Listener Feedback #135

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-336.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-336-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 336, recorded January 18th, 2012: Your questions, Steve's answers, #135.

It's time for Security Now!, the show that protects you and your privacy online with this guy right here. What did we come up with, the security general? The security...

Steve Gibson: No, it was good, too. I forgot what it was.

Leo: It was good. Dang. Instead of "The man, the myth the legend"?

Steve: Yeah. Definitely we want something better than that. We had - I'm sure that someone in the chatroom will...

Leo: We had a name for Steve. We had a name. Anyway, Steve Gibson is explainer-in-chief. That's what we had, explainer-in-chief.

Steve: Ah, I like it.

Leo: Steve Gibson is here from GRC.com. By the way, stop banging your video player or your TV. I know people at home are going, wait a minute, something's wrong, the color isn't - maybe I can get the - no, we're in black-and-white today because this show is being recorded on January 18th, which is a day marked across

the Internet by protests against the intellectual property bills, SOPA and PIPA, in the U.S. Congress, House and Senate respectively. Many sites have gone dark including Wikipedia, Reddit, and others. We decided not to go dark, just dark gray, in order to remind people to call their member of Congress, to let their member of Congress know they don't want them to support SOPA and PIPA, and to let people around the world, because we have a vast global audience, know they are not immune. Many countries are being lobbied by the World Intellectual Property Organization, which is essentially a front for American content creation companies like the MPAA and the RIAA, to pass laws that they have in some countries, like France and Spain. So you are not immune, either.

It may not be called SOPA, it may not be called PIPA, it certainly won't be called SOPA and PIPA in the U.S. next time around. But these companies will not stop until they break the Internet to protect their business models. It won't work. It doesn't work. And it's something we have to defend against because, as you, anybody who watches this show knows, the Internet is the last best hope for mankind, and we want to protect it. So that's why we're in black-and-white, just so you know. It is not the fault of your TV or your video player.

Steve: We have not degraded the audio quality, however.

Leo: Yeah. And those of you listening in audio, we've always been in black-and-white, or whatever color your imagination comes up with. What's the topic du jour, Steve?

Steve: We're in Q&A mode today. So this is Episode 336 of Security Now!, with our 135th Q&A.

Leo: Wow.

Steve: We've got our regular round of updates and news. And, as expected, the WPS, the WiFi Protected Security issue, is alive and well, so we've got a bunch of news about that. And in fact we're going to next week have a really fun propeller-head episode about the protocol because, first, let's see, I think the first instance was an engineer at Nokia explained sort of cryptically, he sent me a tweet saying that it would not work what I had suggested last week, to have the access point not deny that the first half of the eight-bit or eight-digit PIN was wrong. And I thought, oh, okay.

Then Stefan Viehbock, who wrote the disclosure, and I had some discussion on Twitter. And then Dan Kaminsky got involved, and Dan and I moved it off to email to confab about this. And that all caused me to take a much closer look at the protocol. And now I get all the subtle details, and they are really interesting because what the Wi-Fi Alliance tried to implement is something called "zero-knowledge proof," where both sides prove that they have knowledge of something without giving away what it is, because this isn't a one-way authentication, where it's only the user who wants to prove to the access point they know the access point's PIN. It's a mutual authentication because you also want to prevent a rogue access point from impersonating the one that you're trying to connect to. So you need to prove that you know the PIN to the access point; while, simultaneously, it proves it knows its own PIN, which a rogue access point wouldn't.

Anyway, it's really interesting, and there's some new crypto primitives involved that we haven't talked about before. So next week we're going to explain zero-knowledge proofs and mutual simultaneous authentication and why it still doesn't work.

Leo: I love that.

Steve: Yeah.

Leo: Some computer science coming at you.

Steve: Good crypto science.

Leo: Yeah, I like it. Well, before we get to the questions, I presume there is security news to talk about. So let's get to it. This second Tuesday we - we did the show last week Monday.

Steve: Right.

Leo: So we missed the second Tuesday.

Steve: And we didn't know in detail what Microsoft was going to do. They did release, as expected, a handful, small handful of fixes. One of the things that they did fix we were hoping for, which was the problem with BEAST, which we talked about extensively. You'll remember that there were some researchers out on a beach somewhere who came up with a way of breaking the block encryption aspects of SSL. We did a whole podcast on BEAST, which is the acronym for Browser Exploit Against SSL/TLS. I don't know how these guys get these great acronyms, but that's just - that's a great acronym. Anyway, that has been fixed in Windows as of last Tuesday.

The other significant update, because Adobe also had theirs last Tuesday and fixed problems that we had been hoping they were going to fix in Reader and Acrobat and Flash, but Oracle released their big quarterly update just yesterday, so on January 17th, which fixed 78 problems in MySQL, which of course is the big SQL database product. One of them was very important because it could be - it was a vulnerability which could be exploited remotely without login credentials.

So they didn't talk about this before, but now that they have it fixed on their page that enumerates the things that they're claiming are fixed, they're now really pushing people to make sure that whatever products they're using which have MySQL as part of their backend database, that they go through whatever procedure on a product-by-product basis as necessary to update themselves to the latest and greatest as of yesterday. So I wanted to pass that on to our listeners, that there is some important things that were released. And as often is the case, it could be that bad guys, knowing that there is now a no-login, remotely exploitable vulnerability which has been fixed, they'll plow in, figure out what that is, and then go after people who haven't fixed it. So anytime you've got MySQL exposed to the Internet, there's cause for concern. So you want to make sure

that you're up to date with this patch.

In news, there's been some talk, and we've been talking about it recently, of so-called "slow motion denial of service attacks" against servers. I've recently talked about the idea of stalling TCP connections. We were talking about how TCP throttles itself with the notion of advertising a window of buffer space, meaning that, for example, when the client is acknowledging the receipt of data, one of the fields in the acknowledgment shows the server how much receive buffer it has. So that allows the server to send data in advance of its acknowledgment. And that's a beautiful way of having TCP deal with the delays which are inherent in any packet-oriented free autonomous routing system like the Internet uses.

So this is part of the super cleverness of our Internet protocols that makes the whole notion of a routed packet network work. Unfortunately, there are always ways to exploit these things. And one of the things you can do is you can advertise that you, for whatever reasons of your own, have no buffer space available. And what that does is that shuts down the server's ability to send data to you, causing it to send acknowledgments every so often, a so-called "window probe," to continually ask you for new acknowledgements of that probe, hopefully telling it that you've freed up some buffer space.

So the point is that what hackers are now intrigued by is not the big flooding attacks, which is what they've been doing, but various types of slow-motion attacks. And so both researchers and hackers are now experimenting with giving servers, web servers on the Internet, publicly available servers, new kinds of grief by either slowly dribbling to the server their request, or forcing the server to slowly dribble out its reply. And so I'm just sort of seeing in the news sort of a continual flow of new attacks. And this is problematic because there are existing now lots of tools for responding to flooding attacks, where there are upstream gateways that attempt to verify that incoming connection requests, for example, are valid or not.

The problem with these new attacks is all of the requests are valid, they're just very slow. And so what servers normally do is receive a request and respond to it, and they're done. They close the connection. These hold the connections open and overwhelm the server's connection resources, rather than the bandwidth resources. They use, in fact, almost no bandwidth. What they use is many, many, many more simultaneous connections to the servers, and that's a new aspect that right now there aren't any good defenses for. So what'll happen is, of course, the people who provide border security and abuse prevention defenses will have to come up with a new paradigm for looking at, for example, how many connections are open, and whether the connections are actually doing a reasonable amount of work, and terminate connections which are in this slow-motion attack mode. So anyway, just it's one more thing that the bad guys have come up with to wreak havoc on the 'Net.

