SECURITY NOW!

Transcript of Episode #251

Listener Feedback #93

Description: Steve and Leo 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-251.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-251-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 251 for June 3, 2010: Q&A #93.

It's time for Security Now!, the show that covers your security, your privacy, keeping you safe online. And, boy, nowadays there could be no better time to do that. With us our great friend and security guru Steve Gibson from GRC.com. He's the man who discovered the first spyware, coined the term even, and then wrote the first antispyware program. His ShieldsUP! is used by millions. Hey, Steve. That's your new slogan. "Used by millions." Hey, Steve. How are you today?

Steve Gibson: Great.

Leo: I should start saying the creator of the dog - what was it, the ultrasonic dog killer.

Steve: The portable dog killer. That might put a few people off. And you'd wonder then why the sponsors had wandered off.

Leo: Only those who know, know how wonderful that is. And I had somebody come up to me yesterday, you know, was a little behind on Security Now!. And she said that episode was so inspiring, so exciting. You know, it's often parents who tell me that because...

Steve: And that's, I was just going to say, as soon as you were through with your thought, that I've heard from so many parents who have said they made their kids listen to it, and it really got through to them.

Leo: Yeah. Because, you know - and, now, she apologized. She said - it was "funcrunch." It was Julie out at the laser tag we did on Monday. She said, "Oh, but I'm only a programmer. I only do - I don't do physical things." I said, "You know what, me, too. I don't think Steve was saying it has to be building physical things." I mean, that's really cool, and I admire people who do that. But making anything, creating anything - a sonata, a computer program...

Steve: Very good point.

Leo: ...or a portable dog killer, it's the act of creation is the point.

Steve: Yes. Yes.

Leo: And just get kids to turn them from consumers to creators.

Steve: Yes. I think that's an absolutely correct generalization of that notion.

Leo: Well, it was very inspiring. But that was Episode 91, or 90. We are now up to 90 - no, no, I'm sorry. 90? What am I talking about?

Steve: No, that was 248.

Leo: 248. We're now up to 251.

Steve: Yes.

Leo: And we are back on track for Q&A #93. That's what I was thinking of.

Steve: Yup. We've got a Q&A, a bunch of interesting things. I have a new section that we've never done before that I was inspired by a long note from someone that was important. So it's a notes-from-the-field little insert that I want to share with our listeners before we get into the Q&A.

Leo: Great.

Steve: And of course we've got our regular top-of-the-show stuff. But bizarrely enough, not a single security update.

Leo: What?

Steve: Not one. I don't know. Strange.

Leo: Is the world secure? Have we secured everything? Are we ready? Are we done?

Steve: Well, and it's funny because that comes on the news that Adobe is reconsidering their quarterly update schedule.

Leo: Uh-huh.

Steve: Uh-huh. And you may remember that when they announced that they were going to be doing quarterly updates, after I was through laughing, I said, well, we'll see how long that lasts. And of course they began then doing emergency updates all throughout the mid-quarter. And they finally decided that they're going to synchronize with Microsoft's second Tuesday of the month. So, so much for Adobe's quarterly update. That's not going to be happening. Looks like they're going to go to standard monthly updates. And even that may not be enough.

Leo: Even when Microsoft went monthly I thought, well, this seems like a bad idea. But they've done all right with the monthly updates. I guess it confuses people, and it's hard for business, when you update too often.

Steve: I think that, yeah, the problem is, and we understand why there's this aggregation of updates, is that it's purely for the enterprise users who need to calendar this event, because that's what it is. They need to get them; they need to make sure that the Microsoft updates don't mess things up. And we also know that, I mean, against some people's better judgment, enterprise users are often delaying this update cycle to wait to see if anything bad happens because there have been instances where Microsoft's changes have broken things. And so, I mean, not just enterprise-specific things, but things in general. So anyway, it brings some discipline to it. It's certainly nice for us, although then we get these weird weeks where we didn't have anything. However, there was lots of other security news. One probably high-visibility new hack is extremely clever. It was essentially invented by the creative lead for Mozilla Firefox, a guy named Aza Raskin.

Leo: Oh, yeah, I know who he is. Yeah, he's great. Well, he's weird. He's a character, let's put it that way.

Steve: Well, and when you hear this you're going to know why. He realized that there was a fundamental weakness in the multiple-tabbed model of browsing because script running on a page could tell when that page had lost focus to another page, that is, when it had been covered up when another tab was chosen. And the script running, JavaScript running on the page could, after a little bit of a delay, so it wouldn't get noticed, could change its tab name and itself to look like some random other site, and not necessarily random because it's possible for the script to use CSS tricks that we've talked about in the past to figure out what sites this particular user goes to.

So the script could know that this is a Facebook user, Citibank, Twitter, Gmail, whatever; and, when the tab is not being displayed, change itself to the login page for that particular facility that the user uses. Or, like, say you've got new mail on the tab or whatever. The point being that then the user sort of, like, notices the tab, or just thinks he's got Gmail open, clicks that, for example, and he's at the Gmail screen that might say, like, your session has timed out. Please log in again.

So it is a very clever new type of phishing hack where - which would probably catch a lot of people. I mean, I think it would catch me if I wasn't really paying attention because I'd think, oh, okay, and I would type my credentials into this login page, which of course is not Gmail, it's some other site that is using script to masquerade. And so that's the nature, it's called "tabnabbing."

Leo: How close is this - have you seen the likenabbing? Which is I guess kind of like that click hijacking thing, where people are getting the Facebook Like and using it? It's clickjacking, really, it's the same thing as clickjacking. So this isn't exactly clickjacking.

Steve: Right. I've run across the Facebook Like issue and haven't had a chance to track it down yet. And so Aza made a blog posting, talked about it. It's sort of like everyone sent me links saying, oh, have you seen this about tabnabbing? I said, yeah, yeah, yeah, we're going to talk about it today. Anyway, that's what it is. So it's, I mean, it's not horrible. But it - and again, it requires scripting, which we understand is a mixed blessing.

And I think overall the lesson we're seeing here, I mean, this is an unintended consequence of scripting, and it's not an abuse of scripting. Well, I guess it's an abuse of scripting. But it's not taking advantage of a scripting flaw. It's taking advantage of scripting features, and the nature of what happens if you have multiple tabs, and how you can sort of leverage that. And what it says is that, yes, scripting is a problem. But we also know scripting is with us for the long run. When Jobs is prancing around talking about HTML 5 being the future, he's talking about, inherently, scripting and new root features in HTML 5 being an alternative, for example, to Flash, which he's arguing against lately.

So there is no way, as you remind us, Leo, that we're going to unfortunately get away from scripting. I say "unfortunately" because it scares me so much. But what it means is that the sites you go to, you need to trust with running code in your browser. And this is an example of, yet another example, a clever, I think, new idea for how scripting can get you in trouble if you went to a site that wanted to take advantage of the fact that you were trusting it with scripting on your browser. Not requiring anything to be broken; just, oops, you know, scripting can do that.

Leo: Does this work on all browsers? Or is it...

Steve: Yes. You might need different scripting, like browser-specific code in the scripting. So, but you could certainly adapt it so that it would run in different browsers. JavaScript has the fundamental common set of hooks that allows it to do this on any browser platform.

Also in the news we have the continuing Google WiFi inadvertent spying update of the week because this is now a weekly mention. Now they've been class-action-sued by multiple ISPs, in addition to the two people we talked about last week who filed the first class-action suit. Now there's a couple different ISPs that are suing on behalf of their own customers. And the U.S. FTC, the Federal Trade Commission, has formally asked Google to freeze all data and documents pertaining to this, to prevent their destruction, for any of the 33 different countries where Google collected data over the last three years that it was doing this. Google had already destroyed data under request from Denmark, Ireland, and Austria. So that data is gone. And presumably it will comply now with the FTC's request not to do any more destruction. I don't know what Google would do if a country explicitly asked it to destroy its own data. I imagine it would. It would seem to me that would be the thing to do.

