Listener Feedback #136

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-338.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-338-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 338, recorded February 1st, 2012: Your questions, Steve's answers, #136.

It's time for Security Now!. Are you ready, ladies and gentlemen, to protect yourself and your loved ones online? Well, here he is, the man who can do it all, our Explainer in Chief, Mr. Steven T. Gibson. I know. Do you have a middle initial? I don't even know if you do, Steve.

Steve Gibson: M.

Leo: M. "T," I was thinking Tiberius, like James T. Kirk.

Steve: Oh, like that, of course. Yeah, in fact, just last night I watched the very first Blu-ray cuts of the Next Generation series. They're going to be rereleasing the Next Generation with completely remastered, not just up-converting, but they're rematting, at high resolution, all of the special effects.

Leo: That's what they did with the first series.

Steve: And, oh, and the star field looks fantastic, and the ship flying around. Anyway, so they sent out a teaser Blu-ray that has three episodes. And so one of them, actually "The Inner Light" is the one I watched, which is one of my favorite episodes of all time that Jean-Luc did. And so it was fun to see it last night.

Leo: I think, I hope it's not heresy to say, but that might be my favorite of all the series, with Jean-Luc Picard.

Steve: Oh, absolutely. He was the best captain we had. I mean, he wasn't going around bedding all the green aliens, but still.

Leo: Yeah, I mean, look, you can't - Kirk was...

Steve: Kirk was Kirk.

Leo: And Spock. But Data and Geordi and Picard and No. 1, these guys were great. They were really...

Steve: I think the original series that Roddenberry was directly involved in had some classic, really good concepts.

Leo: Right.

Steve: But the writing and the execution...

Leo: It was a little broad.

Steve: ...of the Next Generation, I think was just, oh.

Leo: But that was the time. It was also of an era, and that was the time. I mean, it was the...

Steve: Yeah, and Leo, you know what's sad is we have nothing like that on the air now. There's nothing. For a while we had "Firefly."

Leo: I have to say, "Firefly" to me was even better. I know that's heresy.

Steve: Oh, it was great. It was great. But like this, just, like, here we are, with all this technology...

Leo: "Dr. Who?" "Dr. Who?"

Steve: Yeah, I never - is that even on still?

Leo: Oh, yeah.

Steve: Oh, okay.

Leo: It never will die. I'm not a "Dr. Who" guy either.

Steve: No, it just never got me.

Leo: I don't know. You know me. I've said this before. Science fiction to me is best when read, or listened to on Audible, because your mind...

Steve: [Indiscernible].

Leo: Yeah. And you cannot, I mean, look at "Dune." "Dune" is a great example. Impossible to make a movie out of "Dune." And yet, when you read it, it comes to life. I don't think you need a movie. Just my thoughts. I don't know how we got on this. Ladies and gentlemen, ladies and gentlemen, we are not here to talk sci-fi. If you like sci-fi, tune in to our holiday episode a couple of weeks back. But no, this is a question-and-answer episode, #136.

Steve: It is.

Leo: Yes.

Steve: We have a little bit of news for the week, not a ton. So...

Leo: The weak and the weary, yes.

Steve: And, oh, but before we start, I have a correction to make to last week's "WPS: The Troubled Protocol" episode. I wanted to put it right at the top of the show. And I was mindful of Albert Einstein's famous quote, one that I really like. He said, "Everything should be made as simple as possible, but no simpler."

Leo: It's kind of his corollary to Occam's Razor.

Steve: Yes. And I did oversimplify something. And the reason that was a problem was it changed it in being oversimplified. When I was explaining the protocol and the way the PIN and the nonce are hashed and then sent to the other side and then later the nonce is sent, which allows the other side to verify that the sender had the PIN, it was absolutely crucial that I leave out a whole bunch of things which are also being sent because they're not extraneous, but they would have - there's no way I could have done it without

chalkboard and diagrams.

Leo: I always used to - when I did The Screen Savers, I always used to have a chalkboard for you. Remember we used to do that?

Steve: Oh, yeah.

Leo: We've got to figure out a way. The folks at SMART Board approached me at CES and said, "If you ever want to use a SMART Board...." Now, that might be a good solution because I think that that would be something you could draw on, and then we could get a digital version of it that we could put on the screen or something.

Steve: But we're still largely an audio podcast.

Leo: Yeah, you're right.

Steve: I mean, I know really huge...

Leo: No, no, you're right.

Steve: I mean, in terms of people commuting and driving and flying and all that.

