# SECURITY NOW!

Transcript of Episode #138

## Listener Feedback Q&A #38

**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-138.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-138-lq.mp3

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

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

This is Security Now! with Steve Gibson, Episode 138 for April 3, 2008: Listener Feedback #38. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!, everybody's favorite security podcast. Is mine, anyway, because it stars the great, the one, the only Steve Gibson, the man who discovered spyware. What? What are you laughing at?

**Steve Gibson:** It's definitely my favorite security podcast.

**Leo:** Yeah, well, it's my only security podcast. That's why I'd have to like it. But I would anyway. Steve is an expert at making stuff intelligible. But, and I'm proud of this, we never dumb it down. And that's one of the reasons we have written transcripts and, you know...

**Steve:** No, and in fact I'm a real believer that if something is - if someone understands something and is able to communicate it, it really does not need to be made simple. I mean, I think last week we talked about static and dynamic RAM. And I would imagine that everybody listening kind of enjoyed understanding, if they didn't already know, what is static about static RAM and what is dynamic about dynamic RAM and how that stuff works. And there's no need to dumb it down if it's explained correctly.

**Leo:** I've made my living assuming people are intelligent. And I prefer to do it that way. A lot of broadcasting doesn't assume it. It assumes the worst. I like to assume the best. And, you know, it's self-selecting. I mean, if you listen to this show you're obviously a smart person. And but that's fine. I'm really happy just talking to people who get it and want to get it and care enough to figure it out. And I know this is a challenge. It is certainly the most challenging show we do on the network. But that's part of the fun of it. Your brain grows when you listen.

We are going to talk today, actually we're going to do listener feedback. We're going to answer your questions, so it means we'll talk about at least a dozen different topics, which will be a lot of fun. So do you want to talk about the Paper Enigma Machine first? Because this is so cool.

**Steve:** Yeah, just very quick, Leo. I just thought it would - I ran across it. Bruce Schneier was blogging about it this week. And I thought, oh, that's kind of interesting. So I followed the link, and it's to a really interesting, simple, zero-cost implementation of sort of a reduced-capability but still functional Enigma machine, the Enigma cipher machine used by Germany during World War II.

**Leo:** The story of Enigma is really a significant story.

**Steve:** Right. And so it's - this is just something that you can - they have a PDF you can download which you then print onto card stock. And using scissors and glue and cut some slots and make some strips, you're able to really get a sense for how it works.

**Leo:** So I remember it was - was it Alan Turing who broke the Enigma machine?

**Steve:** Yes, Turing working at, I think it was...

**Leo:** Bletchley, yeah.

**Steve:** Bletchley. There's always an L in there, I'm not sure where it goes. Bletchley Labs, yes.

**Leo:** Yeah, in Britain. And this was, I mean, the Germans were able to use Enigma to really harass British shipping with their submarines. Once it was cracked, it may have been one of the keys to winning World War II. It was significant, significant. And people never thought they'd crack it. It's so cool that you can make one. It was - they were beautiful. They were wooden boxes with gears and cogs and a typewriter on it, I mean, it was really quite a clever, interesting device.

**Steve:** Well, so what people can do is, you and I have links to it on our respective show notes. You can also just simply Google "paper enigma machine." The first link there takes you right to this page. It's also worth noting that there's a link in about the middle of the top of that page to an Enigma simulator. It's a software simulator that runs under Windows or under Wine under Linux, which is a complete emulation of a whole bunch of different Enigma machines. It was beautifully put together. So if anyone is sort of curious about this and wants to play with it, either just print out paper and get a real, intuitive sense, I mean, a real understanding of how that works.

**Leo:** Yeah, and I notice it's math classes that do it. And I think that that's really one of the neat things, to bring both math and history to life. I just think it's a really neat solution. So, yeah, very cool. So today Q&A, yes?

**Steve:** Q&A, yes. I don't have any errata nor security information since we're recording this on the heels of last week's episode because as people are listening to this you're in Australia taking pictures of things.

**Leo:** I'm in Tasmania, mate. I'm taking pictures of the Tasmanian devil and the Tasmanian tiger.

**Steve:** In my eternal search for new and different SpinRite data recovery stories, I had something wacky that I thought I would share with our listeners. Steve Hall wrote with a subject, "Thanks to SpinRite, my daughter can read better."

**Leo:** What?

**Steve:** He says, "Hi, Steve. I just wanted to say thank you for making such a fine program. Recently my father gave me a hand-me-down computer since he was replacing it. The reason he was replacing it is due to the fact that during an act of Windows-induced frustration" - okay, I kid you not - "during an act of Windows-induced frustration he decided to give the computer some flying lessons."

**Leo:** Oh, I can believe that.

**Steve:** "From the second floor to the first floor..."

**Leo:** Oh, no, he threw it out the window? Or downstairs.

**Steve:** I guess he - I think downstairs because there's a reference here to his Pergo flooring.

**Leo:** Oh, man.

**Steve:** "From the second floor to the first floor of his house. Well, after a new motherboard and some replacement sections of his Pergo floor, I had it up and running in no time, keeping the old original hard drive." Which, okay, I don't think I would ever use a machine whose hard drive had gone down a story. But he says, "I kept the Windows XP that was running on it and gave the computer to my four-year-old daughter to run her Hooked on Phonics game. She loves it and uses it daily. Until it stopped booting up." Not surprisingly, I mean, the drive probably had loose bits floating around inside.

**Leo:** Oh, can you imagine what happened to the drive, yeah. I mean, that's the worst thing you can do to a drive, right, is impact.

**Steve:** Oh, yes, yes, yes. You're literally - you're bouncing the heads on the surface. Now, it's way worse if it's spinning. So presumably Dad unplugged the computer during his fit of pique with it, or his peak of pique, the peak of his pique, and before throwing it downstairs. So the platter - the heads would have pulled off the platters to go into the center near the spindle where as the platters vibrate there's less vibration in the center where the drive is anchored. Normally that's what heads do. They used to get pulled off of the platters completely and parked away from the disk. But now they just slide into the center where they're safe. And they generally - there's, like, an electromechanical mechanism. A little hook comes out that locks...

**Leo:** Oh, I had no idea. They park it.

**Steve:** Yeah, they park in the center. And the reason they go into the center, not only do you have much less motion if the disks are vibrating because they're anchored in the center, but also it helps with the stiction problem. When the motor starts up, naturally the heads, which are resting on the surface, they can be a little sticky. And so you'd like to have them in the center where they have less mechanical advantage in preventing the disk from spinning than if they were resting out on the outer edge, where they have a very strong mechanical advantage to keep the disk from spinning. So all of that goes on. Anyway, so...