Leo: Yeah. You've got to adhere to the country's laws wherever you are, yeah.

Steve: I think so. And in a really interesting little bit of news, Symantec security guys discovered a massive stockpile of 44 million gaming login credentials. They've discovered a central repository...

Leo: That's got to be everybody. I mean, how many are there?

Steve: This is amazingly sophisticated. So there's - it's a flat-file database, 17GB of data, 44 million login credentials. And there is a trojan that goes along with this called "loginck." It's called Trojan.Loginck. That's spread around many different computers as, you know, like a trojan network. And what it does is continually refine and filter and validate this 44 million login credential database. So these trojans are scattered in a network across the Internet. They're - and this is how Symantec tracked this down. They're checking back in with the database, pulling out gaming login credentials from the database, and using those to login to gaming servers to verify the credential's current validity; and also checking, for example, the level of the game that this person is at and what assets they've accumulated. All of this is then built back into the dataset. This is timestamped in order to say this credential has been checked on this day. And these credentials are then sold for anywhere between $6 and - are you sitting down?

Leo: Yeah.

Steve: $28,000.

Leo: What?

Steve: Depending upon the gaming value that has been...

Leo: Oh, so if it's like a Level 70 in World of Warcraft...

Steve: Exactly.

Leo: ...that's worth some bucks. But to whom? I want to know who's paying 20 grand to be a Level 70 warrior on World of Warcraft.

Steve: Well, to steal somebody else's Level 70.

Leo: Somebody else's Level 70.

Steve: Yeah. Yeah.

Leo: Amazing.

Steve: So anyway, I just that, okay, this is just strange but true.

Leo: I really think that this actually underscores something that's cultural, which is that there is - increasingly we're seeing there is actual value to the virtual, to virtual goods.

Steve: Yes, yes, yes. In fact, I mean, we've seen instances where people were selling their virtual goods, you know, the ones they actually legitimately owned, they were selling them on eBay; right?

Leo: AlexC says he would pay 20 grand for a Level 80 in Tier 10 with a legendary. I don't know what that is, but, wow [laughing].

Steve: Wow. I don't have any.

Leo: You know, the truth is it probably does represent a huge amount of money because to get to those levels requires grinding for hundreds of hours. So it's probably worth five bucks an hour, really, because it's such a lot of work to get there.

Steve: And Mark Thompson, who follows this industry, has told me that there are people who build up these entities, whatever you'd call them, and then sell them, and then start over.

Leo: Yeah, it's gold farming, or it's - yeah, yeah.

Steve: Yeah. So they, like, they grow a persona in a virtual gaming environment, making it very valuable. And of course they acquire the skill to do that. And then they sell them to people who don't have the skill themselves, but they've got the money.

Leo: Our friend Cory Doctorow has written a new novel about that, "FTW." That's the whole premise of the sci-fi novel. It's a juvenile. It looks to be a great book. I can't say I've read it yet, but I can't wait to read it.

Steve: So a little bit of news from me. I have two new blog postings.

Leo: Man, you're going crazy.

Steve: Over at steve.grc.com.

Leo: Awesome, Steve, that's great.

Steve: The first one is titled "The Obvious Genius of iPad."

Leo: Saw that, yeah.

Steve: And the subtitle is "Thank goodness Apple can't patent what it got right."

Leo: Because, you know, we're already seeing a slew of clones being announced running Android.

Steve: 40 pads...

Leo: Wow.

Steve: ...are being tracked, by some companies, that are in the works.

Leo: I think that's very good news.

Steve: I do, too.

Leo: I'm excited about it.

Steve: And in fact what I wanted, the reason I did the posting was I wanted to just get on the record my position, which is, I mean, I know Paul - I've read everything that Paul has written. And I wanted to explain that it's the form factor that, I mean, like what it is, what are the things that Apple got right. I think it was entertaining to watch all of the industry pooh-poohing the notion beforehand of Apple doing a tablet because the industry felt that it knew better, that tablets had tried and failed famously for years. And here Apple comes along, and I'm sure you saw the news, Leo, that they've sold two million in less than two months, essentially. So their original 28 days for the first million, they have continued that. That wasn't just a burst initially.

And I have to say, as I've been out and about with mine, I mean, I'm an early adopter of technology. I carried my Kindle around for a couple years. Nothing, I've never seen anything like the lust that people have for this thing. And partly, you know, Paul made the point that it was sort of a high-end luxury item, that people like to be seen with it, or like to wave it around or show it off. For me, that's not it at all. I mean, I recognize maybe there are some people that were like that with the iPhone initially. For me it's that it is absolutely functional. It's the all-day battery life and the immediate-on, turn it on, there it is. And it's connected. And, I mean, it just - for me it's serving a function. And it's so functional that I am just really pleased with it. In fact, and this is a little controversial, yesterday I split my personal Twitter account from - I had, of course, SGgrc. I created SGpad because I wanted the freedom of tweeting to my heart's content about pad stuff without bothering people who really didn't care to receive all of that.

Leo: That's really smart. I think that's a really good idea.

Steve: And it's been met with some resistance. People have said, wait a minute, that's not the way Twitter works.

Leo: It is exactly the way Twitter works. Why isn't that the way Twitter works?

Steve: Well, my logic was that, from an economic standpoint, it's extremely low cost to follow somebody.

Leo: Exactly.

Steve: I mean, thus people follow thousands of people.

Leo: My rule is always follow easily and unfollow even more easily.

Steve: Right. And so my feeling was, Twitter makes it so easy to follow. Yet at the same time, if people are getting a bunch of stuff they don't want, then they're being forced to always filter it.

Leo: Right. Or unfollow you.

Steve: Or unfollow.

Leo: Which is kind of a broad brush if they like some of your stuff.

Steve: Right. And so my feeling was I'm willing to accept the responsibility of creating some channels and allowing people to choose which channels they want to follow. And since Twitter is an aggregator, essentially, and it's so easy to follow somebody, if they want all of my stuff, they just follow my channels. And I'll divide them up rather than requiring that they filter from a single channel. So I have had some people who thought it was a great idea and said, hey, that's sort of more like the newsgroup model, which I guess is the way I've been thinking about it. So anyway...

Leo: No, I think you're exactly right. We have a TWiT channel; a TWiT Live channel; I have a personal channel. And I think it makes sense, in fact I think it's a very - because people can follow all of your channels. It's easy. It's trivial.

Steve: And it all comes into one place for them. And they don't even have to pay attention to...

Leo: Exactly.

Steve: ...which of my channels it's coming in on.

Leo: I think that, no, I think you grokked it. I think you have the exact right idea. In fact, I think you've done something that a lot of veteran Twitter users haven't quite understood. There's a whole variety of content in any given feed, some of which you may like and may not like. And that's the real problem with Twitter is there's really no good way to filter. It's interesting because some of the more advanced third-party clients now include the ability to filter. So I could say I only want - I don't want to see any - where it comes up is conventions. E3 is coming up. And there'll be a - you'll see, in Twitter you'll start to see a slew of E3-related gaming news from all the people you follow. If you could say "everything except if it says E3 I don't want to see it..."

Steve: Nice.

Leo: Exactly. So you're doing that by hand, basically.

Steve: Well, I'm glad. And I have to say that my favorite critique showed up shortly after I announced that I was splitting my feed, from a guy named Chad in Baton Rouge. He sent back, "I split my accounts for posts that start with or without prepositions."

Leo: He's joking, of course.

Steve: Of course he was joking, yeah. Anyway, I got a kick out of that, so I wanted to say...

Leo: So now you have SGgrc for your full feed. For pad, not iPad, but pad-specific stuff, SGpad.

Steve: Yes, and that's an important distinction I wanted to also make is that I'm bullish about the pad form factor. Apple, I give them absolute credit for having shown the world how to do a pad. Unfortunately - well, unfortunately for Apple, fortunately for the rest of us - there isn't anything that they've done that everybody else can't do. Or maybe there is.