Leo: I like "slow motion attack mode."

Steve: Yeah.

Leo: That sounds like a new move in a fighting game. Mortal Kombat, slow-motion attack mode.

Steve: And I did - just a little blip on my radar was a note that we talked sometime ago, you'll remember, Leo, that the Air Force base in Nevada from which our drones are being remotely piloted was infected because it was running Windows. And so many people responded by saying, wait a minute, our drone systems are being driven by Windows? Because everyone is always sending me pictures of ATM machines with a...

Leo: Crashed, blue screens of death, yeah.

Steve: Blue screens of death, or a little dialogue saying you must update your security patches, click here to proceed. And meanwhile the whole ATM is nonfunctional because the system is waiting for someone to click a button, using a mouse that doesn't exist and so forth. Anyway, the point is that it sort of made the low-level security news that that Air Force base had moved away from Windows. They were switching to Linux. So, yay.

Leo: Yay. Although, I mean, Linux is more secure. It's better. It's more mission stable. I wonder if it's, I mean, aren't there still viruses and attacks on - of course there are.

Steve: But I guess the way to say it would be there are still vulnerabilities. However, they're just not the big vulnerabilities being developed for Windows, which is still the majority platform and still everyone's big target.

We had a big breach that happened just recently. The online website Zappos was hit by a major database breach. They sent out email to 24 million customers, telling them that they had expired their passwords and giving them instructions for how to go about re-authenticating themselves and using a new password. So their names, their email addresses, their password hashes, and in some cases the last four digits of their credit card numbers were lost, essentially, in this big database breach. They did not lose the critical credit card purchasing records with the full credit card numbers. So that wasn't lost. But still, the login information was.

So as soon as Zappos realized this is what happened, they shut that down, they expired everyone's existing passwords, and began sending out email to a massive customer base, all 24 million customers, explaining that they would have to change their passwords. So by every measure, I thought they responded well. They sent out a letter to their employees to explain what had happened. They attached to that letter the letter that was being sent out by email to all the customers so that everyone would be up to speed. They did suspend their telephone system because they were concerned that it would be completely submerged under people choosing to phone rather than use the online resources. So anyway, that's in our breach news.

Leo: Poor Zappos. I think they handled it well, though, didn't they.

Steve: Oh, I think they really did. It's like you never want this to happen. It's never going to be good. But you want to be responsible. And...

Leo: They separated the credit card numbers out. I presume they were using salt

because it sounded like people were not getting stuff in the clear; right? And they said something that was really good, which is, if you use the same password on other sites, change that, too.

Steve: Yes.

Leo: That was smart.

Steve: Yes. And so they were storing hashes, and it was hashes that escaped, not the passwords themselves.

Leo: Much better.

Steve: So, yeah. They did, I think, they responded as well as they could have.

Leo: Right.

Steve: There is now, we talked last week about Reaver, which was the open source tool whose source code had been posted on Google Code, produced by Tactical Network Solutions. There is now Reaver Pro, as we would have expected. And as I predicted, we're beginning to see the release of additional tools. SourceSec Security Research released WPScan and WPSpy tools which are Python scripts. And those actually existed some time ago. They're not Reaver, but they are scanning tools. They presented these at ChicagoCon, and they said: "WPScan actively sends 802.11" - that's WiFi's IEEE code - "802.11 probe requests to access points that advertise WPS support. It then parses out the WPS Information Element in the resulting probe response and displays the results. This is a very useful fingerprinting tool since nearly all new routers have WPS enabled by default, and most vendors will actually put the exact make, model, and version of the router in the probe response."

So this WPScan has been known for some time and has been actively used as a means of identifying make, model, and version number of router, which of course is very useful for hackers who want to then begin to break into routers using any vendor-specific, firmware version-specific vulnerabilities that may exist. And then the second tool, WPSpy, they say "is a tool to simply monitor and report changes in the WPS status of and access point. This is particularly useful if you are running some of our described attacks that leverage WPS to gain access to the WLAN." So again, I think over the next few months we will be covering and reporting on ongoing WPS things.

And also, of course, there was feedback, as I requested, from the Twitterverse. Anthony Downs in Rockville, Maryland, he sent me a note saying that the Actiontec MI424WR, which is Verizon FiOS's router, claims the WPS functionality will not be enabled with a future firmware release. So Verizon FIOS is going to respond by just disabling it by default, which really does sound like the right thing to do. It means that it's not as convenient and easy for users. But as we will see next week when we go into this protocol, it really does look like there is no safe way to do this.

Someone tweeted with the Twitter handle of Ludden. He said, "@SGgrc, I have a new AT&T U-verse modem/router which has WPS disabled by default." So that's good to know, any AT&T U-verse users, since this all has of course caused a great upheaval of concern over WPS. And in fact, not surprisingly, some of the Q&A questions we'll be talking about in detail are asking about some workarounds and things that people are asking whether they would work or not.

Philip Hofstetter tweeted from Zurich, Switzerland, said to me that Apple routers do support WPS. You may remember that...

Leo: Oh, yeah, I was curious, yeah.

Steve: Yeah, we left that as an open question. And in fact one of our Q&A postings is from somebody who has done a lot of tech support on the Apple side and has some exact specifications of...

Leo: That's weird because I - maybe I - or I guess I have an old AirPort Extreme. But I've never seen the PIN code on that, so I don't know...

Steve: I think it's generated dynamically.

Leo: Ah.

Steve: He goes on to say, "They do support WPS, but only while their config tool is open, and you select a special menu entry." And then he says it shows a random PIN.

Leo: So that's effective in protecting against this attack.

Steve: Yes. I does look like it is. I have not confirmed that WPS is not still broadcasting something. But as you say, Leo, they did not print a PIN on the outside, so there isn't a static PIN. So that's certainly good news.

And then, finally, Ben Naidus tweeted. He said, "Netgear is protected from PIN attack by going into lockout for 'predetermined amount of time.'" And then he cites the Google chart, and he says, "Note: Netgear recommends putting a checkmark on 'Disable Router's PIN.'" So that's good news.

Leo: That's good.

Steve: And then I did get something, it's interesting, it's weird that I ran across this in my mailbag today when I was running through everything for the Q&A because a listener, Sasha in Croatia, said, "Greetings. I am super new to your show. Not new to your page, having used your ShieldsUP! service way, way, way back when you first made it. Loved your sci-fi podcast show." He said, "I started listening/watching actually your and Leo's show a few months ago and love it. It will take me forever to go through them

all. My rant is about your SpinRite page. I hear all the cool stories and testimonials and want to use it so bad. But I can't get what it does, exactly."

Leo: I want to use it, but what does it do?

Steve: He says, "Is it a disk backup tool? Can it be used for that? Is it a disk fix tool? Disk format tool? Disk defragmenting tool? What exactly does it do?"

Leo: I'm glad somebody asked that. That's good.

Steve: He says, "I have a complaint about your demo videos where you assume we all know it and simply talk about how good it is instead of actually showing one example, even, of what it can." He says, "So if you can talk more about this, possibly a few minutes on the show, I know people will think it is made up to increase your exposure time. But don't just assume all," he says, "we're all listening to Security Now! forever." I guess he means we've all been listening to it forever. "Thanks for this, and thanks for everything. You and Leo are awesome. Love you guys. Sasha."