Leo: Yup. No, you're right. Can't abandon them. Can't abandon them. So you've got to do what you can with words alone.

Steve: Anyway, what I forgot, well, I didn't forget it, I mean, I had to strip it out in order to keep this thing manageable, was the very first thing the endpoints do is negotiate a private key. They use a Diffie-Hellman key agreement protocol, which you and I have talked about and described in the past, which is not an authenticating protocol because that's then what they proceed to do with the PIN. But it is a privacy enforcing protocol which prevents a passive eavesdropper from being able to obtain the information that I said last week was possible with passive eavesdropping.

So it is still the case that WPS is not secure against an active attack, that is, a man in the middle who's involved. And even the Diffie-Hellman key agreement won't protect against an active attack. But it absolutely will encrypt the dialogue so that somebody just capturing the packet traffic is unable to, as I said last week, get the data, take it home, and crack the PIN offline. That can't happen because the dialogue is protected by this initial establishment of a secret key which doesn't authenticate, but it does give them privacy. So I wanted to correct that right off the bat. I made it too simple.

Leo: Well, all right. Not an error, exactly, but an oversimplification, I get it, yeah.

Let's see, here. I've got the questions. I've got one commercial. Why don't you launch into the news, and then before we do the questions we'll get the commercial.

Steve: Yeah, we'll do that. So, okay. So I just did want to kind of keep an eye on Chrome. It's continuing to quietly creep forward. Google recently fixed four vulnerabilities in Chrome and acknowledged to have fixed an additional one several weeks ago. So the current stable version of Chrome is now v16. And that's at 16.0.912.77. And of course by the time you hear this, that may have changed again. But that's the nature of the way Chrome is updating themselves. And they're leading the industry in this sort of just automatically keeping it current approach, which as we know, other browser vendors are beginning to look at, thinking, you know, that seems like a good idea. So I think we're going to see other people following that before long.

But I wanted to ask you, Leo, something that I saw that one of SANS's editors said. John Pescatore is vice president at Gartner, Inc. And of course we know them. They've been a market research firm for years. He's worked in computer and network security since '78. And in this most recent SANS newsletter, he said, "The changes in Google's privacy policy are making it questionable whether I want to continue using the Google search engine and the Chrome browser. At some point, the only way to stop the continual ramping up of access to personal data is to vote by your choice of product." And I thought, whoa, okay.

Leo: I'd love to know which product he's going to use because I'll move there, too. But if he's talking about Bing, I think you have exactly a similar situation.

Steve: Yeah. Well, and you really - Google has become one-stop shopping for so many things. I mean, we use it for Docs. I use it for search.

Leo: I think there's been a lot of hysteria over this. And I don't see what Google did as changing the data they collect at all.

Steve: Okay.

Leo: Or changing their privacy controls. I think what they - their privacy controls are superior to anybody's, with the dashboard. You should take a look at the dashboard. Then they're the only company I know of that fully exposes what information they collect about you. So Google.com/dashboard, you can see it all. And what they've done is two things. First of all, they've announced that they will now collate data from all their tools - YouTube, Picasa, search, et cetera - into a single database. That was - if they weren't already doing it, it was for technical reasons alone. Remember, many of these, Picasa and YouTube as examples, were acquisitions. But of course the point of the acquisition - look, Google's not giving you free video and free photo editing...

Steve: Free everything.

Leo: Free everything. They are monetizing you with advertising. That's the trade. If you think Facebook's not doing that, you're not paying attention. So that's the trade. I think they're very clear about what they're collecting, so that is not changed. And they have, for the first time - and this is the other change, so there are two changes. One, they've unified all the data. They've also, as part of that, unified their privacy policy. They have, I think, a very clear, plain English privacy policy. What I would suggest is people read that privacy policy. If you don't like it, there are ways to use Google and opt out. You can log out of a Google account. You remember that most of what they collect comes from the fact that you're using your Google account across all those services. You can delete the Google cookie. And, if you're using Safari or Firefox, you could do anonymous browsing. And you correct me if I'm wrong, but I believe that that prevents the saving of a cookie across sessions and of any personal information across sessions.

Steve: Right, and it will not allow them then to aggregate information about your past history.

Leo: They have no way of doing it because they can't identify you. Now, if they were nefarious, they could, as we know, it's possible to create supercookies that are not deletable and are not trackable and so forth.

Steve: And other kinds of fingerprints.

Leo: Yeah, they could fingerprint you. And to some degree it's a question of do I trust what Google says they're collecting or not? If you do, and you read the privacy policy, and you're comfortable with it, as I am, to me it's exactly what I expected Google to be doing with my information, which is selling it in aggregate to advertisers...