One of the things I was commenting to my friend, we were driving in Southern California a couple weeks ago, and a beautiful Ferrari passed by. And this is a thought that I've had for a long time. I look at this car, and I think, my god, that's just gorgeous. Why don't other cars look like that? I mean, they could. There's nothing difficult about bending the metal in the way that Ferrari somehow magically manages to do. But somehow, even though Detroit, for example, tries to hire, I assume, really good designers, they don't produce cars that look like Ferraris. They, like, sort of do me-too sort of things that never quite make it.

And of course this - I wonder, then, if Apple might not have some of that same magic. Will we see pad alternatives to the Apple that we want in the same way that we want the iPad from Apple? And I don't know. But, boy, it's going to be a really fun thing to watch happening.

Leo: You know I've been an iPad proponent since it was announced because I immediately saw the value of it. But I have to say I also see the value of open. And Steve's closed attitude on the iPad irks me a little bit. So I'm looking forward to Android-based, somewhat more open designs. And I suspect it's really about multi-touch touch, the mobile form factor versus the desktop operating system. I think Android could do a good job. We'll see. It'll be very interesting.

Steve: I'm hoping. So, yeah, so SGgrc is my regular feed. I crossed the 9,000 followers mark yesterday at some point. And then SGpad is the separate feed where I'm just going to be absolutely free to tweet about pad stuff. I mean, I'm carrying it with me all the time. I'm thinking about it. I'm experimenting with apps. I found a pair that I like much better, for example, than GoodReader, which was the PDF reader that got an early start on the iPad. I just don't like it as a PDF reader. It has the advantage of allowing you to get stuff into it easily. But the combination of Downloader and iAnnotate I like much better. Downloader is a fantastic downloader and viewer of stuff. And then you can use the "open with" to send it over to iAnnotate, which is just a feature-rich, very nice PDF reader. So I want to be able to share that stuff without worrying that I'm bugging people that have no interest at all in pad stuff.

Leo: I kind of am tempted because a lot of the newsreader software that I use has the capability to tweet as you go. And right now I send it to Delicious. But some of these don't have Delicious capability. And I'm thinking it might be nice to tweet, but I don't want to fill my stream with - so maybe I should have a Leo's Feed. You're inspiring me, Steve. You're teaching me. You're schooling me in how to do this.

Steve: I'm glad. I wanted to discuss it with you because it seemed like the right thing to do.

Leo: I think you're right, yeah. Giving, look, it's never wrong to give people control.

Steve: Right.

Leo: That's never wrong.

Steve: Give them choice. And of course the proof will be in how many fewer followers I have in the pad-specific account than I have in my general all-purpose account.

Leo: That's true. If you had the same number in both, then it would be an indicator that people wanted everything.

Steve: Right.

Leo: And everybody wanted everything. But we know that's not true. We offer - this is a good example. We offer a Leo feed that is just the shows I'm on, as well as individual feeds. So this is on that, you know, Radio Leo as well as - and we don't publicize it, but there's also a TWiT everything feed that people could get everything. But my feeling is - it's very similar. People are going to build their own assortment of podcasts based on collecting the - what's the trouble of subscribing to four shows? Then you have exactly what you want. And in fact that does seem to be the case. The Radio Leo feed I think has 30 or 40,000 subscribers. But those are pretty hardcore people. Most people subscribe to the individual shows.

Steve: Well, and also remember that I have the nonpersonal Twitter account, GibsonResearch. And that's only got about 5,000 people compared to SGgrc, my personal feed, that's got 9,000.

Leo: Well, that's also a data point. It tells you what people want on Twitter.

Steve: Yes. It says that there are people who want GRC-related news only, period. And I want to respect that and give them the choice.

Leo: And I also think that it shows that people want personality and authenticity, and they're less interested in ads on their Twitter feed. They want to hear from you. They want to hear what Steve says. It's really a personal thing. And that's what I like about it. I want to hear what Steve thinks today.

Steve: And you probably, just to make a note of this, heard that AT&T has announced they're removing...

Leo: [Growling]

Steve: Uh-huh [laughing].

Leo: [Growling] So let's actually say this because it's very important you know this. If you have already subscribed to the unlimited feed, the $30-a-month feed on your iPad, they say - we'll see...

Steve: You'll be grandfathered.

Leo: They say that will persist. But no one will be able to get that anymore. You will have to buy a $25-a-month 2GB-capped account. That'll be the biggest account. And you can add 5GB for 10 bucks.

Steve: My experience was, because I thought, let me see how the $15, 250MB plan works. Well, I got my first warning notice after four days.

Leo: Yeah. My father-in-law, who is 80, got his in a week. 250's not a lot.

Steve: And I wasn't downloading video or movies or any big stuff at all.

Leo: No.

Steve: The problem is that, in our world, everything has gotten big. I mean, the first hard drive on my PC, my XT, was 10MB. So 25 times that I used in four days really not doing much, just sort of poking around. And I thought, well, okay, that experiment told me something. So I immediately switched to the unlimited for 30 bucks. So I guess the only thing we can do to help our listeners is to say, hey, if somehow you're surviving on the $15 plan, or not surviving on it, you may want to jump to the $30 plan to get yourself grandfathered in before that's gone forever. Although...

Leo: I think it's too late.

Steve: Oh, no kidding.

Leo: I think it started, like, at midnight. And I'm hoping, Papo, I hope you subscribed to the $30 plan yesterday. Because I don't think you can get it today. I don't know. Oh, it starts Monday. Okay, they're telling me in the chatroom it doesn't start till Monday. So now is now.

Steve: Yay, yay.

Leo: Now get it. And if you're hearing this on Monday, I'm sorry. You have till June 7th.

Steve: Now, I do wonder if maybe 2GB - they're saying that only 2 percent of users are using more than 2GB a month.

Leo: Yeah, the 2 percent are all the people who own iPads, iPhones - I don't know. I think 2GB is not much. In fact, if you watch, if you use our TWiT Pad application...

Steve: Oh, yeah.

Leo: ...and you watch our shows...

Steve: If you're doing any big media stuff, then...

Leo: ...you're going to have to stop. I mean, this is why I'm pissed. AT&T basically, this was a complete...

Steve: Well, it's a blindside.

Leo: This was a, what do they call it, a loss leader? This was a tease. This was a lie is what it was.

Steve: Yeah, and it didn't last very long for us to be told $30 unlimited. It was like, woohoo.

Leo: I'm thinking that this is - there's something going on behind the scenes. I think AT&T offered this special deal to keep Apple away from Verizon.

Steve: Well, and have you heard that Verizon apparently has CDMA iPads they're testing?

Leo: I saw that. Rumors, we don't know. But I tell you there was something yesterday that happened that may be more than a rumor. Steve Jobs was speaking at Walt Mossberg and Kara Swisher's D8 Conference. And they asked him when's Verizon coming, and he visibly bit his lip, like he wanted to say something, but he didn't. And I think I wouldn't be surprised if Monday, which happens to coincide with the day this is changing, Steve comes up onstage and announces Verizon iPhones or Verizon iPads or...

Steve: At the Worldwide Developers Conference.

Leo: Yes. Now, no one knows. And those are all rumors. But at this point it seems to me that the relationship between AT&T and Apple is - if this didn't shatter it, I don't know what will. It's time, Apple.

Steve: Yeah. He can't have been happy with this. I mean, where you keep hearing stories that people in San Francisco and New York can't use their phones.

Leo: Can't wait to get rid of AT&T.

Steve: Yeah.

Leo: And you just imagine what a Verizon iPad would be, or a Verizon iPhone would be.

Steve: Well, Verizon's my network. I mean, I left Cingular because of the poor performance. Then AT&T bought Cingular. And I was - and I moved my number, yanked my number away from Cingular over to Verizon. Almost said it. Anyway, yeah, it's a great number. I didn't want to lose it.

Leo: Don't say it out loud. I don't remember it, but - you know, you and John both have a certain fetish for numbers, your phone numbers. I won't say any more.

Steve: Yeah, well, it's a thousand number. And those are not easy to come by. Three zeroes on the end, so...