So, okay. Just a minute to answer Sasha's question, what this does, what SpinRite does. Recently I've been seeing the term "bit rot," and I'm not sure why bit rot has been in the news recently. But there is a problem that hard drive data does degrade over time. We know there's things called so-called "grown defects," that is, defects growing over time. And try as they have, and they've done an amazing job, manufacturers are unable to produce absolutely perfect media. And that's become a bigger problem as we've been storing greater densities on these magnetic platters because what it's done is by making the bits smaller, it's effectively made any defects bigger.

So in order to deal with the fact that media is not perfect, and it has never been, even back when we were only storing 10MB on disks, all of us who are old school, Leo, you'll certainly remember when there were little charts printed on the outside of the disk drives showing the location of defects that had been found at the factory.

Leo: Right, right.

Steve: And what people who were formatting these drives were supposed to do was manually enter the list of defects into the low-level formatter, which would then mark those sectors as bad. Well, it quickly became clear that OEMs were not taking the time to do this. They were just pumping these systems out, and they weren't manually entering into a low-level formatter what the defects were.

So one of SpinRite's first uses 20 years ago was people would run it on brand new drives, and it would find defects, often in sectors they were using, which was a concern. So SpinRite would relocate the data to non-defective sectors, mark those sectors bad, and then keep them from being used. So SpinRite was doing the work that should have been done by the OEMs but wasn't being done by the OEMs.

So, over time, drives evolved. Drives began handling their own defective sectors, meaning that even though there were still defects, they would manage them themselves. So then SpinRite's job changed. Then, by running SpinRite on these drives, it would show

the drive that there was a problem that the drive wasn't aware of because the drive isn't omniscient. It only knows there's a problem if it tries to read the data and has a problem reading it.

So the way that works is that there's error correction technology which is able to correct runs of bad bits up to a certain length. That is, you might have, like, you can sort of think of it as a pimple on the surface, but the data only intersects sort of an edge of the pimple. So a few bits cannot be stored accurately there because there's just a problem in the media. So the drive incorporates technology, it actually stores extra data at the end of the sector which very cleverly allows it to correct any small problem which it may have encountered in reading the sector.

Now, what could happen over time is, just because of the head flying over the surface, there is some interaction. There's an air bearing. There is a little bit of mechanical flexing of the surface of the disk. And that can interact with this pimple to make it bigger over time. So while, for example, maybe only four bits had a problem originally, that grew, the defect grew to five or six or seven as this problem on the surface grew over time. So what happens is, again, the drive doesn't know there are these growing problems until it reads the sector.

So one of the things that SpinRite does today, when I talk about it being of preventive maintenance value, is it simply goes out and reads the entire drive. It also writes it, flipping all the bits upside down, and then reads that, and then flips them back and reads it again. What that does is it sort of exercises the surface, and it allows the drive itself to realize, whoa, we have been able to correct a certain spot that was only four bits long in a problem, but now it's eight. And say that a drive's maximum ability to correct is 12 bits. Well, at some point, at some threshold, four it might have been comfortable with. It got up to eight, and then it says, oh, this is getting worrisomely close to our maximum ability of, for example, 12 bits to correct.

So right now, before it gets any worse, we're going to relocate this sector. It didn't bother when it was just four bits of problem. It bothers when it's eight. So it relocates the sector itself and puts a new good sector in, in place. So that's one of the reasons that people say, I've been running SpinRite for years, and I've never had a problem, but it doesn't seem to be doing anything. Well, it's actually doing something. The problem is that it's part of the hidden management and maintenance, surface maintenance that all drives do today.

So there's really nothing I can show. I can show and do show on the SMART page that sectors are being relocated and that errors are being corrected. That SMART analysis page sometimes scares people because it shows, wait a minute, this thing says we're correcting so many errors per megabyte. And it's like, yes, that's the reality of today's drives is they're correcting errors all the time because we've made the bits so small, in order to make the density so high, that no surfaces are error free. They've got errors all over them, but we're just - we're taking them in stride.

So one of the things that SpinRite does from a preventive maintenance standpoint is work with a drive to show it it's got problems and induce it to relocate sectors to safety before those problems get too big. But we also hear testimonials all the time of people saying, I was getting blue screens. I could no longer boot. I could no longer run a certain application until I ran SpinRite. So the other thing SpinRite is able to do, essentially, is beg. It just begs for the data. Because we would like to believe that drives are digital, that they're just ones and zeroes, and that's what's being stored. But the fact is, down at the sizes we're dealing with, it's all become analog. And so we're not just storing digital data anymore. We're not really storing digital data. We're storing analog data which we

reinterpret as digital data.

And so SpinRite has a whole vocabulary of things it's able to do to get a drive to read a sector it will not read, one last time. We just beg. We go out a different distance and come in at a different velocity from both directions, hoping that the head will happen to be in a slightly different position, where just one last time, instead of it being 13 bits that are uncorrectable, it'll be 12. SpinRite has this thing called DynaStat, which is a dynamic statistics system, where it's actually able to reassemble what must be in the missing area in order for that sector to be corrected. It's able to essentially interpolate the missing data and reverse-engineer what was originally there, even though the drive won't read it. So there's all kinds of things that SpinRite can do, if we wait too long to use it. And of course everyone waits too long. Most people aren't buying it for preventive maintenance because it's not cheap. It's $89. But you own it for life.

I've been keeping it alive for the last two decades, so you can imagine you'll end up being able to amortize that purchase out over time. And there will be a SpinRite 6.1 soon to deal with the evolution which has occurred since I finished SpinRite 6.0. And that'll be free for everyone to update. So that's what it does. It really can recover data which the drive tells you it cannot read. SpinRite says, just give it to us one last time. When it does, then the drive says, oh, my god, I'm so happy I was able to read that one last time.

Leo: Thank you.

Steve: It relocates that data to safety and puts a new sector back with the recovered data, and then your computer boots again. Or your applications run. Or you can access your database. Or whatever. It's better if you run SpinRite over it every few months, or often enough, no one really knows what that is, but every few months is probably often enough to show it there are problems evolving before they get to the point that you're holding your breath and crossing your fingers that SpinRite will bring your data back, which more often than not it seems able to. So that's the whole story.

Leo: There's the SpinRite story. Somebody said this is the nice thing about SpinRite. It eliminates all marketing jargon and says here's what I do. That's what's great about Steve.

Steve: Yeah, it just works.

Leo: Yeah. All right, Steve Gibson. Are you ready?

Steve: Yeah. But let's talk about DNSSEC first.

Leo: Oh, yeah, would you? Because I think that this is germane to what's going on today, the SOPA protests. These bills, SOPA in the House and IP Protect Act, or PIPA, Protect IP Act, in the Senate, and other bills like it around the world, one of the features of them is that they modify DNS. They allow the government to say "Take this website off DNS," the presumption being these are pirate sites, and we're going

to take them down.

Steve: Well, essentially, what they're trying to do is to legislate spoofing of DNS. They're wanting ISPs to redirect people to a different website than their actual target. And how many times in this podcast have we talked about the security problems associated with spoofing DNS? That's a big problem. And what DNSSEC, that is to say, DNS Security, does is it signs DNS records so that spoofing can be prevented. So it adds a layer, I mean a valuable layer, of true security.

Leo: But Steve, if we can't spoof websites, those pirates will win.

Steve: Yeah. Exactly. So essentially what happened was, in response to this call for breaking DNS by legislatively requiring that DNS be spoofed, the real engineer techies of the Internet said, wait a minute, we've been working now for quite a while to prevent exactly what you're suggesting you're going to require by law, and it breaks the Internet security. And it absolutely does. It would mean that DNSSEC, that is, valid records signed would not be spoofable, so users would have, at some point in the future, when DNSSEC is fully deployed, will in the same way, I mean, exactly the same way that SSL gives us an authentic connection - remember, it provides not only security, that is to say privacy because it's encrypting our connection, it's also authenticating the other end.

