard drive back to life. But the other day a user came to us because her laptop would no longer boot. We didn't have a spare laptop drive on hand, so I had my tech run SpinRite so that, hopefully, she could keep working until we could get another drive and re-stage her laptop. SpinRite worked like a charm, and she was able to work the rest of the day without a problem. SpinRite, as it always does, came through in a pinch.

But I have a question: We received a replacement drive and took out her bad drive, which SpinRite had been keeping alive, and reinstalled her operating system, programs, et cetera. But would it be okay to use a program like Clonezilla to clone the dying hard drive? That would save time, and the end user would still have their customizations that take the user so much time to reset. Would this work, or do we run the risk of copying errors into the cloned image?

Steve: Interesting question. And I get people from time to time asking questions that are sort of SpinRite-related, and I say I sort of don't want to, like, turn this whole thing into a big commercial for SpinRite. Certainly our listeners are well aware of SpinRite. But I've seen questions like this before. We got a burst of SpinRite sales back when Microsoft was offering the converter from the FAT16 to the FAT32 file system. I don't even remember what that thing was called now. But it was when they were moving people to Win98, I think, from Win95. And drives were getting bigger, so they needed to expand the file system size.

But people were wanting to convert, in place, their file system from 16 to 32 bits. And the point was that any single error anywhere on the drive failed that process. And so what people realized was running SpinRite first would fix the FAT16 file system, and then the converter, which would previously have failed, was then able to succeed. Well, the same is true with drive cloning because typically the cloning software, I mean, it's not SpinRite. It's just doing a simple sector copy from one drive to another. Anything that causes it to glitch will cause it to fail.

So one of the reasons people today still purchase SpinRite is they're trying to back up a drive that won't back up because the image software will say there's an error on your drive. SpinRite will fix that, and then you're able to perform your copy. So the answer to Rob is, yes, running something like SpinRite, well, or SpinRite - actually there is nothing else like SpinRite, so running SpinRite first to fix the drive's errors will then allow a drive cloning or copying system which was previously failing to succeed.

TOM: All right. Good to know. Steve Fintel in Houston, Texas wonders about an HTML5 security analysis. He says:

Hi Steve. I've been an avid listener of Security Now! since Episode 1, and followed your Tech Talk column before that. I recently attended a security conference where one of the speakers talked about methods to attack HTML5. Many of the conference attendees started getting upset at the obvious step backwards HTML5 represented from a security perspective. I would love to hear you dedicate a Security Now! episode to this topic. We don't have time for a whole episode right now, but what do you think?

Steve: Well, we don't. But we certainly will be talking about it, at least in piecemeal. It would be hard to do an episode, like, preemptively because what I can tell you is we're going to have problems. We've already had problems with HTML5. For example, there's something in HTML5 called Offline Web Applications, which is an explicit caching technology that allows sites to cache their web pages statically in your machine. The problem with that, which has already been exploitedm is that if you briefly go to an insecure location, like Starbucks's Open WiFi, and get some malicious JavaScript in your machine, whereas it would only have been able to live in a transient form on the web pages previously, by leveraging this explicit application caching, there is already malicious JavaScript which is able to set up shop in your computer, thanks to HTML5.

TOM: Well, you're essentially installing a program now when you do that.

Steve: Exactly.

TOM: And so you're open to all the same risks.

Steve: Exactly. So there's an instance where it's a feature of HTML5 being repurposed. And I know that we're going to see, as we always do, clever hackers come up with ways of abusing things which are extensions of our browsers' capability a la HTML5, creating problems that we didn't have before.

The second class of problems will be your classic coding errors, and they already exist. For example, HTML5 brings a much-advanced rendering to us. There's a canvas metaphor into which you're able to draw with vectors or pixels in order to perform sort of on-the-fly local graphics rendering, which we have never had before. Now we have it, and there's mistakes in the code. So there have already been exploits, for example, taking advantage of buffer overflow mistakes in the screen canvas rendering technology in some browsers in order to run code that was - run code rather than graphics in your browser. So generically I can say HTML5 is going to keep our podcast busy.

TOM: Yeah. And it's not accepted yet. And that's a good thing because it gives us a chance to look at this kind of stuff, and you still have a chance to address it.

Steve: Yeah. I would say that browsers are rapidly moving towards it. But we're not rapidly using it. It'll have a slow uptake because of course websites can't use it robustly until all the browsers support it uniformly. And we're still - the browsers are rapidly moving in that direction. And there are some cool things. I mean, there are also some disturbing things, like there is persistent data storage which is explicitly available in HTML5, or a la HTML5, that we've never had before. It's like mega cookies. It's another place for identification stuff to be stored in your browser, so we're going to have to have some control over that.

TOM: Yeah. With great progress comes great responsibility, I guess.

Steve: Yes.

TOM: Question #11, Craig in Tyler, Texas wonders about lithium-ion battery inconsistencies: I don't want to beat a dead-horse topic, but something's been bugging me about the recommendations for lithium-ion battery management. Everything you've said on Security Now! about the topic makes perfect sense, and it even helps to explain why my laptop occasionally seems to be charging my battery even though I never use it with A/C power.

My confusion, however, comes from my cell phone. I have a Samsung Continuum which was made within the last year or so, and the manual for the phone quite specifically mentions unplugging the charger when the battery reaches 100 percent. The phone itself even beeps and pops up a message saying "Battery fully charged. Unplug charger." If all that you have taught us about lithium-ion battery management is correct, then why do some manufacturers still lead us, the consumers, to believe that these batteries can be overcharged or that we should be draining them all the time?