Leo: That is pretty good. That sounds professional.

Steve: I had a great, neat note, speaking of your father-in-law, from a grandmother. The subject was YAT - Yet Another Testimonial was her acronym - for SpinRite. She said, "My situation starts out slightly different than your typical SpinRite stories. I'm a 55-year-old grandmother. I have what my husband calls" - I love this - "a thriving not-for-profit computer business. I help family and friends and referrals with software and hardware problems." Apparently for free. She says, oh, she says, "Sometimes I receive cash or a gift card, or even the occasional pie, for my work. I do it because I love computers, and it's my way of helping others."

Leo: Isn't that awesome.

Steve: And I love the fact that Kathy's going to be hearing this. She says, "I have not missed an episode of Security Now! and have been waiting for the right time to buy SpinRite to support your work. Recently my niece brought me her laptop that would boot to a black screen with four choices. Each choice caused the machine to reboot. I immediately knew two things." And Leo says yeah.

Leo: Yeah. Been there, done that.

Steve: "If she brought it in to the big box store where she purchased it, they would surely reformat it. And before hearing about SpinRite I would have spent hours trying things to no result. SpinRite took only four hours, unattended, to get this laptop up and running again. I was going to surprise my niece and back up her data. In my experience, the data from most regular people, non-geek types, can fit on one CD, or certainly one DVD. This 60GB hard drive had only 10GB of free space. I elected not to back up anything. She promised she would pick up an external drive on her way home. I'm pleased to add a YAT - Yet Another Testimonial - for SpinRite to the universe. Thank you for a great product, and thanks also for Security Now!. It is required listening for me," says Kathy Zwolski in Minneapolis. So thanks for sharing that.

Leo: Great story. Hey, there's one other news story I just wanted to comment on. And I knew about this a little ahead of time because, as you know, Colleen Kelly, our esteemed VP Engineering, left for Google a couple of weeks ago. And she told me a couple of weeks ago that Google was not, you know, you get a computer when you join a company, and the offer was...

Steve: Oh, I know what this story is. And you're right, it is a topic for this show.

Leo: ...Mac, Linux, and no Windows. Now, Google is - this is speculation from the press that Google's not doing it for security reasons. Google isn't really saying. But apparently you'll have to go - you have to beg if you want Windows.

Steve: And Microsoft, well, we should back up a little bit and tell people that the news is that Google is formally telling its employees they cannot have Windows any longer.

Leo: Nope. Nope. And a new employee is not offered a Windows machine. I don't know what Colleen chose because she's a big Windows fanatic. So I'm going to guess Linux, but I don't know.

Steve: I'll bet she went Linux, yes.

Leo: Yeah, I would think.

Steve: So Linux or Mac, you're allowed to choose. Apparently some employees are allowed to keep Windows on laptops but not on their main desktop machines. Google is saying this is a consequence of the continuing security problems with Windows. Microsoft has blogged that, like, not happily, that they disagree with this from a philosophical standpoint; that Microsoft is saying, now, wait a minute, let's take a look at the history here. We're doing a lot to improve security and blah blah blah. So you'd expect something back from them. And I don't disagree that finally Microsoft is truly getting a clue. They have hurt the world, however, by taking as long as they have to do so. I mean, it really seems like Microsoft was dragged kicking and screaming into doing a better job with security.

Leo: Apparently Colleen tweeted that she's using Ubuntu 10.04, which is Lucid Lynx, the newest Ubuntu, which I, by the way, love, and I think that was a good choice on her part. Even though I'm a Mac fanatic. So...

Steve: So I have one "notes from the field."

Leo: Oh, okay.

Steve: And then we'll get into our Q&A.

Leo: Great.

Steve: This is from someone who asked to be anonymous for reasons that everyone will know shortly. He said, "Regarding Security Now! 249 on cars and plug-ins, the vehicle ECU remote attack. Steve, I've been listening to Security Now! since the early days, and I think you're doing a good job of explaining basic tech concepts in a very easy-to-understand way. I don't always agree with you, but I do respect your opinions. Mostly I don't agree with you about doing everything in assembler."

Leo: [Laughing] You're not insisting on that.

Steve: And he's certainly - no, and he's certainly not alone. I'm not saying everyone should use it, I'm just saying I do, and I'm sticking with it. He said, "I mainly work in C or C++, and I share a lot of code with other developers, which I think makes assembler impractical. In SN-249" - here we go - "you talked about vehicle ECUs being susceptible to attack."

Leo: Right.

Steve: "But you said that this was not a major issue yet because current attacks require physical access to the vehicle. Well, Steve, I've got some bad news for you. You know how a lot of the security exploits in web browsers are not in the browsers themselves but in plug-ins and extensions? Well, these days cars got plug-ins, too. I work as a real-time software developer and also do electronic design for a small company that develops aftermarket fleet management systems for vehicles. Our units are installed in many thousands of vehicles around the world, including military vehicles, police cruisers, buses, trucks, heavy construction equipment, and of course many passenger cars. These units are GPS equipped and are using GPRS" - the cellular packet radio system - "to send data in real-time back to the server. This data includes the vehicle location, mechanical data such as engine conditions, speed, RPM, current gear, et cetera, and physical data such as hard braking events and even hard turns and accelerations. We have an onboard accelerometer for that."

Just to break for a second, so clearly what they're doing is they're creating an add-on system for sort of monitoring the way vehicles are being driven out in the field, in addition to where they are moment to moment and so forth. So he says, "Until about a year ago our units were designed as passive monitors that were just listening to the communication channel between the vehicle ECUs on CAN-bus or J1708 lines. We then interpreted the data and extracted information like the RPM, speed, and engine temperature. Recently, in order to support a wider range of parameters and vehicles" - here it comes - "we developed units that are able to transmit on the communication buses and request parameters that are not transmitted periodically by default."

So we can see what's happened is they went from a passive background monitoring mode to an active participatory mode because they needed to stimulate the equipment on the bus to feed them information that they could no longer - that wasn't available just by sitting there and listening passively. So he continues, "This allows us to support the OBD-II standard" - whatever that is, clearly some open vehicle thing - "which is a request-based protocol that is implemented in all cars that were made after 2001. We also use it to request extra parameters on J1939 data buses on heavy vehicles. While we were developing this system, we had a few incidents..."

Leo: Huh.

Steve: "...where wrong data was sent to the vehicle, and we did encounter some interesting results ranging from nothing at all to a vehicle engine shutting down and refusing to start, and the dashboard lighting up like a Christmas tree. We now have quite a significant install base of these kinds of units. And we did have one incident where an employee sent the wrong configuration to a number of units in the field, causing a few trucks to refuse to start. That was fortunately solved by sending the correct configuration to the affected units.

"Now, we do try to build our units robustly. But security was never a concern for management and was always treated as a non-issue and thus was not allocated any developmental resources. The units' communication with the server is not encrypted and probably cannot be strongly encrypted because of the very low-end - 5 to $10 - CPUs that are used in these units. These CPUs were selected for both low power consumption and low cost consideration. We know GSM is practically broken, making eavesdropping on communication channel possible. The communication protocol would probably take a while for an attacker to reverse-engineer, but should be possible. And I should know, as I've been reverse-engineering communication protocols between engine ECUs for quite some time, and I've gotten quite good at it.

"An attacker, given resources, it doesn't have to be the NSA by any means, could probably remotely disable vehicles equipped with our system or any similar one, or even cause a system to transmit arbitrary data of his choice onto the vehicle data bus. Thus I'm pretty sure that the same commands that were sent during the research you mentioned, such as the command to disable the brakes, can be sent remotely by an attacker who took control of a unit such as the one our company makes. Now, that would make what used to be a local exploit into a fully practical remote exploit.