We know that when you connect to GRC.com over SSL, you know that you're at GRC and that nothing has gotten in the way to spoof your connection because I have a certificate that DigiCert has signed, and you believe DigiCert because your browser has their Certificate Authority certificate there to verify their signature. So that authentication is every bit as important as the encryption. Well, we've moving towards an authenticatable DNS, which we do not have today. We don't have it. We're assuming that these DNS records which propagate from the root servers and their original origin servers at whichever layer in the network they are, we're assuming that they're correct. But there's no encryption. They're UDP packets that could be intercepted and changed. And all there is in there is an IP. But the records themselves have no protection. I mean, they have a checksum, but you could just rebalance the checksum if you change the contents of the records.

Leo: Yeah, we know how that works.

Steve: Yeah, the entire DNS system is in the clear right now with no protection. So what we're moving towards is providing for the first time the ability to cryptographically sign and verify that the DNS record that arrives at our computer is the one that the owning DNS server sent, and that the technology will absolutely prevent that from being tampered with. Yet what this legislation would do would be to break what we're heading towards and just arbitrarily say, oh, you asked for this URL. We're going to give you a different IP to redirect you to a page that says we're sorry, service has been suspended because that site is believed to be a pirate site. And that breaks DNS.

Leo: Well, there you have it, if you needed another reason to not like this. Actually it segues right into our first question of the day from Robert Van Etta in the United

Kingdom: I just wanted to point out how seemingly small changes by commercial organizations have broken the Internet in the past. Remember this? We talked about it. In 2003 VeriSign introduced something they called "Site Finder." Instead of simply returning a host-not-found type response, VeriSign used wildcards on the .com and .net TLDs to direct users to their own servers. So if you entered, mistyped something, it would go back to a VeriSign server, and they of course would give you an ad, in effect. They'd give you search results and an ad.

Steve: Yeah, they were trying to monetize your mistakes.

Leo: Right. Needless to say, this broke several services that relied on receiving proper DNS responses, like 404s or 503s. And just like the response to SOPA, there was significant public outcry, and in fact VeriSign backed down. So they keep trying to do this kind of crap, for whatever reason.

Moving on, Robert Callahan, Prescott, Arizona, with a WPS question: My router has two modes for WPS, the PIN mode and the Push Button mode. The Push Button mode has a two-minute window before it shuts down. Is this second mode secure?

Steve: Okay. It's way more secure.

Leo: Oh. I was going to say no.

Steve: Well, it's way more secure because it only - it is a different four-digit PIN every time. And I guess he didn't say that. He says a Push Button with a two-minute window before it shuts down. The Push Button mode is a four-digit PIN which is different every time it's used, and it only lasts for two minutes. So that mode is more secure. But as we know, the standard eight-digit PIN mode is not secure. Both in the mailbag that I encountered and also some of our topnotch cryptographic security guys who hang out over in the GRC newsgroup, they did some math. And it was interesting to see what happens just with anything that's four digits.

Four digits, as we know, gives you from 0000 to 9999. So that's 10,000 possibilities. Well, so a single guess, a single random guess has a one in 10,000 chance of succeeding. It is surprising how quickly the probability of guessing once right goes up as you get more guesses. Which is to say that, even in the eight-digit case, where you're trying to guess the first four digits and not guessing correctly, it's surprising, if you're able to guess at even a rate of a couple a minute, how quickly the chances of one right guess are. The takeaway from this is four digits is just not enough. One in 10,000 is not enough if someone is going to be allowed to guess for any length of time.

Leo: And as you say, this is not hypothetical.

Steve: Right.

Leo: The tools are out there.

Steve: Right. And they're coming.

Leo: And how fast does Reaver work? Half an hour?

Steve: Like two to 10 hours. So not super fast, but two hours is - it's a matter of whether it gets lucky or not. And a little bit a function of how quickly the access point...

Leo: It responds back.

Steve: Yes, how quickly it recovers from a mistake.

Leo: That's why a timeout is a good thing. It slows it way down.

Steve: Right, right.

Leo: But your neighbor has all the time in the world to crack into you.

Steve: That's, see, it's the static threats that are the problem. And targeted threats. People may believe, I mean, you could have a high-value WiFi access point that is protected with a user key from hell like I have on mine. I can't enter it into any of my phones because I can't possibly type it. Actually that's changed after the Password Haystack revelation. But still, the point is you could never brute-force that. Yet you could have WPS enabled, and probably do, and somebody who had a reason to get into your network, parked out in front of your business, for example, they've got two to 10 hours, especially on the weekend or at night.

Leo: So we may have covered this, but Brian in Saskatoon, Saskatchewan fills in the details of the WPS implementation on AirPort devices from Apple: I was enjoying the podcast on WPS, found the information very helpful, a bit scary. I admit I have always disliked the option of using WPS. I even tell our customers at our store to avoid using it, opting instead to promote a correctly secured network, even if that means going over to the house and setting it up for them. Your closing thoughts were on Apple AirPort and the question we had in our mind of whether it supports WPS. It does, and has since WPS first came out. Its implementation is a bit different, though, as the base station requires that you tell it to accept a new connection from the AirPort utility in Windows or on a Mac and not with just a button press.

So if your neighbor's trying to break into your AirPort, he's got to wait until you say to the AirPort, okay, let's do this thing. Which, if you've already set it up, you probably never will do. So here's how you do it. You go into the AirPort Utility. You pick the base station you'd like to have your device join. Then from the base station

menu you pick "Add Wireless Clients."

Your next choice is to connect by PIN or First Attempt. If you choose a PIN, you enter the PIN of a device connecting, as the Apple base station does not have a printed PIN. When you choose First Attempt, you are then given a screen that shows you the description and MAC address of the device that's trying to connect, which means you can reject the connection if the bad guy was nearby just waiting for you to turn it on.

Lastly, for both options you can add a restriction of limiting the access to a 24-hour time limit. So this is actually kind of handy if a neighbor comes over, a friend comes over, wants to get on. You could set it up very quickly. But you can have it automatically turn off in 24 hours. I prefer this idea as, no matter how much someone was to knock on the door of the network, only I can say "come in." Thanks for the great podcast. Brian. That does seem like a better way of implementing it.

Steve: Apple just did it right. They really did. I mean, the other aspect of this that people have commented on is that, if someone came over, and you wanted to let them get on your network that time, and you had a static PIN on your router, well, they know...

Leo: Forever.

Steve: ...your eight-digit PIN now, exactly, forever. So they could get on even if you didn't want them to get on at some point in the future.

Leo: In fact, that's what I do with my relatives when they come over. I give them the WPA key. And in fact, when you come to our Brick House and you want to join our WiFi network - we have a guest network - we give you the WPA key. So unless we change that on a regular basis, you have now access forever.

Steve: Right.

Leo: Opher Banarie, who is a regular correspondent to The Daily Giz Wiz, he's from Burbank, helps us to recall when lights once flashed: Steve, I've enjoyed Security Now! since No. 1. Hope you and Leo go on for another 20 to 30 years. That's about it [imitating geezer]. You mentioned the flashing lights on the panels behind you. That reminded me of a planned corporate video about our data center. Since I was the sysadmin, HR, who wanted the video to show new employees, sent me the script for review and comments. So here are some excerpts from the script.

Okay. So Script Item 1: Zoom in on flashing lights. Our system has one flashing light. It tells the operator the system crashed. We hope never to see it flashing. Script Command 2: Show spinning tape reels. Our tape drive is behind opaque doors, so no reels are visible. Request 3: Show rapid motion of disk drive heads.