**Leo:** I had no idea. And it goes on in milliseconds; right?

**Steve:** Yes. Oh, yeah. The moment you power down, the heads are snapped into the center and rest there until you power back up again. And he says - so he says, "Suddenly it no longer booted up" - it's like, yeah, no kidding - "but instead displayed a message that it could no longer locate some key Windows files." Like I said, those Windows files were off on the edge of the drive somewhere. He says, "I also know that the drivers for the very old Netgear wireless card are nearly impossible to locate now. Being a loyal Security Now! listener, I was pretty sure SpinRite would fix it." Okay, he's a faithful Security Now!...

**Leo:** Wow, that's great.

**Steve:** ...listener. "So I decided to bite the bullet and purchase me a copy. After 12 hours of clunking away and many recovered sectors, SpinRite recovered the computer..."

**Leo:** What?

**Steve:** "...and it once again boots up."

**Leo:** The computer that went down two stories, it recovered.

**Steve:** Yeah.

**Leo:** Wow.

**Steve:** He says, "I certainly am a satisfied customer and will always recommend SpinRite to many happy daughters everywhere."

**Leo:** Now, here's the question. Do you recommend this?

**Steve:** No.

**Leo:** See, he's an honest guy. I love this about you. There are a lot of people'd say, oh, yes, absolutely, no matter what, SpinRite. But once a drive has gone down the stairs, probably not worth trying to recover it.

**Steve:** No, I mean, that kind of physical damage is, I mean, I'm glad that SpinRite was able to recover.

**Leo:** Get your data off it now.

**Steve:** I've seen pictures of literally barbecued hard drives that survived fires that our listeners tell us SpinRite was able to get the drive back up again enough that they were able to copy data off it. I mean, it looked like it had been in a charcoal, bottom of a charcoal pit. But...

**Leo:** But a new drive is cheap. Copy the data off. Don't trust that drive now.

**Steve:** Yeah. Yeah. But, I mean, he's been able to keep it going, so what the hell.

**Leo:** I'm impressed. I am impressed. All right. Let's see, shall we get to our questions?

**Steve:** You betcha.

**Leo:** We'll start with number one. We've got 12 good 'uns. Fred Zanegood in Orlando, Florida, he wants a free audible podcast. Well, I don't blame you. Actually there are free - if you go to Audible.com, this is not an ad for Audible, I just want to mention they do have free stuff. In fact, they do a lot of pro bono stuff, things like debates, speeches, state of the union, that kind of thing. I haven't seen a lot this year. I wonder if they stopped doing that. But they always have in the past done a lot of pro bono. So there are a lot of free things on Audible.com. But, he says, just thought you'd like to know that the AudiblePodcast.com/securitynow URL - which we use all the time - doesn't work, he says. Huh? I thought it may have been an OpenDNS problem, but after putting it on my whitelist it still doesn't work. Have you guys tried it or heard of others experiencing similar problems with the URL? I'm using Firefox. Love the show. Love SpinRite. Thanks, Leo. Thanks, Steve. Well, it worked for me. Does it work for you, Steve?

**Steve:** Works for me perfectly. First thing I did was put it in. I did notice, however, that it immediately jumps around a little bit. There's...

**Leo:** Well, don't say the other URL. Here's what's going on. They don't want people to go to the other URL. It does redirect. But the point is they're counting how many people go to Security Now!.

**Steve:** And that's a good thing. But it may be the redirection that is causing Fred the problem. You mention...

**Leo:** Well, let me tell Fred, first of all, that it doesn't matter. While we'd like it to be counted, they don't pay us by number of acquisitions or anything. So, I mean, it's not like we'll get less money. But we do, you know, we just want to - they want to know, and we want them to know, how many people come to them from each different show, that's all.

**Steve:** Exactly. So what happens is, it is doing a redirect, meaning when he puts that in, there's actually a website at AudiblePodcast.com which sees that he's trying to reference the page securitynow. It gives the browser back a new URL, called a redirect, which the browser then follows, all things being equal. However, there have been some shenanigans played in the past with redirection of a security nature, and there's sort of a - it sort of generally makes people feel, I mean, really security-conscious people feel a little uncomfortable. It's like, wait a minute. I put this URL in because I trust it. I don't want to be bounced somewhere else. And in fact we've talked about some sort of shady goings-on with redirection where for example links at PayPal are actually DoubleClick links which take you to DoubleClick and then redirect you back to PayPal.

**Leo:** Well, this all goes through Audible, I should tell you, it's not...

**Steve:** Yes, exactly, there's nothing shady going on there. But as a consequence of the fact that redirection of URLs has been abused in the past, and the fact that Fred mentions he's using Firefox, which tends to be a security-conscious browser, and that Firefox has all kinds of add-ons, it may just be his security.

**Leo:** Ah, blocking it.

**Steve:** Exactly. He may have redirects disabled. He may be using an add-on. He mentioned whitelisting it. I don't know if he was talking about whitelisting through OpenDNS because - and he says, "I thought it may have been an OpenDNS problem, but after putting it on my whitelist it still doesn't work." So that sounds like maybe something whitelisting externally. He may have to tell his browser that AudiblePodcast.com is an okay website and to allow redirections from it to the Audible URL that actually...

**Leo:** Yeah. You end up at Audible.com/podcasts, I think, something like that.

**Steve:** Right.

**Leo:** But, yeah, okay. I use redirects for the podcast URLs because - and the reason I use a redirect is because I may host the - so a podcast is an RSS feed. And I sometimes have in the past moved the RSS feed to different servers for various reasons, mostly because I want to be able to do that should a server go down or be over-expanded or whatever. So if you go to, for instance, the nominal URL for Security Now!, which is leo.am/podcasts/securitynow, it'll redirect you to an XML file. And the reason for the redirect is, again, so that I can - I have one URL that's always guaranteed good, and I can move you around, if I need to, to different locations for that XML file.

**Steve:** And I do, too.

**Leo:** So I should not do that?

**Steve:** Well, no, I do the same thing, for example, on the 64KB versions of Security Now!. We have a URL that looks like GRC. But when the user's browser fetches it, it redirects to you guys.

**Leo:** Right, and then which gets it from AOL.

**Steve:** Exactly.

**Leo:** So it's redirect redirect. And in fact that's how we count podcast downloads, we direct through Podtrac.com and then to the server, whether it's AOL or CacheFly that provides the bandwidth for the show.

**Steve:** Well, and interestingly, I was thinking about this question this morning. I also, when I was originally setting up GRC way back in the old dark days, the way our DNS was set up was with a wildcard in front of GRC.com. So anything dot GRC.com took you to the IP of GRC.com. So you could use www.GRC.com, just GRC.com, or literally anything. I mean, you could just make up something dot GRC.com. Which, you know, I thought, oh, isn't that cool. Well, I don't know how or why, but we, over the years, we accumulated so much, I mean, an unbelievable amount of debris dot GRC.com. And Google was, like, finding it. And if I Googled GRC.com I would see all this random, like, machine names dot GRC.com. So finally I got - I said, okay, this is ridiculous. So I have a redirect now, or I did for years, where anything dot GRC.com redirected you to www.GRC.com. And I think finally, after several years of, like, training the world not to use anything but the real names, I then shut off the wildcard. But so I've had - I make great use of redirects, as well. I mean, again, they never go anywhere spooky or suspicious. But they are very handy. I wish they hadn't been abused. But like everything else that's kind of cool and can be used for gray purposes, they were.