Steve: Anonymously.

Leo: Anonymously - then I'm fine. And then you're fine. If you don't, you have a number of choices, including leaving Google. But I would challenge you in two ways. One is where do you go...

Steve: To replace the functionality.

Leo: Right. I mean, there are engines, search engines that claim to anonymize you. But they're basically using Google in the same way you would if you were doing private browsing. So I think that's the same. And then there are other search engines, but I don't know really what those search engines' policies are. And finally I would say, and I'd love to hear your opinion on this, it seems to me that we already have somebody who knows far more about what we do online, who collects it, we know they do, and who offers it to the government without notice, and that's our Internet service provider.

Steve: Right.

Leo: And they don't have a privacy policy.

Steve: We have no kind of controls over that.

Leo: We don't know what they collect. So I would submit that the best attitude towards this is to assume that what you do on the Internet is done in public, just as what you do in a mall is done in public, or on the street is done in public, and treat it that way. And that will - no matter what's happening, because you don't know what your ISP is doing - that will kind of protect you. That's just my thought. And I've been thinking a lot about it, as you might guess. And I don't want to be apologist for Google. But I think they did the right thing, which is be very clear about what they're doing. That's all we ask. Then you can make the choice.

Steve: Yup. And I guess, by aggregating everything from across their application spectrum, then there's more sort of implicit inter-application knowledge of who we are as we move among their applications so that that's a little more pervasive. But it's all within the Google umbrella.

Leo: Well, remember what Facebook's trying to do. I was talking to my son. He's so smart, 17 years old. And he knows that what Facebook's trying to do is replace the Internet. So he said, oh, yeah, I don't use email anymore. I use Facebook messaging. I don't use instant messaging. And I said, well, you know, they're trying to keep you in Facebook. He says, oh, yeah, I can see that they want to replace everything I do online with Facebook. And it's only a matter - Facebook has its own currency, you know. So it's only a matter of time before they do shopping. That currency could well end up being a global currency that has more value than a dollar.

Steve: Have you seen the projected IPO valuation?

Leo: Right.

Steve: Something like $89 billion out of the gate?

Leo: And we know perfectly well the reason they're valued that high is because they're doing what Google's doing and then some. And what they really want to do is be the entire Internet. So, okay, I agree, if you don't like it, don't use Google, don't use Facebook. Maybe don't go online because your Internet service provider, god only knows what they're doing. That's the price we pay to go online; right? I mean, am I wrong?

Steve: No, I think that's - you got it exactly right.

Leo: You're in public. So if you don't want it, don't use your credit card, either, by the way. You might want to move to Montana, dig a hole in the ground, and get some supplies.

Steve: Not easy to be off the grid.

Leo: It is impossible.

Steve: Yeah.

Leo: And I think Google does a good job of giving you the choice. When people say "No opt-out," well, of course there's an opt-out. There are several stages of opting out of Google.

Steve: It's called wander away.

Leo: You could stop using it. You could log out. I think logging out is a very direct way to opt out. Don't log into your Google account. And if you're really worried, use private browsing. But again, you don't know - I presume not, but you never know - whether they're using some other form of fingerprinting.

Steve: Well, I mean, we have to assume that they're really going to play straight after all the trouble they got into just by over-collecting data from their WiFi roaming.

Leo: They're under intense scrutiny in the U.S. and in Europe, intense. And this is where I always look, but what's the business model? How do they make money? They don't need to use anything more than what they're doing. They have great information. They're telling us, look, we have all these great signals about you. We'd like to use them to make money, okay? And you don't have to say okay. But if you do, they have plenty - most people will say okay.

And I think there's really - the harm is de minimis. So what that Google knows what I search for and then serves me an ad based on it, or what email's going on and serves me an ad. Hotmail does that. Everybody does that. That's how you monetize on the Internet. We've gotten a little spoiled. We expect the Internet to be, you know, everything's free and cool. We have to do advertisements here. Everything has to be paid for somehow. I don't collect information about our users. We have information in our database about your IP address, but we don't use that or quantify that.

But what we do do, actually our advertising agency Podtrac does, is we look at what nations people come from, how much time they spend online, what services they use to download, and then we have a survey which we ask, every year, we ask our audience completely voluntarily to fill out. And they do, very kindly, give us a lot of information about themselves, which is valuable in selling. I think that's the way to

do it. But as long as they're upfront, I think that that's all we can ask. They're being, I think, very transparent.

Steve: I'm glad I asked.