"I'm not sure what can be done about this at this point, as our company, and probably most of our competitors, try to get more features into the market as fast as possible without much concern, or even any understanding of, the security implications. For the automotive industry today, security isn't even an afterthought, it's never thought. The people that are making the decisions usually don't have the knowledge to assess the security implications and are also reluctant to listen to the ones who do, labeling them as alarmists or paranoid. I do try to bring up those issues from time to time, but I'm not going to risk my job over it. As you have foretold, I'm pretty sure that these issues will surface in a few years and make headlines. Only when that occurs will both vehicle manufacturers and aftermarket equipment companies be forced to address the issues. But I'm afraid it would take a few years and a lot of bad press to see any change.

"Now, Steve, feel free to contact me if you want any more information. But if you decide to discuss this on the show or on your website, I would appreciate if you would leave my name and any details that could identify me out of it, as it would not take much to trace this information back to me. This is a very small industry. And as I said, I do like my job. Name withheld by request."

Leo: Wow. That's an interesting story. Wow.

Steve: And does it surprise any listener of this podcast that this is the nature? I mean, anyone who has been paying attention for the five years we've been doing this and following along, I mean, you would guess all of this if you hadn't just heard it from someone who actually knows. I mean, unfortunately this is the nature of security, and it's the nature of the way our systems are still being developed even today. We need to learn the hard way, unfortunately.

Leo: Every time I get in the car now I look at my OBD-II port, just to make sure there's nothing on it [laughing]. Oh, dear. That's scary. Steve, we've got some great questions for you. And we've got about an hour left in the show. So we're going to get through them as quick as we can.

Steve: Great.

Leo: All right, Steve. Are you ready? Q&A time.

Steve: Let's go.

Leo: Let me open up my questions and start with numero uno. Where is it? Where did I put it? Dan in Sioux Falls, South Dakota. He's asking about HTTPS instead of HTTP. Steve, after hearing stories such as Google capturing data that was sent in the clear via WiFi, and ISPs performing deep packet inspection on customers' traffic, I was wondering why we don't all move to a system that allows all Internet traffic to be encrypted. Couldn't HTTP be deprecated in favor of HTTPS, mail sent using SSL, et cetera? I realize not everyone would want to buy an SSL cert for their personal website, but maybe we could have two levels of SSL certification - first a free cert that allows the website and the visitor to encrypt data, but not necessarily verify the identity of the website owner. The second level, a traditional SSL cert with encryption and verification that the owner of the website is who he or she says he or she is.

Is there any technical reason why you couldn't do this? Nearly every Internetcapable device sold within the last five years can handle SSL certs; right? I personally would love to see ISPs become merely a dumb pipe, transmitting data but having no idea what the data is. Thanks for the great podcast. Dan. Well, great minds think alike because we talked about this, didn't we, Steve.

Steve: Yeah. Well, okay. So in general we're certainly seeing a movement in the direction of more use of encryption. And it would be nice if at some point in the future we figure out how to do this. But it turns out we can't at the moment. The reason SSL works is that it provides both encryption and authentication. And the authentication part is really the focus of Dan's question. It's what he left out of the equation. Because without authentication, then you have the problem of impersonation. And that means that man-in-the-middle attacks are completely possible, no way to detect or stop them.

The point being that it's because you have an authenticated certificate being offered by the remote server, that is signed by someone you trust, the certificate authority. That's what prevents a man in the middle from being able to splice into an SSL connection. Essentially you connect to the man in the middle. The man in the middle connects to the server. And you see an SSL connection, but in the middle it's been decrypted and then reencrypted. Meanwhile the man in the middle can see everything in the clear.

It's certainly the case that if we were only trying to protect mistaken eavesdropping like what Google did, then, sure, you could just have sort of an in-the-clear exchange of a cryptographic key and use that to encrypt the traffic so that passive eavesdropping would be thwarted. But you wouldn't get any verifiable security, which is what SSL gives us. And I worry a little bit if people might not think that was all they needed. That is, sort of saying, oh, look, I've got - what do I have, sort of half a padlock, or sort of something, I don't even know how you'd show it. But so the reason we just can't sort of have like a universal free cert is then the bad guy would have one and could easily intercept your traffic which you think is encrypted, when in fact it wouldn't be.

I've thought about this a lot, as it happens, because, for example, this CryptoLink product that I'll be working on next doesn't use SSL, doesn't use certificates, and is much stronger than SSL because, I mean, it really obeys a TNO, a Trust No One model. Remember that with SSL you're trusting the certificate authority. So it's not that you're trusting no one, you are trusting someone. It is possible to set up a true TNO system, Trust No One, and that's what I'm designing with CryptoLink that even goes beyond SSL in terms of absolutely not trusting anyone. It can be done, but it can't be done in a uniform open Internet where attackers have the same knowledge that everybody else does because then they can impersonate one of the endpoints. There's just no way around that.

So unfortunately we're not - I can't see a solution today for what Dan suggests. You have to have some information which is not known to the attacker in order to thwart man in the middle. And that requires something like a PKI, a Public Key Infrastructure such as we have now, with chains of trust and trusted roots of some sort.

Leo: So you're saying, well, but a guy who just wants encryption, I mean, it doesn't have to always be verification. You're saying the man in the middle even means that encryption is no good?

Steve: Well, it means that you can't - you could have encryption, but you couldn't...

Leo: Verify that you were talking to this person you thought you were talking to.

Steve: Correct. And so the idea would be that you could say, okay, casual eavesdropping would be thwarted. Google would have caught nothing but pseudorandom noise.

Leo: But your ISP could still spy on you by replacing the cert.

Steve: Exactly.

Leo: I see.

Steve: It's analogous to what we've seen corporations do, where they put their own cert in their employees' browsers...

Leo: Or Opera, which is what Opera does with Opera Mini.

Steve: The Mini, exactly.

Leo: And so at that point you have, yeah, you've got encrypted traffic; but whoever is on the other end may not be the person you think it is. And they, of course, are decrypting because they have the other key.

Steve: Well, the way to say it is you have encryption, but no privacy. You have no guarantee of privacy.

Leo: Right, right. Google is now offering, I think this is very interesting, HTTPS search.

Steve: Yes.

Leo: So...

Steve: So what that means is that it's no longer - so the things you search on and the links you click on are no longer eavesdroppable.

Leo: Casually. But an ISP could still break it.

Steve: Well, and Google has it all.

Leo: Yeah, but, I mean...

Steve: Nobody else got it, but Google...

Leo: Google, obviously, if the search is to work, Google needs to know what you're searching for. You can't hide the search from Google. But you can't even hide the search from your ISP. People always say, oh, well, how could you - if you don't trust Facebook, how can you trust Google? And I always say, well, the person you really are trusting is your ISP, who sees everything.

Steve: Well, now, your ISP would not see your search terms unless...

Leo: Unless they broke the cert, did that man in the middle with the cert.

Steve: But they can't.

Leo: Oh, they can't.

Steve: Yeah, the ISP is unable to unless you've agreed, you've implicitly agreed to allow that by accepting a root certificate from them.

Leo: You could verify that it wasn't Google then.

Steve: Correct.

Leo: I mean, if you checked, you would say, oh, it's not Google.

Steve: Yes.

Leo: In the same way that, if you use Opera Mini, and you use the HTTPS search in Opera Mini, yes, Opera Mini is intercepting it, but the cert won't say Google, it'll say Opera.

Steve: Right. Now, what your ISP would see is the links you click on. So they wouldn't see your Google search request, not the page that Google returned. But when you then clicked on links, then unless those were SSL links, well, they wouldn't see the content, but your ISP would know where you were going.

Leo: They have to.

Steve: That's, remember that that's not encryptable, where you're going. Your computer makes DNS requests saying what's the IP for this server. And the IPs are to known destinations. So an ISP, even if the world were SSL, they would still know who you were and where you went. They just wouldn't know what you said.

Leo: It's very interesting stuff, isn't it.

Steve: It is.

Leo: Yeah. Question 2. Actually 3. No, 2. Gary Robinson in, now, this is a good one, Magherafelt, Ireland, asks a question: What happens after arbitrary code execution? Hey, Steve and Leo. Thanks for the great show in Security Now!, especially the ground-up computer principle series. I've been listening for just over a year now and have finally caught up on all 250+ episodes. Leo's right, I'd much rather listen to podcasts during my hour-and-a-half daily drive than the same boring thing on radio. It's true. That's our plan, anyway, our evil plan.