**Leo:** They're not going to go away. I mean, there's just a lot of reasons why you would have a redirect. And it's just, you know, it's just unfortunate, I guess.

**Steve:** It can cause problems, which is of course what caused Fred to write to us saying, hey, why can't I get to AudiblePodcast.com/securitynow?

**Leo:** Well, and I appreciate your trying, Fred. And it's okay if you just go to Audible.com. It's fine. We don't have to count every single person.

**Steve:** Well, I imagine Fred would like to know if his security settings in Firefox are causing redirects to break.

**Leo:** Or Norton Internet Security, McAfee, there are a lot of security programs doing that.

**Steve:** Anybody that is doing a filtering on his browser stuff.

**Leo:** Yeah, a lot of security programs do a proxy. And you go through them to get to the 'Net. And at that point who knows what's going on.

Rene van Belzen in the Netherlands is worried his drives may be getting too much sleep: I have a Mac, and recently bought a shareware utility called TinkerTool System - I use it, it's excellent, this is Leo saying that - developed by Marcel Bresink. In the Hard Drives tab of the System Setup there's a warning message: "Switching off the hard disks of desktop computers too often may reduce lifetime." All right. I'm trying to be green and save energy when I can, but I don't want to kill my hard drives prematurely, either. So what, Steve, in your expert opinion, is an appropriate period of inactivity to put my hard drives to sleep? How soon should they go to sleep? And this is true on Windows, too, you have that slider. 15 minutes? An hour? Never? What's the best for hard drive longevity?

**Steve:** I'll tell you, I never sleep mine. My feeling is that, I mean, I know in the old days it was when you powered up systems that hard drives failed. They were working the prior evening, everything was fine. You said okay, you know, I'm done. You turn off your computer, you come back in the morning, it won't boot.

**Leo:** Well, that's true of everything. That's true of light bulbs. They always blow out when you turn them on.

**Steve:** And that's exactly why, is that - well, in the case of light bulbs, there's an interesting phenomenon with them. And that is that the resistance of the filament is lower when it's cold than when it's hot. So there's an inrush current that is the reason light bulbs blow out when you turn them on, is they get more power than they're supposed to have during that first instant when the filament is really cold. There used to be an oscillator, in fact, I think it might have been a Wien bridge oscillator, I can't remember if that was the one, that actually used a light bulb to regulate the oscillator because of this weird characteristic that, as more current went through, the resistance went up, which limited the current. So it was, I mean, a cold light bulb is sort of a regulator all by itself as a consequence of that. But so anyway...

**Leo:** So it isn't the same for hard drives. But it is more stressful when the hard drive's spinning up.

**Steve:** Well, the other thing that goes on, given that you are changing - he's just talking about spinning down his hard drives. But turning the whole computer off, of course, causes it to cool down to room temperature, which may get low at night. Then when you turn it on you're heating it back up. So now you've got big thermal swings from hot to cold and hot to cold. I mean, I never turn my machines off, and I never spin my drives down. I'm sort of self-conscious about it. I've had drives last a long time just by leaving them going.

**Leo:** I'm changing all my settings right now.

**Steve:** I think they're happier that way.

**Leo:** They don't heat up, they don't cool down, they don't expand and contract. They're consistent. And, you know, you may not save power by switching them off and on because of all the extra power used to spin up.

**Steve:** Well, yeah, I mean, it is a function of what your duty cycle is of using a computer. If you're somebody who gets on for an hour in the evening to check email, do a little web surfing, and then you're sleeping at night and you're gone at work during the day, it's like I don't want to tell anybody to leave their machine on 24 hours a day if they're going to use it one hour a day. For me, I'm sleeping - the only time I'm not in front of my computer, Leo, is when I'm sleeping or at Starbucks. Otherwise I'm here.

**Leo:** And because he goes to Starbucks so often, he doesn't sleep much.

**Steve:** Exactly. Exactly. There's that caffeine effect.

**Leo:** But that's a good point. For power reasons it would be a good idea. In fact, I've seen statistics that said that if businesses turned off their computers at night when people went home, it would power hundreds of thousands of homes. I mean, it's a significant - when you think of millions of machines in use, it's a significant power saving.

**Steve:** It really is. And so what I tell people who are not massive computer users like you and I, who are literally using our computer when our eyes are open, I say, look, if you're going to use your computer again this day, probably better to leave it on. If you are done for the day, at whatever point you're done, shut it down. I mean, I don't. But my power bill demonstrates that.

**Leo:** I leave them - I guess I leave them on, come to think of it, I do leave them on. But I have had the drives being powered down. And you know what, I'm going to now turn that off on all the systems. You've got to balance greenness with the length of the drive. The other point, I guess, to make is that systems last a long time nowadays. We're not killing off our drives.

**Steve:** True, and hard drives are cheap. And SpinRite fixes them when they die, so what the heck.

**Leo:** Buy a copy of SpinRite, and then you can turn them off and on. Scott Hemmeter in nearby Orange, California is curious about IronKey's private TOR network offering: Hi, Steve. During the IronKey episode - what was that, that was 136? 135, I think - your guest explained how it could be used as a TOR network. If I recall from way back in Security Now! - when we did a whole thing on The Onion Router, TOR - you said that traditional TOR is anonymous but not secure. Did I understand correctly that the IronKey TOR network is both anonymous and secure? If so, could this be used as a VPN? I'm currently using HotSpotVPN as a VPN service. That's $10.88 a month. And HotSpotVPN slows my connection considerably. I'm looking for an alternative. Could IronKey be that solution? If it can, boy, it would certainly justify the cost of the IronKey. Is it secure and anonymous?

**Steve:** Well, let's review a little bit about TOR. TOR is a system that was designed for anonymity. And TOR is an acronym that stands for The Onion Router. And if anyone really wants to know everything there is to know about TOR, we did an episode which I really liked because we explained, I think, very clearly and carefully what this onion model is, what is the onion, and how it's possible for people's traffic to be routed or bounced from one onion router to the next with the design deliberately created so that no intermediate onion router knows anything about the traffic other than which router it got it from and which router it's going to give it to. The payload itself is encrypted. It cannot decrypt it.

It's not until it gets to the final onion router, after so many hops, however many you want to configure, that only the last router peels the final layer off of the onion, as it's called, gets inside there the crypto keys which no prior router is able to access, then decrypts the traffic and puts it out on the 'Net. So the goal is that no one monitoring that router is able to determine who generated the traffic. However, they are able, if they were monitoring that router, that final onion router where your traffic finally is emerging onto the Internet, if somebody were monitoring that router they would see your traffic. They would not be able to backtrack it one hop to the next in order to determine your identity. But at that point it's no longer encrypted.