Leo: Yes. I'm sorry you asked. Go ahead.

Steve: No, I am because - no, no, I mean...

Leo: That's my attitude on this thing.

Steve: Several times I had seen this notice of 60 different services being amalgamated under a single privacy agreement, and I thought, oh, I want to see what Leo thinks about that. So...

Leo: I changed - I'll give you a good example. I changed my Facebook status to "single" yesterday and immediately got ads for over-50 singles, lots of them. Lots of them. Dating services for old men. And do you think Facebook - now, do you think Facebook knows anything about Leo Laporte? They don't. But their advertising stuff is set up to look. And the minute you change - just try it. Change your relationship status, see how it changes your advertising. I changed it back, but I just was curious. And, boy, if I were looking for women over 50, I'm set, buddy. I'm sorry, go ahead.

Steve: Okay. On that note, my best title for this next little bit of news is "Duh." This comes to me thanks to a tweeter, Andrew Burns, who tweets as @ErebusBat. From Birmingham, Alabama comes a story: "Personal 401k retirement plan information [from a company called] Regions Financial Corp. current and former employees was lost in November" - now, get this - "when a flash drive with the data came up missing after being mailed by outside auditor Ernst & Young in the same envelope as the decryption key."

They said, "'At this time, we have no indication that any fraud has occurred due to the situation,' Regions said in a letter explaining the data loss to [its] employees. Birmingham-based Regions informed employees of the missing data in a letter dated January 23" - so just last week - "which the company shared after inquiries by The Birmingham News," who is reporting this story.

"The company also shared a copy of a letter sent to its employees by auditor Ernst & Young, which mailed the package with information about the 401k retirement plan participants to another of its offices with the [encrypted] flash drive and the decryption [key] together. When the package arrived, the flash drive was gone, but the page with the decryption key was still there, the companies said in their letters.

"'Ernst & Young takes the security and privacy of personal information very seriously, as does Regions, and we deeply regret that this incident occurred,' reads the letter from the auditor to the Regions employees. 'Ernst & Young is taking steps to prevent this issue

from reoccurring, including providing additional training to the Ernst & Young team that works with Regions regarding the proper handling of confidential information.'"

So the lesson here is, I mean, the good news is they encrypted the information, put it on a flash drive. The bad news is that they sent the decryption key for the flash drive in the same envelope as the flash drive. So when the drive was lost in the mail, they have no idea what the circumstances of that loss were, how the drive disappeared from the letter, and whether the people who have the flash drive decrypted it with the key that was included with the drive.

Leo: Just so you know, here's how you unencrypt it. Wow.

Steve: So to anyone who wants to send encrypted information safely through the mail, send the decryption key...

Leo: Separately.

Steve: ...some other way.

Leo: Even Julius Caesar knew this.

Steve: Oh, my goodness.

Leo: You send the messenger separately from the code.

Steve: Yup. Duh. And in other news, many people tweeted Symantec's somewhat embarrassing news of the week, which was that they, Symantec, doing their due diligence, was forced to acknowledge, when hackers posted the news of this, that six years ago the source code to many of the Norton utilities, including pcAnywhere, was stolen from Symantec's servers. So in SANS...

Leo: Oh, boy.

Steve: SANS Institute, reporting this, said, "Symantec now says that source code that was accessed by cyber intruders puts users of the company's pcAnywhere software at increased risk of attacks. Symantec is urging users for whom the software" - get this - "is not absolutely necessary to disable it until a fix is available."

Leo: As Web3562 says, pcAnywhere is now pcEverywhere. Fortunately, it's been obsolete for years. I don't know...

Steve: I was going to say, it's got a bad - it's had security problems in the past. I mean, and it would always make ne nervous if you had something like pcAnywhere with an

open listening port accepting connections from anyone on the Internet that gives you access to your machine. It's like, just, ooh, talk about goose bumps.

Leo: That's why we - I hope everybody's using GotoMyPC.

Steve: Yeah.

Leo: Because it uses - whoa, there it goes, it blew up. Sorry. I couldn't resist.

Steve: Did you just sink? We need a visual on this, Leo.

Leo: Boom.

Steve: Oh, goodness. For those listening, Leo, before the podcast began, repressurized the ball...

Leo: I did.

Steve: ...that he sits on and bounces on.

Leo: I did. It could explode at any moment. Okay. Continuing - I'm sorry. I'm silly.

Steve: Anyway, so SANS continues: "While the Norton products have been updated and therefore do not put users at risk, pcAnywhere does [put users at risk]. This contradicts earlier statements Symantec had made that its products were not vulnerable due to the theft."