I've a question about what happens after a bad guy has found a vulnerability in an application and gets that arbitrary code to run. Based on your descriptions of this subject, bad guy uses some buffer overflow or some other vulnerability to get the arbitrary code into memory, causes the program counter to jump to that arbitrary code instead of returning to the previous function, or however else they've corrupted the program counter. When the bad guy's arbitrary code finishes, does the application crash? Is the bad guy smart enough to populate the arbitrary code with the correct return address so the application continues as normal? If the app will always crash after arbitrary code execution, isn't that a good indicator for us to know something bad may have just happened?

I know it could be hard to tell this application crash apart from the other standard common application crashes, but might be one way you could kind of be aware that something may have gone wrong, and we should run some diagnostic tool or virus checker before going to that banking site. I would be delighted to know what you think on this. Please keep up the good work on Security Now!. Gary.

Steve: I thought it was a great question because we've absolutely not even once discussed that.

Leo: We've talked about the mechanics of it, but not what happens afterwards.

Steve: Yeah, exactly. And the answer is, we don't know.

Leo: Well, couldn't they just push the return code on the stack?

Steve: Precisely. I love the fact that in his question he was talking about the program counter and setting it to something. And you're exactly right, Leo. It may very well be that the attack could look like a subroutine. In which case, if it was clever, I mean, if it deliberately wanted not to crash the application, it could push the current program counter on the stack, immediately push any registers it was going to modify on the stack, do whatever nefarious things it wants to do and then, just like a subroutine, pop the registers off the stack that had been modified and do a return instruction, which will continue just like nothing happened.

Leo: In fact, exactly how a subroutine works.

Steve: That's a subroutine. Now, in practice, it's more often the case that whatever function was trying to execute fails. That may be the whole app crashing, as Gary suggests. Or it may be that, like, edit/copy doesn't work. That's a bad example because edit/copy often doesn't work for other reasons. But it might be that what you try to do fails, and you kind of think, oh, well, I wonder why that was. Maybe it's not feeling good today.

Leo: We'll never know.

Steve: We'll never know. So there isn't a definitive answer because three things could happen: nothing at all, the application runs, meanwhile something bad happened in the background and you never noticed; or part of the application no longer works, but the rest of the application manages to continue limping along and sort of doesn't need to be restarted; or the application completely just crashes. It disappears from the screen, it locks up, something bad happens. And again, I got a kick out of him saying, but, you know, that happens all the time anyway, so would we really know. I would say more likely, from what I've seen, it's more common that the application does die after having achieved the hacker's goal. The hacker is generally much less concerned about a smooth exit than they are about getting their stuff to run, figuring, exactly as most of us would, oh, well, it just crashed.

Leo: Yeah, crash.

Steve: I mean, it's funny, I've sometimes spent hours working in a graphics editor on something, and then thought, oh, goodness, I haven't saved. Then I'll quickly save my work because, similarly, I've spent hours working on some graphic stuff, and then it just disappears from the screen. It's like, [groan], why didn't I, you know, save it.

Leo: Right.

Steve: So both things happen.

Leo: And I believe, correct me if I'm wrong, but this special code only has to execute once. It executes to install the trojan horse, which will then continue to execute normally without crashes. So it's not like you're going to crash all the time. You're going to crash once when the bad guy gets the code injected. And after that the trojan will run.

Steve: Correct. For example, it would establish a connection to a remote server, which it turns out is very simple to do, just a few instructions because Microsoft in the case of Windows provides an API for that. Then it would download a block of code which allows it to get much more of its own code into your machine. And that code might - just might be another process. It would spawn another process with that code in it, which it would then run. And none of that takes up that much space. I looked at shell, as it's called, shell code, which is this kind of stuff that does this. And it's, you know, it's written in assembly language, and very tight, and doesn't take up much space. But by the time the app crashes, the other thing is now running in your system. It then tends to be a bootstrap to go and get much more code from the remote server, and it just starts shuttling stuff into your computer in the background while you're thinking, huh, I wonder why my word processor just died. I'll just fire it up again and hope I saved a copy recently.

Leo: Wow. Question 3 from KD Martin in Dallas, Texas. He spends a lot of time gazing at the stars. Subject: Tau Ceti. The correct pronunciation of this star is "tau see-tie." I say set-tee.

Steve: Yes, I do, too.

Leo: See-tie. Okay. It really hurts my ears every time you say "set-tee." Okay, sorry, didn't mean to hurt your ears. Credentials: I'm a professional astronomer, member of the American Astronomical Society, big sci-fi fan with 10^3 - that's a hundred books, right? Oh, no, a thousand books - since the early 1950s to today. I presume he means reading, not writing. I like your recommendations. I'd like to hear an entire episode on assembly language, in fact, its evolution, its use today. You and I are the only ones I know who use it. I sure enjoy your podcast. I've hear every episode ever made. You and Leo do a great job. Tau Ceti.

Steve: That's going to be so difficult for me, but I wanted to let our listeners know. I have always pronounced it "tau set-tee."

Leo: Why did that come up? Did we mention Tau Ceti?

Steve: Everyone pronounces it "tau set-tee." I mean, I think Jerry Pournelle pronounces it "tau set-tee." And I guess we're all wrong.

Leo: It's the closest sun-like star to us; right? So...

Steve: Yeah, so it's a frequent target of science fiction. I mean, that's where you want to send your probe, right, to somewhere close, not somewhere [indiscernible]...

Leo: That's where they're coming from.

Steve: ...chance to get to.

Leo: And so that's where they're coming from.

Steve: But it's "tau see-tie," phonetically s-e-e hyphen t-i-e. Ceti. So...

Leo: Ceti. Just remember, when you see Thai food, you will love it. You will eat it. How interesting.

Steve: Yeah.

Leo: It must have been somebody's name or something. I will look it up. I will Wikipedia it.

Steve: I know you will.

Leo: Thank you, KD, for correcting us. We always want to say things correctly. I'm listening to a book, an audio book from Audible right now. And there's four mispronounced words, that's all, in the book. But it bugs the hell out of me. I don't like to - you know? And it just - and I listened to a reading of one of my favorite all-time books, George Gilder's "Microcosm," which really explains everything that's happening in the technosphere right now. And the guy who reads it does a great job except he says, instead of "kludge" (klooj), he says "kludge" (kludj). Oooh.

Steve: Yup.

Leo: And there's a lot of kludging in this book.

Steve: A lot of kludgery.

Leo: So I completely understand, KD. If you know the right pronunciation, and we keep saying it wrong with some authority, that's annoying.

Steve: [Indiscernible].

Leo: Oh, yeah, Tau Ceti, of course. "Tau see-tie."

Steve: Went there for lunch.

Leo: All right, thank you, KD. Lance Reichert in Backwater, New York wonders about building the Internet. When you address building the 'Net - which you're going to do in our next fundamentals...

Steve: Next big series.

Leo: There's one aspect of routing - by the way, for our Australian and English users, we're talking about "rooting" - that I hope you'll cover. See, they say "rooters," and we say "routers."

Steve: Oh.

Leo: How routers/rooters choose the path. This is where pronunciation can really bite you. I have a masters in CompSci, and I had to study many aspects of the 'Net, but I never, even though I have a masters, understood the following concept: Suppose I am a "rooter" on the 'Net, and I've just received a packet not addressed to any of my hosts. If the destination of that packet is far enough away that it's not in my routing table, or "rooting" table, how do I decide which of my neighbor "rooters" to pass it to? Or routers.

Steve: Okay, we're going to standardize on the pronunciation.

Leo: Am I driving you crazy? Let's say routers.

Steve: I think - oh, please, please.

Leo: They'll just think we're quaint Americans, mispronouncing it.

Steve: Besides, he's in Backwater, New York.

Leo: So he probably says routers.