Now, that's, however, exactly the same with any of these HotSpot services. HotSpot is a VPN, which Scott was talking about, where his traffic is encrypted from wherever he is to the HotSpot network. And at that point it is decrypted. It's taken out of the VPN SSL tunnel and, similarly, put onto the Internet in its natural form, in its unencrypted-by-the-VPN form. You might still be using an SSL connection, for example, to a remote website, in which case your end-to-end connection to a website is encrypted. So, for example, if you're using Gmail, we talked about this before, using https://mail.google.com, then all of your access to Gmail is maintained through an SSL channel.

Now, subsequent to our talking about The Onion Router network, there was some news about malicious TOR nodes, meaning that bad people were - or people of varying badness, maybe even state-run agencies, were creating TOR nodes and monitoring the traffic. Which is really not what you expect or want from a TOR node. You would like it to be run by a white hat, by somebody who is pro-anonymity who's offering a TOR node because they believe in the concept of supporting the anonymous use of the Internet.

So this is what IronKey is providing. IronKey has a private TOR network which they completely control. So unlike the public normal TOR network, which uses volunteer donated TOR nodes that no one is really vouching for, the IronKey guys have said, look, we like the idea, we're going to run our own TOR network, and we will allow IronKey users access to our TOR network. So the TOR client creates an encrypted, a securely encrypted SSL connection to the first TOR server. So very much like HotSpotVPN, your traffic is encrypted. Then it bounces around IronKey's own TOR servers to obscure the path that the traffic has taken, and then emerges from IronKey's final TOR node out onto the Internet.

So it is secure. The problem is, it tends to be lower performance. I can't vouch for the performance of IronKey's private TOR network. But I do know that TOR in general is a dramatic tradeoff between anonymity and performance. That is, you know, using TOR is a very sluggish process where you're trading performance for anonymity because your data is bouncing around among these servers. So the only thing I could suggest would be to give it a try, if you have an IronKey. It is absolutely secure, but it may not be giving you more performance than a regular HotSpotVPN service or something similar.

**Leo:** And the security is somewhat compromised by the fact that it's all through one company. I mean the anonymity. The advantage of TOR is it's a certain - it's whatever it is, 20 different, completely unconnected people hosting this. So it wouldn't take one subpoena to catch it.

**Steve:** That's a very good point.

**Leo:** So in some ways this really isn't a true TOR network because all they have to do is go to IronKey and say, who is it? And they say, well, okay, it's him.

**Steve:** That's a very good point.

**Leo:** So, okay. That answers the question. I need not go any further. Bryan Moore in Carlsbad, California - are there caves in Carlsbad? Carlsbad Caverns?

**Steve:** Yup.

**Leo:** That's what I thought.

**Steve:** Probably bats in the cave, too.

**Leo:** Actually as this airs I will be in Tasmania, where they have bats the size of foxes.

**Steve:** That's a big bat.

**Leo:** Scary. They have scary animals there. There's an ant that can jump two or three meters. And its bite is as bad as a bee sting. I don't know, maybe I'll stay home.

**Steve:** And I think they have really, like, serious tarantulas, as well.

**Leo:** Oh, yeah. Big, bad spiders. They have snakes, lots of 'em, many poisonous. Bryan Moore in Carlsbad, California, where the caves are, doesn't want to create Flash Trash: Dear Steve - this is a long question. I'm going to be reading. Let me get a drink. Okay. I listen to every Security Now! and love and recommend your show, but I will not buy an IronKey unless they make a variation of the product. He wants them to use a slowed-down password failure punishment method, not a shiny doorstop Flash Trash destruction. Let's explain.

**Steve:** Please do.

**Leo:** Please do. A few users might prefer Flash Trash, but many of us don't want e-waste or a shiny doorstop when someone else might try to sneak a peek at our data. He's talking about the fact that, if you try to break open the IronKey, it destroys itself; right?

**Steve:** Actually he's talking about the fact that if you...

**Leo:** Oh, if you fail the password.

**Steve:** Yes, yes..

**Leo:** So how many times did he say it's - 10 times or something? But you could change that. But 10 failed password attempts and you've got nothing. You've got a doorstop. He says: A few users might prefer this, but many of us don't want this. It seems far more highly probably for most of us than for someone to guess our password in a million tries. In other words, that you would not guess it in 10 tries. The possibility created by Flash Trash, where the USB key permanently self-destructs, requires that I maintain an accessible copy of my data in a secondary, possibly less secure backup. This weakens the whole concept. He points out Kingston also does this. Anyone doubting the truth of the severe warnings displayed might use up the counter. And then I wouldn't know until I needed to use it myself. Oh, he's got a point. Somebody tries to break in, tries it eight times and then says, oh, never mind. Now you've only got two chances. Even if they stop at "we really mean it" and I have one count to go, I might have two IronKeys, and I myself might need more than one try, or else I wipe out my own data, but only because of someone else's surreptitious attack and IronKey's mistaken use of permanent counters. So you get 10 tries lifetime. Is that right?

**Steve:** Oh, no, no. It's 10 tries, and then if you successfully authenticate within 10 tries, that resets the counter to zero for your next authentication.

**Leo:** He says what he'd prefer is time sequencing. So after two or three failed guesses, the UI replies more slowly. I've seen this happen with other programs. After several more it goes into "Sorry, no more tries until power cycled," so you have to reset the machine, or even "ignore/stealth mode," where even a correct password does nothing until power is cycled. True, the attacker now has unlimited time, but we can easily characterize the risk profile. After three guesses we could require five seconds between guesses. After five or 10 guesses the attacker must physically remove and reapply power or even have a nonconventionally controlled USB host. The rate slows down to one guess every 10 seconds. An internal capacitor could provide means to detect a repeated attack within 30 seconds. And since there are only 31,536,000 seconds in a year, this would - I thought it was 325- anyway. This would reduce the maximum attack frequency to about one million per year. And even a very weak five-character all-upper-case password has 11 million possibilities. The knowledgeable user simply unplugs the device, plugs it back in, and gets two or three more fast guesses before it slows down again. Isn't that better for most of us than these consequences? Thanks for having David on the show. Perhaps their team, if not their competition, has already considered these improvements.

So just to summarize, he doesn't like it because you only get 10 tries. And if an attacker tries eight of them or nine of them, then walks away, you may actually fry your own key.

**Steve:** Yeah, I thought this was an interesting question.

**Leo:** Good point.

**Steve:** Yeah. The point worth noting is that his attack model is different from what many other users may feel. I could see users who have an IronKey, I mean, absolutely seriously don't want their data to fall into the wrong hands under any circumstances. And so their model is, if I lose control of it, and someone tries to break in, and it's really not me, we're assuming we're not going to get it back when the guy is pissed off after trying eight times and didn't push it over the edge with two more tries which triggered the self-destruct. So here we've sort of created a synthetic situation where somebody is trying to crack it, brings it very close to the point of its self-destruct, and then sneaks it back under our control.