So what happened is, bad guys recently posted that they had reverse-engineered pcAnywhere from the source code which had been stolen six years ago and would now be attacking corporations who were using pcAnywhere. Symantec has verified that the risk is real. So if anybody within distance of this podcast is using pcAnywhere, stop it. Symantec has confirmed that it is not safe. I don't know whether they will be updating pcAnywhere, or they're just simply going to say we have to formally tell people stop using it. But at the moment Symantec has affirmed that it is not safe, that in fact there were vulnerabilities that could be discerned from the source code which allow unauthorized authentication and login to pcAnywhere, which is about as bad as it gets.

Leo: That used to be the king, that program. Everybody used it. But I think it's been a while since...

Steve: I never used it. That just could never be safe. Just too scary.

Leo: Can't possibly. Couldn't possibly be safe.

Steve: Two little burbs from the Twitterverse. Dylan S., who tweets as @NastyMan9, mentioned @SGgrc that Reaver 1.4 is out, and they renamed "Walsh" to "Wash." So that explained that naming disparity that we had a couple weeks ago when you and I were talking about it, Leo, because I was sure that I had seen it as "Walsh," but "Wash" is the name of the pilot of the Serenity starship in "Firefly." And so thus where "Reaver" came from and also "Wash." So somebody had a typo or believed it was Walsh, which was originally what it was named, and that's the WPS scanner portion of the Reaver utility.

And then Jason B. had a nice little mention. He tweets as @AlienCG, and he said, "#SpinRite saved my GF's" - so that's short for girlfriend's - "computer. Nothing bad found, but once she restarted it, it worked. I just bought it for that purpose." So he sent a little note out that he had succeeded.

And since we're doing a Q&A episode this week, I thought I would answer a listener's SpinRite question. He asks about SpinRite and speech. He said, "Hi, Steve. First I wanted to say the podcast is great and has taught me so much. You do such a good job. Also I was wondering, because SpinRite doesn't use the operating system of a computer - i.e., Windows, Mac, et cetera - obviously screen-reading technology [for the blind] is not going to work. I was wondering if there was or could be a way to get SpinRite talking, so people who cannot see the screen can use the program, as well."

Leo: Hmm, interesting.

Steve: "Thanks for an awesome podcast. I've been very educated from all you've taught. Thanks. A. Smith." And the good news is, lots of people through the years have used SpinRite with screen readers because it is, while it's not a Windows or Mac utility, it is a DOS utility, and it brings a copy of the FreeDOS OS with it, which is MS-DOS compatible. But it also runs atop any of the DOS-compatible OSes.

So although it's not something we support out of the box, anyone who wants to twiddle a little bit and can, for example, if you install it on a USB, which is bootable, and also because it's USB it's writeable, if you look, then, at the USB drive, you'll see that there's an autoexec.bat file and a config.sys and all the familiar things from DOS world. And you can certainly add a screen reader to it, and have it install before SpinRite runs, and then get screen-reading stuff to work. And I know for a fact that many people have successfully used SpinRite, now and in the past, with screen readers. So it absolutely is compatible with that use.

Leo: All right, Steve. Let's see. I've got a question file right here, ready for you. Are you ready to answer?

Steve: You bet.

Leo: Let's go to Ottawa for Question #1. John Lockman shares his experience with Reaver. Oh, it's going to be one of those Reaver days, I have a feeling, and WPS.

Steve: Actually not. We didn't - we've already had some.

Leo: Not too much Reaver.

Steve: Not too much.

Leo: I run Linux as my desktop OS, and my wireless card supports packet injection out of the box, so it was little work for me to get Reaver running. I did a quick scan of the APs around me and decided to fire an attack against a few. Oh, my goodness. Now, that doesn't mean he's doing anything bad. He just wants to see if it works. I hope.

I didn't want to wait two to ten hours, really, and I had no interest in these access points, but one I tried returned immediately. Apparently some access points have a hard-coded eight-digit PIN which has been set on purpose. I think that's not unusual. This one had a PIN of 12345670. I'd be shocked if that weren't on purpose. Reaver got it in a single attempt and spat out the WPA key for it, too.

I wonder if Reaver has been coded to try this and possibly other common keys first. I really hope other vendors are not going by this practice. This was a device from a large Internet service provider, Rogers - oh, good old Rogers - so I worry that many other devices may be vulnerable to similar attacks. Disclaimer: Of course I own all those access points I may have attempted this on. So, well, but that was one of the problems with WPS, wasn't it, is most PINs are hard coded. What's interesting is...