Steve: It's a great question. And I loved it because it highlights a distinction that I have made before, but I clearly need to make more clear. And that is, there is an absolute separation or difference between the chemistry and the technology of lithium-ion battery function and the management of that chemistry. And I'm aware of it, and I'm careful when I'm talking on the podcast to make sure I use the right words. But it would be very easy for someone who didn't recognize the importance of the distinction to miss it.

And so the idea, for example, is that we've talked about lithium-ion batteries not being trickle-charged. That is, some battery technologies like, famously, good old lead acid batteries, you're able to trickle-charge. You're able to, after they come up to a full charge, you drop the current to them and just feed it in at a very slow trickle, which has the effect of keeping lead acid, old, like, car batteries, full topped off. That kills lithium-ion batteries. They do not - the chemistry, the actual electrochemistry does not behave well if it's trickle-charged. You will damage it.

So the proper way to charge a lithium-ion battery is to charge it to a terminal voltage and then stop all charging. Now, there's no reason that Samsung hasn't done that except that they chose not to. Their manual says unplug it when it's fully charged. The phone says, "Unplug me, unplug me." Now, here's Apple and all other laptop makers, they don't have any problem with stopping charging when their battery's full. I don't know why Samsung has a problem. But they've chosen to. So it's not that their lithium-ion batteries are different from anybody else's. It's that, for whatever reason, they've chosen to manage the same electrochemistry differently than others. Maybe there's some advantage to them doing this that isn't apparent. I can't really see what it would be. But they've sort of - they've transferred some of the responsibility of proper battery management from their own hardware and firmware over to their users.

TOM: Well, they read all these great stories about crowd sourcing, Steve. And they said, well, we'll just crowd source battery management. The problem is they don't have a crowd. There's only one person using the phone.

Steve: Yeah. So anyway, so the distinction is, I've tried to be careful about assigning the responsibility in the proper place. But I would say that, Craig, the upshot of this is absolutely definitely do what the manual tells you. But the management aspects are different from the electrochemical aspects, which are pretty much absolute.

TOM: Now, is that why sometimes my computer will say "You're fully charged, we're not charging your battery," but it'll still say 98 percent? Because it's just saying, look, we're not going to keep charging this thing, it's dangerous.

Steve: Yeah, actually, and there is a good reason, a rationale for that. The term "battery," like, a battery of cannons in old Civil War era is a bunch of cannons. A battery is a bunch of cells. And the cells are series-connected, and it is crucial that you never overcharge a cell in the line of batteries. So what happens is, if the cell's charge is desynchronized, that is, if some cells have a few millivolts lower charge than others, as the battery as a whole is being charged up, the second that any one of the cells in the series-connected pack reaches its maximum charge, all the charging has to stop.

And so that's the reason that sometimes so-called conditioning can be useful, where you deliberately discharge the battery pack all the way down to zero, and then recharge it. Because what that does is it allows those cells with a greater charge to discharge and sort of re-zero themselves. And then, when you charge it back up, they all come up at the same time. It can also be the case that the cells were not well matched by the factory, and that you're always going to have some that are a little bit weaker. And so through charging and discharging, charging and discharging, they will tend to sort of lag behind the pack, so to speak. And exactly as you say, it's fully charged, but that only gives you something less than 100 percent of full charge. It's because of inter-cell variations.

TOM: All right, let's finish up with Question 12 from Paul Brogger in Tenino, Washington, bringing news of the resurrected HP-15C. He says: Have you heard that HP has released the HP-15C in a limited edition model? The original batch sold out instantly. It's out of stock right now, but more to come.

Steve: I tweeted this, and I wanted to thank Paul for bringing it to my attention. I've often talked about those. They're a family of calculators which are 30 years old, I think. Well, maybe not 30, maybe 20. But long since discontinued, except for the 12C. For some reason the financial version has stayed in continuous availability over time. But my favorite one was the 11C, which was iterated to the 15C. It's a landscape-orientation calculator rather than sort of the more traditional portrait orientation. I just love my 11C. And, I mean, it's sitting right next to me. I've got various of them in various places in the house so that I always have one near me, depending upon where I'm working.

And so I tweeted the news and wanted to let our listeners know, for anyone who's interested, if you just put in "HP 15C" into Google, you can find HP's website. It's $99 for this limited-edition HP-15C. It is, in my opinion, the best calculator ever made. It is just, I mean, and it's RPN, and RPN only. So you've got to be a Reverse Polish Notation person. But I'm dyed-in-the-wool that way. Ever since I was in high school, I spent the $400 that I saved up from a summer job to buy myself the HP-41 was the very first scientific calculator that Hewlett-Packard produced. So, love those machines.

TOM: I'm still partial to the TI-35.

Steve: Yup, another classic.

TOM: Not as programmable. Actually not programmable. Had a memory, though. All right. That's the end of our questions, Steve. Thanks so much.

Steve: My pleasure, Tom. And next week, as our listeners know, we will - I'll have Leo back, and we're going to do a special science fiction episode for the holidays. We may cover a little bit of security news, if anything fantastic happens. But mostly we're going to talk about sci-fi: movies, TV, and books.

TOM: I can't wait. You know I do a sci-fi podcast with Veronica Belmont. So I'm definitely tuning in for this. I can't wait to hear what you guys talk about. I always get good recommendations from you when you talk about sci-fi and stuff.

Steve: Cool. Thanks, Tom.

TOM: All right, that's it. Don't forget, Steve Gibson, you can find his work at GRC.com. All kinds of good stuff there, like SpinRite, like ShieldsUP!, like Haystacks. Look that up, you're going to love it. Appreciate you watching Security Now!. Leo will be back next week, like Steve said. I'll see you later.

Steve: Thanks, Tom.