**Leo:** Never mind.

**Steve:** Uh-huh. And then, you know, we kick it over the line. So, I mean, I don't know. I thought it was worthy of discussion, and it's a sort of an interesting issue. I know that because I have so many different passwords, there are systems that I use, for example, well, I mean, many OSes adopt this slowed-down log-on approach where, if you miss the first couple, then you have to sit there and wait for 10 or 15 seconds. And it's like, it's annoying when I'm trying to remember which one of my many passwords I used. But it's sure better than having the hard disk wipe itself.

So it's like, I can also appreciate this notion of slowing it down. I do think, however, that the typical model is I have lost my IronKey, I absolutely don't want anyone to have access to it. Remember that I talked, I think it was last week, maybe it was the week before, I talked about the sort of the annoyance of a non-IronKey solution, which I myself use, my little 4GB little tiny Kingston RAM that I like so much, my little thumb drive, where I use TrueCrypt. It's sort of uncomfortable that somebody who can't provide the password can still have my data in encrypted form. That is, it's an almost 4GB file that is just pseudorandom data. It's like, okay, well, they can't do anything with it. But it's like, eh, but they could still copy it and have it and keep it and then be poking away at it. And I have to say yes, but they really, really, really can't do anything with it. I mean, that's the whole point. And the strength of TrueCrypt is it is really, really good encryption. But it's still annoying that they could have the file. And IronKey prevents them from ever getting the file, the raw data off of it under any circumstances, right up to and including killing itself.

**Leo:** Now, I should point out that you shouldn't only have one copy of your data on your IronKey anyway.

**Steve:** Correct, and that was the point he was making, a point that David, the founder of IronKey, made is that they provide a backup service. I don't think I would use them, but I would certainly want to keep all of that critical data, I mean, basically everything I'm doing with my key, for example, my own case is I'm using it, as you mentioned earlier, sort of as a sneakernet. I'm using it to shuttle stuff back and forth. This morning, in fact, I was working on some outlining stuff on my laptop, and I copied it to my key to bring it back home. I mean, I brought the laptop, too, but then I wanted to transfer it to my main machine. And it was just easier. Sometimes I'm doing that with Amazon's S3 and Jungle Disk, or sometimes I use my key. So I've always got another copy of anything on my key.

**Leo:** Right. I think that anytime you have one copy of anything, you're going to lose it somehow. And the point of all this encryption is not that it's your only copy, and this is a special, highly secure storage, but if you carry this key around and you lose it, that you're protected. That's the real point.

**Steve:** Exactly.

**Leo:** I am the kind of person, though, I have to say, who would forget his password, enter it 10 times. I almost have to call my bank every time I want to enter the bank site because I've tried three times and the bank locks me out. Every time. So there you go.

A listener named Steve in Florida - good name - wants details. Steve, says Steve, in describing your newly built Windows XP system you said, "For example, I've got every unnecessary process stopped so that when it boots it uses 131MB of RAM." So which are unnecessary? I've used BlackViper.com's list of services and disabled about 20, then found I might need one or two. It's a pretty good site, but I'm sure we'd like to know your list of what we can disable safely for a given setup. That's what Black Viper does. You have gaming, standalone, home wireless network with fax/scanner, wireless laptop, desktop hardwired to router, and also acting as print server for a freestanding printer, et cetera. Fewer unneeded services equals good. So what do you think? Do you have a list?

**Steve:** I use BlackViper.com.

**Leo:** There you go.

**Steve:** BlackViper.com.

**Leo:** He's the guy.

**Steve:** Yup. When I was doing this I poked around. I think I first learned of Black Viper when I was up with you, Leo, in Vancouver a few months back. And I thought, oh, that sounds interesting. And I'm very impressed with his work. I looked at some other sites. I also merged it with all of my own experience, although I don't have as much experience with XP as I do with Windows 2K and NT and earlier Windows. But I found Black Viper's advice to be exactly correct. I don't think I've - basically I used it as confirmation. But there's some weird services that it's like, what the heck does this do? And so it's useful to use somebody who's experimented with it, who's certainly had lots of feedback. And this guy is known for his service-disabling site. So certainly people are writing back to him and giving him feedback. So BlackViper.com is what I use. And it's terrific.

**Leo:** It was gone for a while. I was very glad when he came back. He does it for

Vista, too.

Matt in Virginia asks: How secure is SSL VPN? Steve, I have a question about VPN security, which I've researched extensively online. And of course we've talked a lot about it on the show some episodes back. He says: You're my only hope. Does an SSL VPN such as that offered by WiTopia or HotSpotVPN - or, I might add, Astaro - protect non-browser activities? In other words, when I check my email through a desktop client, not webmail, with an SSL VPN enabled, will my login info be sent through the VPN tunnel and therefore be secure? Will the contents of the email be downloaded to the client securely? I've found that IPSec and LLTP are generally not options because their ports are often blocked by hotspots. So what do you say? Thanks for your help.

**Steve:** Yeah. I mean, a VPN is secure, absolutely secure, so long as all of your traffic goes through it. I'm a little uncomfortable about the way OpenVPN works because it uses a routing table and sort of dynamic changes to the routing table in order to hopefully route all of your traffic through the OpenVPN interface. But it's finicky configuration-wise, and it makes me a little bit nervous. It sort of seems...

**Leo:** OpenVPN is not the only one that can do SSL VPN.

**Steve:** That's totally true. And so any well-designed SSL VPN should route all of your traffic through the VPN.

**Leo:** What is SSL VPN?

**Steve:** Well, okay. We've talked a lot about HTTPS, you know, the protocol used for a browser to connect to a remote server. SSL stands for Secure Sockets Layer. It was originally designed by the Netscape folks when they wanted to add cryptographically strong secure connections between browsers and servers for the purpose, for example, of allowing people to transmit their credit card information to a web server through their web connection. It has evolved through several versions. SSL is now at v3.0. And it's also sort of morphed into TLS, which is Transport Layer Security, which is sort of the formal official name now, although it still goes by SSL because that's how it was born. And essentially it is a secure, certificate-based, strongly authenticated, strongly encrypting, point-to-point connection that can be trusted as long as it's all set up correctly.

**Leo:** So when we talk about SSL VPN, we're merely saying that the VPN technology is - you can use different security technologies like IPSec or LPTP. You're using SSL instead of IPSec.

**Steve:** Exactly.

**Leo:** So it secures the whole thing. It's not that it's the SSL for your browser, it's an encrypted tunnel using SSL for all traffic.

**Steve:** For all of your Internet connection traffic, yes, yes. Whereas, for example, HTTP, which your browser uses, even though you may have a secure connection from your browser to a remote server, if you have no other VPN or security, when you do email it's not going through an SSL connection unless you've got email configured for secure connections, which you can also typically do. So, and SSL VPNs are often more robust in mobile environments, exactly as Matt says, because, for example, IPSec and LLTP, as we discussed very early on in Security Now!, they use well-known ports that are not, for example, port 80 or port 443, which browsers use, or other ports. They use well-known ports as part of their protocol, which many people who don't want VPNs to be used can block. As he says, they're generally blocked at hotspots.