Steve: Well, this is another problem, and I haven't mentioned it, but John's point brings it up. It's something that I have known about. All of the PINs are generally hard coded. The problem is that they're static. Believe it or not, Leo, it is the case, and it has come to light, that many routers all use the same one.

Leo: Just as they do adminadmin for their password and all of that.

Steve: Exactly. But this you can't change.

Leo: That's really annoying.

Steve: It's, well, there are several manufacturers that have been identified whose wireless access points all use 12345670.

Leo: Just ridiculous.

Steve: That passes the checksum. Remember that the eighth digit is not actually free to be whatever it wants to be. It's a checksum. So that's the reason they didn't do 12345678, because that would not pass the checksum. But 12345670 does. So they've used that because, oh, that way they don't have to print custom labels on every router.

But, I mean, what this means is that the thing is enabled and has a default PIN, which is also static. So anyone...

Leo: Yeah [laughing]. It's probably printed on the - it's probably painted on the case. But that saves them money, doesn't it.

Steve: It does.

Leo: Holy-moly. Anyway, I'm sure that was hard-coded into Reaver, since they knew that a lot of people use that.

Steve: Oh, it absolutely is, yes. There is a bunch of them that it tries.

Leo: Try that right away, yeah.

Steve: Yes.

Leo: It's easy. It's free. Question 2, John J. Jobst, Columbia, Illinois, provides some insight from pilots and flight attendants. Oh, I love it. We have, by the way, a ton of pilots who listen. I read an article that asked questions like "Why can't I use my device during takeoff and landing?" and provided the answers from pilots and flight attendants. In the case of our devices, they're not really worried about electronic interference at all. They're worried about all those three-pound missiles flying out of your hand during a rough landing and hitting someone. Okay. I'll explain why that's bogus.

They also don't want to be liable for the damages if you simply drop it. And they want you to pay attention to crew instructions should an emergency arise. You can't do that if you have music blasting in your ears or if you're desperately trying to save your spreadsheet before the crash. But rather than explain all this to you they use FUD - fear, uncertainty, and doubt - and say your device can interfere with critical flight systems.

You know, I don't buy it because this all started with electronic devices. And they don't say "Put your Steven King hardcover novel away." In fact, this encourages you to hold heavy hardcover books instead of a Kindle.

Steve: True.

Leo: Which would you rather have hitting you? So I don't buy that. I think that they've never had this policy before. They didn't say put your books away.

Steve: Well, my gripe is that I have always known it's not about interference. So what is it about? I mean, these things do not radiate in any significant way. And now that they're turning it into a profit center by allowing you to use your WiFi, by having WiFi onboard all

the time, it's like now they're admitting that, oh, well, yeah, actually you can use it. I mean, and WiFi is way emissive.

Leo: Right. Bogus.

Steve: So what do you think it is? I don't know.

Leo: I think it's probably just misguided.

Steve: Yeah. So it's a policy. It's easy for them to say. And so it's like, okay, why should we change this?

Leo: Yeah. Why take a chance is, I'm sure, their attitude. And I don't blame them. We certainly don't want to bring down a plane because I was reading my Kindle. I wouldn't want to be that guy. But there's plenty of research that shows that there's no interference, so...

Steve: Yeah, all the avionics is so well shielded and so well designed and expensive because of all of the extra care that's been taken to shield all of the cables and everything as they run around the plane.

Leo: I think it's fine to tell people to turn off their cell phone. That one I can explain, for several reasons. First of all, the cell phone does radiate a lot more. And when you're, as somebody in the chatroom says, at 30,000 feet, it's searching like crazy for a signal. So I understand that. And there's nothing more annoying than that jerk, "Hey, I'm on the plane." Of course they sell their own phone service, so people can still do it, at great expense. So I understand that, and I hope they continue to force people not to use - in fact, I think they should say turn off your cell phone before you get on the plane. Just say you may not use it on the plane at any time.

Steve: Oh, that'd be nice.

Leo: I wish they would do that. But I like to read, and more and more people are going to read on eBook readers. And that's one where you just say that's - I understand, don't put headphones in. In fact, in Canada the law is you have to take out your headphones of any kind. And I think that that's a good law because - during landing and takeoff - because you need to hear instructions, if there's an emergency. So I don't have a problem with that. I don't have a problem with laptops because those are really, if they were flying around the cabin, that would be scary. But what about eBook readers? I've always thought that's - more and more people, I would say in a year or two everyone will have an eBook reader in their hand.