Steve: Oh, that's exciting.

Leo: Our disk drives are sealed and no motion can be detected. Show tracking high-speed printer. Our high-speed laser printer doesn't have a print head. You could show the paper coming out, but it looks just like a photocopier. Here's my favorite: Show punch card in action. We haven't had a card punch for at least 20 years. Maybe 30, in fact. Needless to say, the video was never produced. Oh, how computers have changed. Opher Banarie, Burbank, California, happy SpinRite owner. So those blinking lights behind Steve go back to the punch, almost to the punch card era.

Steve: Yeah, and today they're in black-and-white, even.

Leo: Yeah, they look like they belong there.

Steve: I got a kick out of his post and this script that HR said they wanted for their video because it reminded me, computers used to be physical.

Leo: Right.

Steve: They took a lot of space. You were in their presence; and, like, stuff was happening. I mean, all of the classic sci-fi movies with the reels and spinning back and forth and banks of lights...

Leo: That's where all these shots came from, by the way, the sci-fi. That's where every one of them...

Steve: Yeah.

Leo: Including the hard drive heads.

Steve: And I love that he says, "Show the high-speed printer running." He says, well, it just kind of looks like a photocopier. And it's true. And I guess I feel a little bit the way people probably who are car enthusiasts used to feel because it's been taken away from us. Now it's just all in a black box.

Leo: Solid state.

Steve: And algorithms are really interesting. We're going to be discussing a really interesting set of algorithms next week. I'm actually working on a really interesting algorithm myself at the moment that I'll probably talk about in the future, an interesting challenge of finding the longest repeating strings in a large corpus, which I'm using to eliminate duplicates from the SpinRite testimonials database.

Leo: Ah, clever.

Steve: Yeah, it's because I don't want to have any duplicates. And the way to do it is to find strings that are long and repeated within a large text, which turns out to be very difficult. But it's just changed. Now we just don't have - you're not in the physical presence of a computer. It's like, eh, yeah, here's my phone. It's my iPad. It's my whatever.

Leo: Such a good point. It really has. It really has. And there are computers embedded everywhere that you don't even see.

Steve: Right.

Leo: The physical nature of it. Those lights are PDP-8 lights on the front panel of Steve's PDP-8, which we've described before. Question 5, Paul Brown in Ham, Richmond. He actually sent this via Twitter, so it's nice and short. His Twitter handle is @brownmeister. In Security Now! you mentioned you have a four-disk RAID 6. Wouldn't it be better to use RAID 1/0 as it's three times faster at writes? Why do you use RAID 6, Steve?

Steve: Many people picked up on that, so I just wanted to comment. And others said, well, use RAID 10. RAID 10, as the digits look, is actually a combination of one and zero. Those, zero and one are the lowest level of RAID architecture. Zero is just striping, where you span two drives. And one is mirroring, where you record the same thing on two drives. So RAID 10, which is what a number of people suggested, and probably what Paul actually meant, is both. You're spanning drives for size and then mirroring that span onto another pair for redundancy. So you end up with twice the amount of storage of a size of a single drive.

What RAID 6 does is, given any number of drives, rather than you having a single parity drive, which is what RAID 5 gives you, you have two parity drives, which is RAID 6. And so what this means in practice is that any two drives could fail - or actually, more properly stated, the same spot on any two drives could be unreadable, and you still recover the data despite that. So the benefit of that, for example, over RAID 10 is that, if a particular two spots died on either of two drives, you're in trouble. So RAID 6 gives you the same amount of storage, that is, you end up - in my case, with a four-disk RAID 6, I end up

with twice the storage of a single drive, but double redundancy, not just redundancy where any spot can be read, can be figured out from the remaining drives, but any two of the same area anywhere in all the drives could die, and I'd still get it.

So it's just more redundancy. There's a little more overhead, and people have commented that computing the parity takes time. I'm using a very fast physical hardware RAID controller, and it's got a big buffer that I'm using with battery backup, and it's a write-back cache, so I only have to write to the physical media. If the data in the cache is about to be overwritten, then it writes that back to the drive. So data which is changing often stays in the cache and never even gets written to the drive. So it's very fast because it's got a big cache, megabytes, I think it's maybe 8 or 16MB of cache. It's

lots of cache, maybe even more, I've forgotten now. And so I don't see much write time. But a web server is doing much more reading than writing. And in fact my whole website lives in RAM because, remember...

Leo: Wow.

Steve: Yeah, it does. The actual - I looked the other day, after you and I talked about it, Leo. I have less than 10GB for the entire partition. I mean, the partition itself is 10GB. I'm using four for the data storage of the server, including the web server and the entire site. So that's how lean GRC is. GRC ends up loading up into RAM, and then it's just being served out of the cache during the day.

Leo: You don't have a lot of pictures on GRC.

Steve: Don't have a lot, no. And actually the media is on a separate - is on a sort of partition. And that's, for example, all of the 16Kb versions of the podcast are all on - are not in that same partition. So anyway, RAID 6 is just, for someone who really never ever ever wants to think about their system. I did an actual reboot of the server a week and a half ago because there was something funky going on with our eCommerce, and I wanted to make sure that it was them and not us. I hadn't rebooted for years. That thing is so stable I never reboot it. And I looked at the up time, and it's like, oh, okay, well, it'd probably be good to do it just to dust it off a little bit. So, yeah, very stable.

Leo: Reboot once in a while, once every decade. Not a bad idea to reboot. Isaac Hanna, he's also on Twitter, @isaacrhanna in Melbourne, Australia, tweeted: Any chance you could offer more info on the problem with full-disk encryption and SSDs? This is actually a great question that you and I emailed about some months ago because somebody asked about it. And we ended up getting Allyn Malventano on the line. It's very interesting. And also the issue of deleting stuff on SSDs. TrueCrypt points out that any device that implements wear leveling, which an SSD does, is vulnerable to attack. You could see that on the TrueCrypt site. So can we do full-disk encryption on SSDs?

Steve: Oh, absolutely. And there's no reason not to. The concern is, and this is what the TrueCrypt site mentions, is that if you add full-disk encryption after you have already recorded sensitive data, you cannot absolutely know that the sensitive data wasn't spared out due to wear leveling and not overwritten. So it's very much like the sector sparing I talked about a minute ago with SpinRite, where SpinRite sees a sector having problems, it'll take it out of use and swap in a different one. Well, that out-of-use sector is still physically there. The good news is it's probably hard to read, so that would slow the bad guys down, or the NSA, or the CIA or whatever IA.

So the problem is worse with SSDs because there they may be deliberately remapping on the fly, not just bad areas, but wear leveling deliberately tries not to write to the same spot over and over and over. So TrueCrypt will read a chunk of plain text which is not encrypted, run its encryption algorithm, and write it back to what is logically the place it just got it from. But wear leveling may intercept that so that it's written to physically a different location. So what you encrypted will be read back encrypted, except that it didn't overwrite the plain text of it.

So the lesson is, if you're really concerned about the safety of SSD-based TrueCrypt-style full-drive encryption, install TrueCrypt before first use. That is to say, as long as you have put TrueCrypt on a blank drive, then dump all your valuables on, you're fine. But adding it when you've already got sensitive data on the SSD, that's where the concern is.

Leo: How interesting.

Steve: You cannot know, wear leveling prevents you from knowing that you actually overwrote the sensitive data with its encrypted version.

Leo: So you really can't put TrueCrypt on a drive you've been using.