Steve: I think it's routers, yeah. I love the question. We will absolutely cover it. And I will tease our listeners by saying that there's something known as "longest prefix match," which is the way routers determine where to send the packet when they're not sure. It's the way of getting - it's sort of like closest match, or best match, longest prefix match. And we'll be covering it in detail in the future.

Leo: It's such a great topic. I really look forward to this. I just love it. It's like all the other topics in this series where really smart people put their heads to a really thorny problem and came up with an elegant...

Steve: And Leo, it's funny, you just hit it. I was going to say that - and I'll probably say it again - unfortunately, our listeners are going to get a little annoyed with me just being ga-ga-goo-goo over the phenomenal design of what was originally created. Yes, it's not perfect. Or that should be no, it's not perfect. Anyway, it's not perfect. It's got problems. I mean, we know denial of service attacks and spoofing and all this other stuff. But look at what this thing has done. Look at how it's grown. Look how it's survived. Nothing that we have has scaled the way the Internet has from its original design. I mean, it is phenomenal. And I know why it works the way it does. And I get it. I've spent a lot of time in the last decade really playing with this stuff. So we're going to have a great series. And again, I believe our listeners will come away saying, wow, I understand all of it now.

Leo: Yeah. There's a wonderful book on the Wizards of the Internet that was written by Katie, oh, I can't remember her name. It's just a great book on the history of the Internet. It's not Bob Metcalf. He did Ethernet.

Steve: He was Ethernet at Xerox, yes.

Leo: It's those original guys at BBN who did all this. I'll find the name of the book in a second. But we've got another question. Chad Masters, Leavenworth, Indiana. He says the iPad ain't instant-on, Steve. It ain't instant-on. I've heard you mention on several episodes now that the iPad is instant-on. Hey, instant-on means a device can be powered on from a non-powered state and not have to boot an OS before it is ready to surf the 'Net or play a movie, et cetera. I can understand how you'd think the iPad is instant on. You press the power switch and, boom, there it is. However, the iPad in this instance isn't off, it's coming out of standby and not a powered-off situation. The iPad never really turns itself off completely without either, A, the battery dying; or, B, you pressing and holding the power switch for more than three seconds. And then you slide the switch to power off button, and that switches the entire unit off. Now it has to boot when you turn it on, and that takes - it takes about a minute, or no, about half a minute to do in mine.

Now, I will contend that for most uses the device is instant-on. However, it is not an instant-on device in the truest definition. Saying it is, I believe, is disingenuous - no, come on - and perhaps merely an overstatement on your part. Could you please correct yourself on the air so as not to mislead your listeners? No, he's being a little picky.

Steve: I stand corrected.

Leo: I'm just powering up now. I'll give you - we'll let it - we'll watch it happen.

Steve: I do know that. And I mentioned these two recent blog postings of mine. The first one was "The Obvious Genius of iPad." The second one is "Pads ARE Next." And in those I explicitly talk about...

Leo: There, now it's on.

Steve: ...coming out of standby quickly. So, yes, I know that they're not instant-on. For me, okay, what, "instant use" I guess is a more correct term.

Leo: Well, here's the point. You don't ever switch it off.

Steve: Right.

Leo: So from the purely practical point of view of the user picking it up and using it, it's instant-on. It is not technically instant-on. But you don't switch it off. I mean, when do you switch it off?

Steve: It's hard, it's hard to switch it off. As he said, you've got to hold the power button for three seconds. Then you get a scary-looking red slider that says, oh, push me at your own - slide me at your own risk. And in fact I became quite adept at this with that first 3G iPad I had, remember, that was locking up all the time. And it was you who said, unh-unh, Steve, that should never do that. The good news is the replacement has never misbehaved, not once. Absolutely never. So it is definitely the case that some of them were a little glitchy coming out of the gate. But the replacement has behaved itself perfectly, so.

Leo: That's kind of part of the reason I do the radio show is because people don't know what normal behavior is necessarily. So sometimes just having a reality check, like is it supposed to do this, is valuable. And then you say, no, it's not, take it in. Because it wasn't, and it's fixed.

Steve: Yeah, absolutely.

Leo: Molly Wood has a great phrase. She calls it the "Literal 'Net." And she said it drives her crazy. Every once in a while she'll hear from somebody who's very literal minded. Because we, you know, we geeks are. Engineers are literal minded. It's this is the fact, not that. That's, you know, something else. So the fact is, no, it's not an instant-on device. You're absolutely right.

Steve: Yes. And, I mean, I absolutely can see Chad saying, wait a minute, do you understand what you're saying? It's like, yes.

Leo: I don't think it's disingenuous. I think what we're saying is, in practice, as users use it, it turns itself on the minute you need it. Oh, I'm sorry, I said "minute." The second you need it.

Steve: And for what it's worth, it does take, like, a minute to come out of - to do a full cold boot. You sit there looking at the little silver apple for, oh, feels like about 60 seconds to me. It takes a while to get going. Which is fine because I never do that.

Leo: You never do it. By the way, it's Katie Hafner, and the book is called "Where Wizards Stay Up Late: The Origins of the Internet." Highly recommended. It is still in print and available on Amazon. If you want to prepare for next week's lecture on the beginnings of the Internet, it is really - starts with Lickleiter and goes on from there, and it's really fantastic. "Where Wizards Stay Up Late," I loved it.

Moving along to our next question, Ray Siposs in Irvine, California wonders about emptying trash from an encrypted folder. Steve, I'm a Mac user, and I've listened to your show since the beginning, and I have learned much. Thank you for doing it. I purchased SpinRite several months ago though as of yet I have not had any need for it. I like that. Proactive purchasing. Consider my purchase a sign of support for the work you and Leo do. I hope a Mac version will one day be made available. Don't hold your breath. Next question: If one uses TrueCrypt, or Mac's Disc-Utility encryption application, to make a container for holding files, what happens to the files when you throw them out? In other words, do I need to do a "secure delete" of those files - oh, this is a good question.

Steve: It's a great question.

Leo: Or are they already encrypted, by being held in the encrypted folder, and a normal delete will suffice as they are already unreadable? I have never been able to find information on deleting files from an encrypted container, and I'd like to know. Thanks much. By the way, if I'm ever in the UC Irvine area Starbucks, I shall buy you a cup. Cheers, Ray. That's great.

Steve: Now, it's a great question. And it's a tricky question. If you delete a file from an encrypted container which does not have a trash can, that is, where you've configured that drive for non-undelete, then it's a safe, secure undelete. And I would recommend that that is how people would set up their system. That is, the problem is, if you have a container which is not a drive, but for example looks like an encrypted folder, and you delete a file from that, then it's moved into an undelete, or into a deleted location so that - which, you know, is called the trash can, which you can optionally empty. But in the act of it being pulled out of the encrypted folder, it is decrypted.

So, for example, if you moved it to your desktop, then deleted it, well, the bits are unencrypted while they're on the desktop, so they're marked as - that chunk of the disk is marked as available, but it's been unencrypted prior to those bits being marked as available. If you delete them in place, then they're not getting unencrypted before being deleted. So it's a great question, and it really does require that you be careful.

So the bottom line is, use an encryption system, like TrueCrypt does, that creates a drive. And in Windows at least you're able to specify which drives have undelete capability. You would want to disable undelete on your TrueCrypt drives so that, when you delete something from there, it deletes it in place rather than - now, okay. Also in Windows normally you've got a trash can per drive. So in Windows you could - the trash can would be encrypted also, so it's safer. I just don't know what the status is on the Mac. Have you looked at it closely, Leo? Like is there one trash can, or is it a trash can per drive on the Mac?

Leo: The Mac works just like Windows does, I believe. Now, I haven't looked at it in the last version of OS X. But I believe there's a hidden trash file in each directory, just like Windows does. And the Mac has a secure delete, so you might as well just use it.

Steve: Right.

Leo: But...

Steve: And secure delete, is it writing over the file?

Leo: Yes. It has a multiple-write secure delete. And Windows you can empty directly; right? There's a shift-delete is instant. But I don't think Mac has an instant delete.