Steve: Yeah. You probably saw the numbers, about the number of Kindles that Amazon sold over Christmas? 177 percent up from the prior year.

Leo: Why not? They're great. Pat Leonard, Tampa, Florida wonders about LastPass and a fake SSL cert. Uh-oh.

Steve: Yeah.

Leo: Uh-oh. Steve and Leo, while I was listening to you record the January 18th, 2012 episode of Security Now!, I was logging into my LastPass account from my school's WiFi. After I logged in there was an error message saying the security certificate could not be verified by LastPass. When I inspected the cert - thank you so much for explaining that could be done, how, and what it meant - I saw that the cert was coming from my school.

My question is, is it possible that my school could have decrypted my LastPass password if I disallowed use of the cert? Does LastPass use a local copy of stored passwords? Or am I or was I in any danger caused by this? I love LastPass. I've been using it since you approved it. I hate to think that my school or other organizations are snooping out LastPass master passwords by reissuing certs. Thanks from a listener since Episode 1. Pat. What's happening here?

Steve: So this is what we've talked about so many times, where there is an SSL gateway at his school which is decrypting encrypted traffic, SSL traffic, in order to provide content filtering so that...

Leo: Many businesses do this.

Steve: Yup.

Leo: Opera Mini does this, not for content snooping, but for compression. So does the Kindle Fire browser, the Silk browser. This is not uncommon.

Steve: So the good news is, the reason I chose and got fully behind LastPass - and I should mention, many people tweet and write and ask if I'm still using it. And the answer is yes. It is I absolutely depend upon it. So nothing that has happened since my analysis and evaluation of it has in any way diminished my love for this solution. And the reason is that it does not depend - or another reason for that is it does not depend upon SSL security for protection. That is, the user's password is hashed in the browser before being sent to LastPass.

So the danger could be, and I haven't thought this all the way through, but I could see if someone at the school were malicious, then they could impersonate the user, and that could be a problem. That is, since they're decrypting the connection between the user's browser and LastPass, they would not be able to get the password, but they would get the hash for the password. And I don't remember whether there's a nonce which is used in the password, and I think there is not. Meaning that what I remember is that the username and the password go through some hashing, and that those together produce the decryption key for the stored library of data, and then it's hashed again in order to produce the hash for the password.

And the beauty of that is that LastPass, that ends up receiving all of this, never has the ability to decrypt the data. So what the man in the middle could get would not be the decrypted data, but they could impersonate the user. And I don't think that lets them decrypt - I don't think what they'd be getting in the wire would ever allow them to decrypt it. But it would allow them to log on. So there might be some risk there, but it's not huge. It's not like all the security of the system collapses in the event of this kind of SSL proxying.

Leo: But they are seeing your password. So if I - right? I mean...

Steve: No.

Leo: They're not - not your LastPass password, but the password and logon to Amazon, for instance, using SSL. Is it not now going through them?

Steve: Oh, other passwords, yes.

Leo: So they don't get access to LastPass, but they get every password you use during that session.

Steve: Correct. Oh, yes. So it's absolutely the case that, in that school setting, you are really having to trust the SSL proxy. What LastPass does is they hash in the browser using JavaScript before it goes over the wire.

Leo: So it's secure.

Steve: And remember that - yes, so it's, like, extra secure. And remember that we also talked about the idea of, wow, that would be a cool way of avoiding SSL proxying man-in-the-middle problems is if the browser hashed the password rather than just sending it - rather than trusting SSL for its protection because, unfortunately, as we're seeing, SSL is not necessarily safe any longer in these sorts of situations.

Leo: It's a common practice in businesses, as well.

Steve: And increasingly common, probably.

Leo: Yeah. But the good news is you can tell because you will get those alerts from a lot of sites saying, hey, this doesn't match. If you ever get that warning, the certificates don't match - I've gone to www.gmail.com, and the certificate is not matching - investigate. Look at the certificate and see. It will tell you. It'll say, oh, Bank of America. You go, oh, if you work at Bank of America, oh, they're watching. But they have the right to do that. We should point out, every court has said this

over and over again. There is no privacy. There's privacy - it's ironic. If you are on the phone, and your boss picks up the line and hears you having a personal conversation, the law says he must hang up. He cannot eavesdrop.

Steve: Yes, yes.

Leo: If you are using Gmail, he can watch everything you say. If you're using Instant Messenger, the courts have said again and again, this is not the same. Just so you know.