Steve: You really can't, not and have absolute knowledge that all of the sensitive data has been overwritten with encrypted data.

Leo: Isn't that interesting, huh.

Steve: Yeah.

Leo: Question 7 from Joseph in Los Angeles wonders about WPS and MAC address filtering: I've finished listening to the WPS podcast. As usual, great job of exercising my brain while I exercise my butt at the gym. Of course my Linksys router has the WPS button and no way to disable it. But since I trust no one, I have configured the router to allow only whitelisted WiFi MAC addresses to access the router because I was concerned that WPA would be one day hacked. It's amazing this stuff persists.

Do you think that whitelisting MAC addresses is enough to make my WiFi router WPS hack-proof until the firmware is updated? I'd also be very curious whether the WPS spec automatically whitelists MAC addresses for convenience, as well. Thanks again, Joseph.

Steve: So the WPS spec does not address MAC addresses at all. And unfortunately, MAC address whitelisting is not safe, ever safe, actually...

Leo: Never did anything.

Steve: No.

Leo: It just annoys people.

Steve: Well, the only thing it was useful for is if you wanted to prevent mistaken use of your access point.

Leo: Or casual snoops, people who didn't have any skills.

Steve: And for whatever reason you did not want to use encryption. So if you wanted to have a non-encrypted access point, but didn't want someone using your access point by mistake, then MAC address filtering would prevent the access point from using the traffic. It doesn't prevent bad guys because the MAC addresses are in the air. They are never encrypted. Even if you've got encryption on your network, the MAC address, it's the way the packets get from point A to point B because we're talking about wireless Ethernet.

And so MAC addresses are Ethernet addressing. They cannot be encrypted. They have to be - essentially they're the outer envelope. They're the addressing of the packet. The packet's contents, the envelope's contents, can be encrypted. The outside can't. Which means that a determined hacker could simply watch your wireless network traffic, see the MAC addresses which are being accepted by your access point, and then clone the MAC address for their own use; and it, too, would be accepted by your access point.

Leo: It's just amazing how this MAC address filtering will not die. There's still a guy in the chatroom says, well, it's a useful tool. It's not. It's not. It doesn't do anything. Not a useful tool. The only, yeah, it's useful in this weird situation Steve mentioned where, if you don't want somebody accidentally to use your unencrypted WiFi, I guess it might slow them down.

Steve: The only thing I can think it's really useful for.

Leo: It's not useful, in other words. And it's such a pain because you have to register MAC addresses and...

Steve: Oh, yes. And there are a bunch of hex characters, which is not easy to type. And you've got to figure out what MAC address is and, as you said, Leo, manually enter it, or grab it from the table and then allow it to continue being used. Yeah, it's just a mess.

Leo: So I'll say it again. Because you said it, but I'm going to say it again because this doesn't sink in. Doesn't do nothin'. The MAC address is floating through the air all the time unencrypted, no matter what, easy to capture, easy to spoof. You can do it yourself in your own router. You'll have a setting that says, "What MAC address would you like to be using today?"

Steven McDonald in Scotland comments on today's JavaScript blocking value: Don't know if you know, but Wikipedia shut its doors a short time ago to protest the USA SOPA. Of course. We are, as well. Well, we're not shut, we're just black-and-white. You go to any article, and you're redirected to a dark page. That is, of course, unless you're a Security Now! listener, and you've disabled JavaScript. I'm browsing Wikipedia right now. Page only redirects if you have JavaScript enabled. Well, I guess if you're smart enough to be running NoScript, you probably don't need to be informed about the bad idea that is SOPA and PIPA.

Steve: Precisely. Precisely. So if you've got scripting disabled, you're probably already

clued in to the fundamental problems that this day is dedicated to educating people about.

Leo: If you do have JavaScript turned on, that's what you'll see: "Imagine a world without free knowledge. For over a decade we have spent millions of hours building the largest encyclopedia in human history. Right now the U.S. Congress is considering legislation that could fatally damage the free and open Internet. For 24 hours, to raise awareness, we're blacking out Wikipedia." Then they ask you to enter your zip code, and it will look up your Congresscritter and give you a phone number.

Best thing to do, call that number and say, hey, don't pass, don't vote for SOPA or PIPA or anything like it. I've got my eyes on you. If you pass it, you've lost my vote. And members of Congress, of the House anyway, are all up for reelection this year, and a third of the Senate's up for reelection. So that should actually have - be polite. Be nice. Just say, I want you to know I will not vote for anyone who doesn't protect the free and open Internet. Simple. I like this. So it doesn't work with JavaScript off. But that's probably their intent; right?

Steve: I would think so because you see it briefly, then the black page comes up. And they could certainly have done it differently. So to me it does seem like sort of a soft shutdown. They could have just done - just redirected anything to a page, and you would have never been able to go any further. And I'm thankful. I used it already this morning.

Leo: You know, it really is dramatic. I think of all the sites that could go dark, that is the most dramatically effective because we do, we use it. And by the way, I hope people donated when they were asking for money. It's not too late. You can always donate. I donate every year a considerable amount of money to Wikipedia because it is the single most useful thing on the Internet. If you had to pick one thing. Just fantastic. By the way, NoScript also works to remove the black-and-white and make this show in color. Just in case you want to try that.

Andrew Mason in Adelaide, Australia was slightly disappointed in you, Steve.

Steve: Oh.

Leo: Steve, a few episodes ago someone asked a question about your assembly code being open source, and I was slightly disappointed in your response as it failed to mention open source isn't really about the visibility of the source code. You know, that's actually a good point. I mean, it's part of it, but it's not the only part of it. It's about the license. Just because I can read your source code doesn't mean I'm allowed to do anything with it. Open source licenses list a set of rights that go along - and responsibilities that go along with that source code. Thanks for a great show. Andrew. Good point, Andrew.

Steve: So, yes, and that's why he made it here into the Q&A because I wanted to let people know that I'd forgotten to mention that. And he's absolutely right. I have deliberately open-licensed a bunch of stuff. The Perfect Paper Passwords technology, the algorithms and all that's open. The Ultra-High Entropy Random Number Generator that I developed for the Off The Grid system, all the JavaScript is there and explicitly open. And

the Off The Grid system itself, the architecture, the technology, all of that is open. So when it makes sense for me to give stuff away, I'm more than happy to do that.

Most of my things it just sort of doesn't make sense. And there is a security side. I mean, I didn't open source, for example, the DNS benchmarking tool because it would make it really easy for bad guys to create evil versions of it that look just like mine and that could fool users into using it. So although it's weak protection, it just makes more sense to keep those things which are utilities, which are used on the surface, just as they are. I'm not an open source publisher, but I'm certainly an open concept publisher.

Leo: And conversely, everything I wrote when I was writing software 20 years ago I gave away the source code to, but there weren't open source licenses at the time. So this was 1986, I think. So I just public-domained it, which isn't the same at all. But I did give away source code. So that's not technically really open source. You want to use GPL or the Apache License or there are lots of open source licenses. And that...

Steve: Right, or Creative Commons.

Leo: Creative Commons is a kind of open source license. Yeah, that's a very - everything we do is Creative Commons.

Steve: Right.

Leo: So, for instance, if you decided to take these shows and hand color them and re-release them, you could do that. In fact, I hope somebody does. We're black-and-white to protest SOPA, obviously.

Steve: Be kind. If you hand color them, be kind.

Leo: Make me bright red. Just look at the bug in the lower right-hand corner, and you'll see a website you can go to to find out more, AmericanCensorship.org. Question 10, Mark White in London wonders, seriously, whether governments can break our crypto. This has always been the question. What can those three-letter agencies get up to?