**Leo:** Right, right. You can't block SSL because then people wouldn't be able to go buy stuff on Amazon.

**Steve:** Exactly.

**Leo:** Yeah. Kyle Hasegawa in Tokyo, Japan - nice to have you, Kyle, listening to the show - is wondering about quantum crypto cracking. It just sounds good. Dear Steve and Leo, thanks for the great show. You always mention the astronomical times it would take to break strong encryption using even the largest clusters of the fastest silicon transistor-based CPUs. But what happens when government agencies begin to use quantum computing? Will the trusty TrueCrypt be worthless against protecting ourselves against oppressive state agencies? This is a question actually I've asked quantum computing experts. And some of them, in fact, use that as an example, that yes, it would be easy to break. It's a little early days, though.

**Steve:** Yeah. Well, not only is it early days, and quantum computing still doesn't exist yet, and we're not even close to it existing yet, but currently 128-bit keys, symmetric keys, 128-bit symmetric keys, are considered incredibly strong. I mean, here I am talking about astronomicals again. But 64-bit keys are no longer considered safe. But remember that every bit we have doubles the complexity of the key. So when we add another 64 bits to the 64 bits we had before, I mean, 64-bit keys were considered strong for a long time. I mean, they're still strong. That's still a lot of bits. But when you double that to 128, unless we're using 256-bit AES, where we've doubled that to 256 bits, I mean, and these numbers are huge. So, yes, if and when quantum computing actually happens, it's going to be way faster than silicon. But I still don't think that we're going to have a problem with either 128-bit or 256-bit encryption. This is, I mean, really, really astronomical.

**Leo:** Well, but that's, I guess, the point of quantum computing is that you go from bits, from on and off binary bits, you go to three-state, four-state or, you know, systems which have that same astronomical geometrical factoring. So these computers, if - you're right, it's pretty theoretical. There are companies who claim they've built simple quantum computers. But if this were to happen you'd have that same kind of, you know, geometric jump in computing power, as well.

**Steve:** Okay. But geometric and astronomical, I don't know.

**Leo:** Okay. Yeah, I can understand where the question comes from because this is an example that quantum computing proponents use.

**Steve:** We'll have lots of notice. We'll let our users know with plenty of time when they need to go to 512-bit encryption.

**Leo:** Well, but if you're paranoid about the government, those are the first people who are going to use such a thing if it works. And you may - they may not warn you. I don't think the NSA is going to say, uh, guys, we've got quantum computing now. You might want to double the strength of your keys.

**Steve:** Just want to let you know.

**Leo:** Just want to give you a little heads up. Chip Mason - I like the name - from Raleigh, North Carolina wants to revisit the good old PC vs. Mac security question: Steve, I'm a longtime Windows user. And while I've used Macs over the years, generally Windows is what I end up using due to legacy software and, you know, the amount of money I've spent on software. I've recently listened to six hours of Security Now!, including episodes discussing nasty banking trojans and other issues. And that got me thinking, maybe I should just switch to Mac and be done with it. But my concern is Mac doesn't have these issues primarily because it doesn't have the market share to attract hackers. I feel that Mac will get its trojans and viruses sooner or later. But is that so? Is there something inherently more secure about Mac with its BSD UNIX Mach kernel under the covers? Actually it's really BSD UNIX and Mach kernel under the covers. I know UNIX protects root and limits permissions very well. But does this really mean viruses and trojans won't ever be a problem on Macintosh? I'm guessing it would be my luck to invest, heavily, I might add, as Macs are pricey - they're not that much more pricey, I think really it's more getting new software that's the investment - and then find the same issues showing up on a Mac that I want to escape on PCs. In other words, is it safe to move to Mac, or is it just going to - are the problems going to chase you?

**Steve:** And there's the question.

**Leo:** It's a good question.

**Steve:** I know, Leo, that I turn my little Mac on an hour or two early every time we're going to be recording in order to give it the chance to update itself. This morning I had a 50MB OS update and a 39MB Safari update. That was 80-plus patches to the Apple OS and 13 patches for Safari. I'm seeing, for whatever reason, a lot more of this security updating happening on my Macs than I have in years past. My sense is that Apple is staying ahead of the curve, that is, that again, probably because it's a less large target than Windows and Microsoft, I think that the actual incidence of exploits of these vulnerabilities is still substantially lower than is the case for Windows. But I don't think there's anything inherently different from the Mac in terms of some fundamentally more security than over on Windows. And it's worth noting that there were, like, 40 problems that were patched at the end of last year in addition to the 80 that just got patched. And I looked at a breakdown of them. Half of the vulnerabilities repaired by Apple are in open source applications. And Apache had 10 advisories. The AV had nine. MIT's technology had four, and PHP had 10. And so the other half were found in Apple's own applications or components, with that first half being in open source.

So, I mean, we know it is difficult to write really, really exploit-proof software. And I think Apple is in the same boat as Windows, and applications are in the same boat that the OSes are. And that is, people are - the ante is being upped. There's increasing value behind cracking into software. And it's the eternal cat-and-mouse game.

**Leo:** I will say that, I mean, we still have yet to see any big exploits on the Mac side, for whatever reason.

**Steve:** And I think that the Mac, and I've said this before on our podcast, I think the Mac does benefit from the horrible history that Windows and Microsoft had. I mean, Microsoft now finally has a clue. It took them a long time, an amazingly long time, to have a firewall running in Windows by default. The second they did that, the second Service Pack 2 came out for XP, everything changed. Well, the Mac learned that lesson with much less pain than Microsoft did. So it will probably always have a better reputation than Windows. And it's going to take a long time for Windows to shed the reputation it probably doesn't deserve now as much as it has it because Microsoft getting serious about security, we see that as an event in the not-too-distant past rather than it always having been the case.

**Leo:** I'll also say that Microsoft suffers because it's an old operating system, and Microsoft has always attempted to preserve compatibility with legacy hardware and software. To the degree that you do that, you compromise your ability to make a truly secure operating system. Apple, probably because it had less market share, has been very quick to abandon legacy hardware owners and legacy programs. They've done it before. They recently did it with the move to Intel. And by that - you know, it's a new operating system. So by their willingness to do that I think they're also saying we're willing to take the hit and be more secure. So, you know, I understand why Microsoft doesn't do that. But maybe if they, well, look what happened with Vista 64, you know?

**Steve:** Well, and a perfect example, too, is we've talked about Vista when we were covering the security in Vista. One of the things that we ended up making very clear was that Vista has a ton of fundamentally sound new security technologies which they have had to deliberately neuter for the sake of backward compatibility, exactly as you were saying, Leo.