Steve: Oh, yes, right, a non-recoverable delete. And then you would either want to use that or just configure your TrueCrypt drives not to be undeletable, in which case it would mark that space in the TrueCrypt drive as available, leaving it encrypted, and you'd have a safe, secure delete.

Leo: Right, right. But there is on the Mac a secure delete. So I would just use that.

Steve: Yup.

Leo: That's a great question. Boy, I'd never even thought of that. Because you're unencrypting as soon as you're removing it from the encrypted folder, so...

Steve: Yes. And so if it goes anywhere else, like into...

Leo: Now it's clear text.

Steve: Exactly.

Leo: I don't think - I'm trying to think if shift-delete is an instant delete on the Mac. I don't think it is. I think it's only Windows and Linux. Question 7 - but we will have to test and return with our answer later.

Ben Rexworthy in Bedford, U.K. asks for SpinRite licensing

clarification: Steve, I've been an avid listener of your podcasts for many years now. I've often heard testimonials of SpinRite from listeners saying how they've saved the day, how you've saved the day with relatives and friends - just like our emailer earlier today, using SpinRite. However, when I looked on your licensing option it clearly states a single license is for "individual end users on one or more of their personally owned machines." It sounds like you are endorsing the use of the product outside of the personal licensing guidelines you have written, my friend.

Steve: Oops.

Leo: [Laughing] The Literal 'Net is back. I'm not going to use it for commercial use, and I don't really want to buy four copies of the software if a friend needs help. I do understand the need to protect your intellectual property, and I wouldn't want to break any copyright laws. This is why I'm writing to ask, he says. I think there will be others who are also concerned they may be breaking your licensing agreement, and I think it would be good for you to clarify, possibly allowing for two distinct categories, maybe commercial and non-commercial - in addition to commercial and non-commercial use. Anyhow, many thanks for the wonderful work you do in educating the public. I've used you as a reference many times. Kind regards, Ben. See, Steve, you're a nice guy.

Steve: Well, and I'm...

Leo: That's the problem.

Steve: Well, I think I'm a practical guy. And one of the things that's always irked me is when you buy a disk utility, and it says you can use it on one drive. It's like, oh, come on. Who's going to buy one of these for every drive they own? And so I immediately - we never had that policy. I said, okay, look. If a person buys it, they can use it on everything they own. If a corporation buys it, I ask them to buy four copies, and then they can use it on all the computers the corporation owns, a so-called "site license." For individuals, though, I mean, yes, I would just ask you to use your best judgment. I mean, we're basing this on trust anyway because SpinRite has no activation nonsense or copy protection or installation lock or any of that. I hate all that stuff. I always wonder, Leo, like when I use a program where I have to activate it, what happens when that company goes out of business?

Leo: Right. Well, and it's happened.

Steve: Yes.

Leo: It's happened. Or activation servers are down, suddenly you've got something you can't use. That pisses the hell out of me.

Steve: This is wrong. Especially for a product like SpinRite, where it's an emergency recovery tool. So anyway, there's none of that. And so I just - I trust my users rather than not trust them. And I would say, if someone you care about is in trouble, fix their problem. Use SpinRite to fix their problem with my blessing. And if they're destitute and can't buy their own copy, fine. Then I didn't lose a sale anyway, and the world is a better place because SpinRite was able to help them. Maybe they'll refer someone to SpinRite who can buy a copy. So...

Leo: I think that's really sensible. I'm sure a lawyer listening would say...

Steve: Oh, he'd be rolling over in his grave.

Leo: ...oh, you're just - you're ruining the whole purpose of the license. But anyway, I think that's the sensible - that's like a - you have a what's called a reasonable human being licensing point of view. It's just not done in the industry.

Steve: And so, yeah. So for our listeners who have been neat enough to buy SpinRite, I thank them all the time. It does make it possible for me to dream about getting going on CryptoLink, which I intend to do, and continue supporting SpinRite. So, yeah. You just use your best judgment. I appreciate when people say, hey, I know that I've sold copies of SpinRite because I've fixed other people's computers, and they've been so impressed with it, they bought their own. There's nothing better than word-of-mouth marketing. I couldn't ask for anything better than that. And the flipside is, hey, if you fix someone's machine, and they don't buy one, well, fine. I say it's all working out.

Leo: Steve, some great questions. Of course, as always, great answers. People can find this show online. You can download it. In fact, if you go to TWiT.tv/sn, this is kind of our standard for all of our shows. We have a list there of all the RSS feeds because there's at least three now. There's an audio version; there's a large video and a small video version. And you can subscribe to those, and it will work on almost any device that can subscribe to podcasts, podcast feeds.

Steve goes us one better. You can go to GRC.com/securitynow, and he has not only the 64KB version, but he's got a really squoze down 16KB version for those of you who are bandwidth impaired, or you're on an iPad and you're trying to keep under the 250MB limit. Couple of podcasts would put you over that. So GRC.com/securitynow. He also has transcriptions, which is really nice to have the written version of this. And they're human-transcribed by a real human with a brain, Elaine. So they're actually good transcripts. He also has all the show notes and every show going back 251 episodes.

Steve: And I have to give a shout-out to this new daily news podcast of yours, Leo, for our listeners of Security Now!. I was talking to you about it before we began recording, so it bears repeating. It's fantastic.

Leo: Thank you. It's Tom Merritt. He calls it Tech News Today. Thank you because it's coming up this afternoon and every afternoon, 5:30 Eastern, 2:30 Pacific, Monday through Friday. That's 2130 UTC. Tuesday, Wednesday, Thursday Tom's co-host will be the great Becky Worley, who was my first producer at TechTV for Screensavers and Call For Help and is ABC's tech reporter, and Good Morning

America. And she's just great. So Tom and Becky every weekday. Sarah Lane will join them. We'll have other co-hosts. Tom of course did the great Buzz Out Loud on CNET. And he's really brought his talent, his brains, his enthusiasm, and his skills to TWiT. And we're so happy to have him.

Steve: Well, and it's just, it's professional and polished and interesting. I mean, these are smart people who have a real professional feel to them. When I started watching it - you were replaying yesterday's, I guess, as we were getting set up. And I thought, I mean, immediately I thought, whoa, this is good.

Leo: This is better than Leo's usual crap.

Steve: This is way good.

Leo: Well, thank you. I'm really thrilled that we were able to get Tom to join us. It is No. 1 in podcasts right now, I'm seeing. That's pretty...

Steve: On iTunes.

Leo: On iTunes. That is really good news. We're very happy about that. And you can - that show is TNT, Tech News Today. So you can also subscribe to that at the same system, which is TWiT.tv/tnt. And there is audio and video, and you can get that right away.

Steve: And that's a variation on my slogan of Trust No Turtles.

Leo: Trust No Turtles.

Steve: Yeah.

Leo: Tech News Today is No. 1 with Tom Merritt. It's No. 4 for the video on the podcasts. So we're really, really pleased. Tom's done a great job, and it's a great show. And please watch live at live.twit.tv, or subscribe so you can hear it every day. And it will get you off to - it complements TWiT perfectly. TWiT is really us sitting around and talking about what it means. But if you want to know what happened every day and get the instant analysis, get the instant information, Tom does. There's nobody better than Tom Merritt. Tech News Today, TNT, on TWiT.tv. Thank you so much for reminding me to plug it. I'm not good at plugging. Steve, we'll see you next week. If people have questions for our next Q&A, which will be two episodes hence, please go to GRC.com/feedback and ask that question.

Steve: And I will remind our listeners that I'm now tweeting up a storm. It's GibsonResearch if you want just GRC updates and news and nothing else. SGgrc is my personal Twitter account. And I'm also talking about pad stuff a lot over on SGpad. So you can subscribe to all or one or two or whatever you like.

Leo: That's great. It's really fun to be able to follow Steve Gibson around the clock.

Steve: And of course the blog, steve.grc.com.

Leo: We'll see you next week.

Steve: Thanks, Leo.

Leo: On Security Now!.