Steve, I recently had a discussion with a friend of mine regarding security and crypto services that are available. My assertion was that by using something like TrueCrypt with a 256-bit AES encryption to encrypt a hard drive or to create an encrypted container with a sufficiently long passphrase, using a combination of upper and lowercase letters, digits, punctuation, it would be impossible for anyone to open via brute force. Furthermore, the open nature of TrueCrypt and the AES encryption cipher ensures that there are no backdoors for anyone to surreptitiously get access.

My friend takes the view that governments simply would not have allowed TrueCrypt or other software to exist without ensuring that there's a way to break the cipher and access the encrypted data. His reasoning comes from his own military

experience whereby he had firsthand experience with some very advanced technologies. While he wouldn't tell me what those technologies were, he did think that government departments like the NSA in the U.S., MI6 in the U.K., will easily be able to access encrypted data, as the alternative would represent too much of a security risk.

We came up with the following thought experiment: The NSA has a securely encrypted hard drive with a Priority 1 order to get access to the data it contains as a matter of worldwide security. Assuming there's no access to anyone who might have the encryption key, is there any way for the NSA to access the data? After listening to several years of Security Now! I simply do not think this is possible. Am I being too trusting of the software? Or is it a safe bet that governments around the world could break into our encrypted files?

I look forward to hearing your thoughts on this. Thank you for all your hard work on Security Now!, for a great tool in SpinRite, and all the great free services at GRC.com. Keep up the great work. Mark in London. There's only one error in his thought experiment. He says that, if he uses a sufficiently secure password, it would be impossible for anyone to open it via brute force.

Steve: Good point.

Leo: And that is not what encryption says.

Steve: True. And so "impossible" is wrong. But the idea would be it would take an unfeasibly long time is the way to correct that one mistake. But there's something else. And so this is a great question. We have seen on this podcast that tools like 256-bit AES are almost certainly absolutely secure. That is, we know how they work. Everyone's been pounding on it. We understand, I mean, it's a simple bit scrambling that you do enough. We've seen reduced-round versions of it where we can sort of - we get a sense for how quickly it gets soft as we do fewer rounds, which tells us how much extra strength we have with the number of rounds we are doing.

So, I mean, it's just like that's just so clear. It seems absolutely verifiably secure. But the way it's used may not be. And that's the key lesson. As we will see next week, there is a problem that we know about with WPS. There's nothing wrong with the underlying crypto, with the hashes, with the secure key exchange mechanisms. It was the protocol which they built on top of those absolutely bulletproof crypto technologies, it clearly had a problem. And the implementation. We saw that routers are not going - they're not going dark, either at all or often for a long enough period to practically prevent brute-forcing. So there was an implementation error at one level. There was also apparently a protocol error that we'll be looking at next week, or protocol issues.

So in the case of TrueCrypt, just the fact that it is open and has been seen and looked at by a lot of people, even that doesn't mean a mistake hasn't been made. BEAST, that we talked about earlier, is another example. There is something that was a block encryption protocol in SSL where, if you could finesse some of the way it worked, you could leverage a weakness in the protocol. So again, nothing wrong with the underlying crypto. But you have to be so, so careful with the way you use it.

And the TrueCrypt guys I'm sure have been. And we know that law enforcement is being

frustrated constantly now by TrueCrypt-encrypted drives. Certainly there is nothing out in common knowledge that allows someone to get into TrueCrypt. If there were, it would be fixed immediately. So could the NSA know something about TrueCrypt we don't? Could, I mean, anything's possible. But it's not the crypto that's being broken. So Mark's original question, wondering seriously whether government can break our crypto, I would have to say no. They're not happy. He says, "My friend takes the view that governments would have simply not allowed software such as TrueCrypt to exist." They don't have any control over that. They're not happy about that, either. The MPAA doesn't have any control over digital content once it gets out of their vault.

Leo: They're trying. Chris Dodd's right now on CNN. Of course, remember, CNN is owned by Time Warner. You ever hear of Warner Bros.? And they're naturally giving the MPAA lots of time to explain why the SOPA bills protect jobs in Hollywood, which is unmitigated garbage. Just sad to see that. And I'll be curious to see if they have anybody on to rebut him. So I'm going to give you some conspiracy theories. You ready?

Steve: Okay, yup.

Leo: You can shoot them down if you choose. First of all, it is why I always say use open source crypto. I don't like closed source crypto because you can't tell if the government has put a backdoor in it. We're presuming TrueCrypt, because it's completely open source, you can compile from source, you know what you've got, we're presuming that smart people are looking at that. I'm not smart enough to know, but smart people are looking at it for backdoors. So let's presume that that's effective. That's not the conspiracy theory.

Here's a couple, though. One, all of this is based on number theory, the simple theory that it is much more difficult to factor a large prime number than it is to create. Right?

Steve: Well, public key technology is. But TrueCrypt does not use public key technology.

Leo: Oh, that's right. All right. But let's, well, we'll use public key as an example. It is possible that some mathematical genius has, in secret, figured out a way to factor large primes.

Steve: Yes. You're right. We know that, if that breakthrough occurs, the world ends.

Leo: And maybe he works for the CIA, and they're keeping it secret. That's conspiracy theory No. 1. Conspiracy theory No. 2 is that there are such fast machines at the NSA - and this, I think, is a given, that they are building the fastest machines money, unlimited federal funds can buy.

Steve: It's the only thing they can do.

Leo: And that maybe they have machines that are so fast that this "unfeasible to crack" has been downgraded to "difficult to crack."

Steve: Yeah, they may have quantum computers...

Leo: We don't know.

Steve: ...that are running that just sort of you hand the problem to it, and the quantum computer says, is that all you've got? Come on. And then hands you back the answer.

Leo: Right. So those are the conspiracy theories. But barring those, I think we can feel fairly secure that - and by the way, they would have to devote significant resources. So unless you are in fact planning to blow up the world, you're probably okay. No one to rebut Chris Dodd on CNN. What a surprise. Time Warner owns CNN. They make movies. What a surprise.

You will see much more about SOPA, PIPA, and the attempt to break the Internet that is currently being proposed in the U.S. and around the world. That's very important. We are going to have more coverage to come on TWiG, on TNT, and Triangulation will be entirely devoted to that. Trevor Timm from the EFF is going to join us in a little bit, Mark Frauenfelder and Rob Beschizza from Boing Boing. Wikipedia is dark. Reddit is dark. Tumblr is dark. And we are black-and-white so that we can continue to give you information, but remind you that we are not safe.

And you should visit AmericanCensorship.org; and, most importantly, today would be a very good day to call your elected officials, whether you're in the U.S. or outside the U.S., and tell them we will tolerate no attempt to break the Internet to protect these old business models. The Internet is making jobs, not costing jobs, in Hollywood and everywhere else.

Steve: Well, and jobs, too, I'm tired of hearing everyone talk about, oh, the job-killing bill and the job-killing this and the job - because we have high unemployment right now, "jobs" is the buzzword for everything. And it's getting overused.

Leo: Well, you want more jobs for filmmakers, actors, and writers? The Internet. Excuse me. Hello. If SOPA passes, there's no TWiT, that's 20 jobs down the tube, including me. And you.

John J. Jobst in Columbia, Illinois comments on the WPS flaw and possible workarounds: Steve, thanks for a highly informative podcast on the latest cyber threat. There are a number of threads on the - I bet there are - on the Cisco/Linksys community support forums talking about the WPS flaw, and naturally no official word from Cisco. Oh, my.

Steve: Huh.