**Leo:** Yeah, yeah. That's the tough one. I think ultimately it comes down to that. Certainly Apple is less of a target because there's fewer machines installed. Hackers know Windows. They know how to attack Windows. And there's more profit in attacking Windows. But I think they also benefit because they're willing to perhaps be a little less secure.

**Steve:** And the fact is, you know, there was a comment about how Macs are pricey. Of course, that again, that's history. That's really not true today. So it is the case that hackers hack the machines they own. They don't hack machines they don't own. Traditionally people were receiving Windows machines for Christmas. They have them at school. Hacks had Windows. Now the hackers have Macs. And so we're beginning to see more Mac hacks.

**Leo:** Right. I don't think you're going to see a massive change in market share for Apple, however. I mean, yes, market share's going up. But you're not going to see - Apple's never going to be more than 10, maybe 20 percent at best. Not for years.

**Steve:** Which is good for the Mac people.

**Leo:** Yeah. I mean...

**Steve:** It is.

**Leo:** You're not going to be the dominant operating system. It's just not going to happen.

John Hurst in New York City has a question about IronKey. He says: The rep from the company - well, that was our guest a couple of episodes ago - said they planned a number of improvements for the near future. Will the buyers of the current IronKey device be able to update, or will they need to buy a new IronKey? Well, I asked him that because I was wondering. And he said they'd be updatable.

**Steve:** Yup, I wanted to make that very clear. The question had been asked a number of times. And so I finally said, okay, let's make sure everybody knows. First of all, of course, this was not a rep. This was the founder and CEO and chief techno bottle washer guy. I mean, absolutely the guy.

**Leo:** We don't talk to reps. Ever.

**Steve:** And we did make it very clear. We said, if we buy the keys now, will all this cool next-generation stuff be retrofittable? And David said yes, absolutely.

**Leo:** Yeah. Which was really encouraging. Justin Gerard, lurking somewhere in the USA, wondered about Firefox preaching: Hey, Steve and Leo. On Windows Weekly I heard about how Firefox was gobbling up - oh, I'm sorry. Did I say "preaching"? I misread it. There's a "C" in there. You know, it's interesting, you take out the "C," it is "preaching." He said "pre-caching." On Windows Weekly I heard about how Firefox was gobbling up tons of memory by using pre-caching. And that is in v2, by the way, not in v3. So I was wondering, if Firefox pre-cached a link with an exploit in it - oh, this is interesting - could it exploit the machine even though I didn't click the link? So pre-caching is you go to a website, and it loads, starts to load all those other sites that are on that website before you click them. He wonders if, by very virtue of the fact that they're loading those pages, could the exploit be triggered. Keep up the great podcast. I hope to be like you someday. Aw. Justin Gerard. Oh, he's Gamer's Edge. That's actually a great podcast.

**Steve:** Well, I'm glad to hear that because he's also the neat, I think he was either 12 or 13, who had the Best Buy computer guys, the Geek Squad guy came out and I think ran a copy of SpinRite that he didn't own.

**Leo:** Oh, yeah, yeah, yeah.

**Steve:** And it was funny, too, because I used GRC's sitewide search. I put Justin Gerard's name in and, wink, there were the - I got three hits on his name, thanks to Elaine's transcribing it. So I was able to remind myself that, yeah, that's who I thought it was.

**Leo:** Yeah, Justin's a great guy. Great kid. Who will undoubtedly succeed us and do better.

**Steve:** Well, and to answer his question, it's a really great question because, exactly as you said, what Firefox is doing is it's going and sort of going out and pulling in content that are referred to by the pages that you are - by the page that you are viewing. The good news is, though, that it's not until the page is displayed that, for example, JavaScript is invoked, that active scripting comes into play, that the images of the page are run through the image rendering. And it's the image rendering that can cause malicious JPGs or PNGs or whatever to get exploited. So it's almost certainly the case that the pre-caching would not expose people to exploits from linked pages that you did not click on. But it's a really great point.

**Leo:** Yeah. So it doesn't get exploited until you click on it. Doesn't get - it doesn't run.

**Steve:** And I was curious, Leo, because I did not listen to that episode of Windows Weekly. Apparently it's, what, filling up its cache with pages you never visit?

**Leo:** Yeah. So people had noted in the past that Firefox 2 takes a huge memory footprint. And it's because it's loading these pages. And I think that's bad 'Net behavior, frankly. I think you're using bandwidth you shouldn't ought to be using. It does speed up browsing, of course, and there have been programs that have done this in the past. For years people had programs that would do this. And I believe it is behavior that they have stopped in Firefox 3, which makes it more reliable, reduces the memory footprint. And you know what, I have to say, everybody has broadband now. It's not that much faster.

Hudson Seiler of Janesville, Wisconsin has a cautionary data recovery message for our listeners: Steve, he says, I recently bought a dead and broken Xbox 360 hard drive. I took the drive out of its proprietary Microsoft mounting mechanism - I guess once you do that you've got a standard SATA drive - and utilized SpinRite on it. SpinRite not only allowed the drive to boot, but to my astonishment - whoops - it completely recovered the data of the previous owner. I of course immediately deleted it, reformatted the drive, and it works great. Thanks, Steve. However, listeners of Security Now! should grasp the imminent security risk of having your gamer tag stolen - oh, that's a good point - because it contains your debit or credit card information. Also, for security, store your gamer tag on a 360 memory unit. That way if somebody does get your drive, at least they can't get your credit or email information. SpinRite rocks. Boy, I didn't even think of that. But that's true, your gamer tag is on there, and password.

**Steve:** Yup. So I thought that was a great thing for Hudson to mention.

**Leo:** Thank you, Hudson, for reminding me. You know, when you send your Xbox 360 - and Microsoft says detach the drive, do not send us the drive. But if you were to sell the drive, that would be - or your Xbox, that would be an issue.

Now, our final question, it's really a statement, from Chris Noble of Wellington, New Zealand. He brings us our Cool Firefox Add-On Tip of the Week. Hi, Steve. Just finished listening to your latest Q&A episode in which you discussed the problem of not knowing the URL with which a form is being submitted, or to which a form is being submitted, for instance is it secure or not. But there is a Firefox extension, he says, just for you, called FormFox. Have you checked it out, Steve?

**Steve:** No, I haven't. But I posted the link because the way he describes it I thought, hey, this is very cool.

**Leo:** I'm going there right now. Let's see, will it install? Yes, it will install in my beta version of Firefox. "Do you know where your form information is going? This extension displays the form action, the site to which the information you've entered is being sent." In any place where you can enter data from search boxes to order forms, just mouse over the form and it will say where it's going, including the HTTP or the HTTPS. So you'll know immediately if you're going to a secure server or not. That's cool.

**Steve:** I think that's very, very cool. I mean, I could easily wish that browsers just did this by default, is that you mouse-over the button and a pop-up tool tip gives you the URL, and maybe color-coded, green if it's HTTPS and red if it's not, just as some additional quick verification that it'll be a secure access when you press the button. I thought that was a really nice little add-on for Firefox, and I wanted to let our listeners know.

**Leo:** It'd also be useful if they were routing it through somewhere like, say, DoubleClick.

**Steve:** Exactly.

**Leo:** He says: I've used this, and it works a treat. The form's destination URL is revealed in a little text pop-up when you mouse-over the button. A very nice solution for security-conscious Firefox users without having to dig through the source code. Thanks for the podcast. Keep up the great work. Thank you, Chris Noble. We love tips as well as questions. How do people submit or ask their questions?

**Steve:** They go to GRC.com/feedback. And there is a web page form that they can put their question in. Telling me who they are is optional, although we like to have that so we can, for example - that Chris is named Noble, Chris Noble in Wellington, New Zealand. He volunteered that information. And so that is fun to share with our listeners. So I appreciate him sharing that with us.

**Leo:** Very cool. GRC.com is a great place to go, too, for your security software. There's all sorts of little utilities, really fun stuff. And of course the world's famous ShieldsUP!. People go there to test their router, first thing they do when they set up a new router, go to ShieldsUP! at GRC.com. And while you're there don't forget SpinRite, the world's best, the finest, the must-have hard drive recovery and maintenance utility. GRC.com. We also have 16KB versions of the show there for quick download. Elaine has the transcripts up there so you can read along. It's just a really great place to go. By the way, when they do the transcripts of these Q&A sessions, Elaine just puts the entire question in its entirety, so you can just read it exactly as it is.

**Steve:** Yup, she asked me for the text so that she can spell everyone's name right. And then I realized, hey, you know, the text is there, use the text and save on typing.

**Leo:** Yeah, don't use Leo's fumfering around, just put the whole text right in there. Steve, we're done with this episode. That's great. Next episode, next week, I'm still going to be in Australia, so we're going to pretape. What do you want to talk about next week?

**Steve:** Well, there's been a lot of controversy about - and we've talked about this several times - about the issue of so-called "Network Neutrality." And a lot of Internet engineering is going into looking at what the real problem is with essentially users essentially colliding with each other. I want to talk about, not the politics because that's for the politicians, as always, but the technology of congestion and how congestion is handled and how it can be changed to change this. This isn't directly obviously a security issue, but it's something that affects everyone.

**Leo:** Well, it kind of is, kind of is.

**Steve:** Well, and it turns out, I mean, our listeners, as you were saying either this time or before, we have smart people. And I think that if people understand some of sort of the key concepts behind congestion, because it turns out that, for example - I'll tease people a little bit this week. Once you've got a network in place, the cost of using it is the same whether you don't use it or you use it all until congestion occurs. It's when congestion occurs that is when you max out. That's when you start having a cost associated with overusing it. And it turns out that TCP does not do very well in congestion. And there are other things like multiple connections tend to abuse the way routers handle congestion. So I want to talk about all of that and sort of set some context for sort of some engineering and sort of a theoretical context for the impact of people using YouTube so much and downloading TV shows over the Internet and, like, what's happening as the model of how people use the 'Net is evolving from a technology standpoint.

**Leo:** You know, I often say that there's two kinds of 'Net neutrality. There's one thing if a company is trying to be anti-competitive and filter out any Skype calls so that they can charge you for their Voice Over Internet. But there's also a legitimate need of a company to stop bandwidth hogs. If there's four or five guys using BitTorrent to download the entire library of movies out there, it impacts your ability to get decent bandwidth and decent speeds, and their ability to make a living selling Internet access. So I think it isn't unreasonable for companies to try to control some of this bandwidth and how it's used.

**Steve:** Yeah, I completely agree. And in fact an old model of a network is the phone system. And we know that the phone system is unable to handle everyone talking at once. During emergencies, when people all try to get on the phone, nobody gets a dial tone because the system is unable to actually service the number of subscribers it has. Similarly, no ISP is able to provide all the bandwidth simultaneously that they're selling to people because they use a model for how much bandwidth people are actually going to use. That model is being skewed. And as you said, Leo, when there are some hogs who are sucking out a disproportionate amount of bandwidth, and I guess I have to use the term "hog" provisionally because users can argue, hey, wait a minute, my ISP said that I have unlimited bandwidth, so I want to use it. I want to get as much as I can. Anyway, it turns out that the way the Internet's technology fails in the case of overuse is currently not optimal because it was never designed for what has happened. And that's what we're going to talk about next week.

**Leo:** Yeah, yeah, yeah. I mean, some of it's they're cheap and they don't want to buy more bandwidth or have more connections. But there's some legitimate need to control, as well. All right, good. That's a good subject. We will be back next Thursday on April 10 with a great...

**Steve:** Never missing a week.

**Leo:** Never missing a week. Rapidly pulling away from TWiT because we miss weeks all the time. In fact, I should mention that you've probably noticed that a number of podcasts are not arriving. It's because - except for Security Now!. It's because I am in Australia, and we're not recording This Week in Tech, Net@Night, MacBreak Weekly. So we're taking a couple of weeks off. I'm thinking of it as a spring break minus the over-consumption of alcohol. So enjoy your spring break. Catch up on the podcasts you've missed. There are still podcasts coming out. And we'll get - in fact, I'm going to be doing some, I think - you might check my blog, Leoville.com. I should have pictures, blog entries, and even some audio available if I do put out podcasts or audio from the trip to Australia. I'm going with some brilliant photographers, you know, this is our new Lightroom Adventure, and some of the greatest people out there. So you can check, if you subscribe to the Radio Leo podcast, that'll get automatically pushed to you. That's Leo.am/podcasts/leo. That's the Radio Leo podcast.

Do you know about the Radio Leo podcast? Some people don't, and I should mention there is one feed - you could subscribe to the individual shows like TWiT, Security Now!, and MacBreak Weekly. But I made one feed - somebody asked me, well, I'd like a feed with everything that you do on it. So there's one feed, Radio Leo, that has all of the shows that I appear on. And there's also a feed of everything that TWiT puts out. And that you can subscribe to. That's the TWiT feed. Actually the Radio Leo feed is, as I said, Leo.am/podcasts/leo. The TWiT feed is through the TWiT.tv site. It's actually Drupal does an RSS feed automatically of everything we put out. And I think - let me just check to see exactly what the URL is for that. It's http://twit.tv/ - let me just see what it is. I think it's /node. I want to get this right so I don't - let's see, show info. Let me see if I can find the actual feed, dagnab it. It's hidden here somewhere. TWiT.tv/node/feed. And that will be - what that is is an RSS feed with everything that comes out on TWiT. Everything. Not just stuff I'm on. So there's Radio Leo if you want just the stuff I'm on. If you want every podcast - and that's a good way to make sure you get everything that we put out, including blog posts and everything. It's TWiT.tv/node/feed.

All right, enough of that silliness. We'll be back next week with another episode because Steve refuses to miss even one episode. I hope you'll join us. We'll see you next time on Security Now!.