Leo: Most of the advice falls into two camps: Don't worry - what are you going to say? Don't panic. Your chances of someone wanting to hack your router are extremely slim. Or switch to an open source solution like Tomato or DD-WRT, neither of which support WPS. One interesting workaround mentions, if you use WPA-2 Enterprise, which we tell everybody to use, you're safe. But good luck to the typical home network owner setting up a RADIUS server. I've been an enterprise network administrator for years, and I'm sure I could easily implement any of these solutions. But since there are only three houses near enough to me to be barely in range of my Wi-Fi router, I'm going to be just doing nothing. I will look at my logs periodically to see if there are any stray clients. If I find one, I'll mention the FBI and federal anti-hacking statutes to my neighbor, which should be enough to make it stop.

Steve: Oh, by the way.

Leo: Even if I were in an apartment complex with lots of Wi-Fi-enabled neighbors, I wonder how big the threat really is. Are there any statistics out there to say how often the WPS flaw is being exploited? Good question. P.S.: My wife is usually in the room or in the car when I listen to Security Now!. Oh, I'm so sorry. Last week she asked me if I have "that Spin thing," and if I could fix her computer. I told her, hey, I bought SpinRite a long time ago, and it fixed your unbootable computer about three years ago. Unfortunately, her current problem is a defective wireless keyboard. SpinRite I don't think works on that. Keep up the good work!

Steve: No. Can't do anything about the keyboard. And yes, I liked this. I wanted to put it in just to sort of tell people - I think our listeners probably have a good sense. Or if you have something which at the moment is Linux-only, and it takes two to 10 hours in order to get onto someone's network...

Leo: You're not a high-priority target.

Steve: I wouldn't worry about it that much. The big problem is that it's in all routers made in the last few years. And it's enabled by default. And it's not going to go away. Routers, I have an interesting thought, Leo, that router firmware is not self-upgradeable the way virtually all of our other mainstream computer devices are now. Windows, and as we know Google Chrome, it updates itself constantly. Our phones, our pads, our tablets, I mean, everything, we're now in this sort of autonomous update mode. Conspicuously, routers don't.

So it's not possible for Netgear just to push out, or for all Netgear routers to be, like, checking in to see if there's any new firmware for them. And we're probably to the point where, as this demonstrates, it would sure be nice if it would be possible for our router manufacturers to essentially push out a fix by making something available, and have their routers checking in to see if there's an update, and make it trivial for users to do that. But routers are typically - they run without a UI most of the time. So it's not clear how that would work. But it would sure be nice. The problem is we're stuck with an industry full of established routers that have this vulnerability. And it's just not going to go away anytime soon.

Leo: Is he right when he says WPA2 Enterprise is not liable? Or vulnerable?

Steve: Good question. Whether...

Leo: I guess if you used a RADIUS server to do it, you'd probably be all right.

Steve: Yeah, you're probably up at a different level where you don't have the...

Leo: You just don't have WPS. That's the...

Steve: Right.

Leo: If you're doing that, no WPS with RADIUS.

Steve: Yeah.

Leo: Yeah, I mean, I think that's really important because we often, I think, imply that this is a huge security issue. You were on the radio show both Saturday and Sunday to warn people about this. And it may become a bigger and bigger security issue as tools come out.

Steve: Well, there's no doubt we're going to get tools. This is not going away.

Leo: Right. Our final question. Dan in the USofA wonders about audio-to-text conversion: I love your site. I listen often. I was just wondering, how do you create the text transcript of the audio-based show? Steve offers a text file with each and every show at his site, GRC.com. He says: Do you use a free or commercial product to automatically type out a text form of your podcast? Or does someone hand-type it in? Thanks.

Steve: And her name is Elaine.

Leo: Yes. She is not a robot.

Steve: No, she's not.

Leo: She's human.

Steve: Yup. She's very human. She's very good. I stumbled on her. I Googled something

like "audio transcription" or something, and On-Site Media is her company, and it came up. And there may have been some others, but she had a little form you could fill in to, like, request a quote. And I thought, well, okay. And so I did, and I sort of liked that she was technically savvy enough to have a site like that. And, boy, what a win. I've recommended her when people asked for transcripts. She's not inexpensive. Apparently there are send your audio off to China or India or something places. But you get what you pay for. And I really care about quality. Elaine is actively using Wikipedia and Google and the 'Net as she's transcribing the podcast, tracking down the spelling and the location of things and making sure that she's got it exactly right. So, I mean, these are perfect transcriptions. So I just wanted to give her a little shout-out to let our listeners know that there is a terrific service that, if you've got an audio that you need transcribed, there's just none better.

Leo: Well, and that's one of the reasons I really appreciate you, Steve, because you make a lot of extra effort on this show. Not only do you put a lot of work into prepping it, but you make 16Kb versions available, on your own time, on your website. You also make those transcriptions available. You pay Elaine, so we really are very grateful. I know you consider this a significant public service, and you really put your money where your mouth is. So thank you, Steve. I do appreciate that.

You can find those 16Kb versions and transcriptions at GRC.com. That's a good place to ask questions, too. There's a feedback form. That's the way to do it. Don't email Steve. Go to GRC.com/feedback and leave the question there. He can't guarantee a personal response, but the questions that get asked the most, by the most people, are often answered in these Q&A episodes which we do every other show. Next week we will talk more about - what is it?

Steve: WPS Protocol.

Leo: Yeah, okay.

Steve: It's the way - the idea is how do you - they're called zero-knowledge proofs. And if Wikipedia weren't dark right now you could go find out what that is. Very interesting problem in computer science where you want to prove to somebody that you know something without revealing anything about what it is. So you give away no knowledge, yet you prove you know it.

Leo: I know nothing.

Steve: Yeah. But you will in a week, Leo.

Leo: I can't wait. GRC.com, the place to go for SpinRite, as well, world's best hard drive maintenance and recovery utility. There. That's it. That's all you need to know. World's best hard drive maintenance and recovery utility. Steve, thank you for letting us do this show in black-and-white this week in order to, again, underscore the risks posed to a free and open Internet by legislation, not just in the U.S., but all over the world, designed to protect content creators against piracy. It would not do

that. In fact, pirates are never thwarted by these kinds of efforts. But it would break the Internet.

Steve: Right. And that's the other thing we forgot to mention, Leo. It wouldn't work anyway. We talked about blacklisting. This is blacklisting. If blacklisting worked, there would be no spam because we would have blacklisted the spammers, and that would have been the end of it.

Leo: Yeah. So there.

Steve: So, I mean, it doesn't even work.

Leo: Look how spam-free we all are now, thanks to the blacklists.

Steve: Exactly.

Leo: And everybody knows, I hope you know, we've talked about it enough, that blacklists inevitably punish legitimate sites like mine. And so it would in fact, without slowing down piracy in any way, it would break the Internet. It would inevitably bring down sites like Tumblr, Reddit, and Wikipedia, innocent sites. It's just a bad idea all around. They'll come back. They're not done. They'll rewrite, rename. But the motion picture industry, the recording industry will not stop until they get a law like this. We have to say, this and no more. No further.

Steve: And what they will probably do - this will be incremental. We're going to lose this battle a little bit at a time. They bit off more than they should have this time. And I'm sure they got a big lesson on this. So instead it'll come back, and it'll just chew around the edges. And then they'll chew a little bit more, and they'll chew a little bit more. They'll wait a few years, and they'll chew a little bit more. I mean, there is this pressure, unfortunately.

Leo: Oh, yeah. Alas. Thank you, Steve.

Steve: My pleasure, Leo. Thanks so much. Talk to you next week.

Leo: We'll be back in color, full living color next week on Security Now!.