Rob Williams, Sugar Hill, Georgia - I just love the name Sugar Hill - had a thought about SOPA: Steve, I'm a longtime listener and grateful user of SpinRite. It saved my butt by fixing my wife's PC a couple of times now. With SOPA in the news and what it proposes to do with DNS, a thought occurred to me. What would stop a website owner from publishing his site's IP address versus its domain name? I mean, DNS translates the domain name to an IP address; right? And that's where the government wants to insert itself; right? So just link to your IP rather than your domain. I'm sure I mustn't have a complete understanding here. I must be wrong; right? It was just a thought. I enjoy your work with Leo and recommend the podcast all the time. Rob Williams. I'm adding that extra little dramatic "I'm sure I'm wrong here; right?" because of course, if such a hole were to exist, it would completely make SOPA useless, Steve.

Steve: Yeah. Yeah. So, okay. So first of all, the good news is I don't think, even with the RIAA and the MPAA and all their lobbying clout and Chris Dodd's sunset provision that prevents him from actively lobbying for two years after he's left Congress, and that'll be expiring soon...

Leo: I'm not lobbying. I'm just talking on CNN, that's all.

Steve: I'm a consultant. I'm a historian.

Leo: I'm a - yeah.

Steve: Okay. I think the notion of the DNS spoofing has been killed forever.

Leo: I think so.

Steve: The DNSSEC argument against spoofing just shoots that one in the head. There's just no way we're going to get DNS spoofing to happen because it is so important that we have the security that DNSSEC will ultimately be providing us, where we know that our DNS has not been spoofed, that no legislation is going to allow that to be changed. So I think DNS is safe. But this is still an interesting question because it brings up some other things.

So, first of all, Rob is right. For example, GRC, 4.79.142.203, that's GRC.com. The problem is, even I don't really have that very well memorized. So it's not at all easy, of course, to memorize IP addresses. Some DNS servers, like 8.8.8.8, which is Google...

Leo: That's easy. That's Google, yeah. Or 4.4.4.4, which is Verizon...

Steve: Exactly. Those used to be the old Level 3 servers, was 4.4.4.1, 4.4.4.2, 4.4.4. and so on. So they chose those specifically to make them easy to remember because - in fact, OpenDNS has some simple ones, too.

Leo: They're not that simple.

Steve: They're not as - they're not as simple.

Leo: I wish they were simpler because I always forget them.

Steve: Yeah. But so it is the fact that the IP address is difficult to memorize, which is the reason we have DNS. However, it is definitely the case that using the IP address will get you to the site. And also places like Pirate Bay or Megaupload or so forth, where there would be an incentive for looking up and writing down the IP address, that's where people would tend to do it. So you could imagine if somebody had some torrent site that they really liked, it would make sense for them to write down the IP address if there was a threat that at some point they might not be able to look it up using DNS. And you could imagine also that there would be - people would be soon pushing around in the gray zone lists of websites and their IP addresses so that people could use those rather than DNS.

Leo: Or buying ads in a magazine. Or, I mean, there's lots of ways to do that. And I bet you there'd be a pretty brisk market in vanity DNS addresses like 8.8.8.8.

Steve: Oh, you mean IP addresses.

Leo: I mean IP addresses, yeah.

Steve: Yes, very good point. So it is the case that just using an IP address does work. It's worth mentioning, however, that DNS does other things than just provide a one-to-one mapping. For example, if you look up the IP address of Google or Microsoft, you don't get one IP. You typically get five or six. And if you look it up again, you get a different one, which is to say that every time you look it up, you end up getting a different IP. What DNS servers do is they can do a round-robin rotation so that, in general, people looking up the IP address will be spread evenly across a set of them. And that has the advantage also that, if one server has an outage problem, then DNS automatically knows to go to the other, which is why we normally get two IP addresses when we look something up, is we have a primary and a secondary DNS server.

Similarly, sites can have multiple IPs if they want to have, like, their traffic coming

through very different routes to get to them on the Internet. Even though they end up resolving to the same DNS name, they could have very different IPs. So there's more services being provided by DNS than just mapping to an IP. But it absolutely is the case, Leo, as you say with your sarcasm, which is quite well justified, that SOPA was just going to be blocking DNS, but it certainly wasn't going to be blocking people from getting to those things.

Leo: No. And...

Steve: And IPs work.

Leo: Right. There's all sorts of ways around it. It was a bad solution.

Steve: Bad idea.

Leo: Although they're working on other things. They've got ACTA now. They'll find a way. They are not done. But I think you're right. I think they're probably done trying to break DNS.

Steve: I think it's, well, and I think, it looks to me like one of the pressure points is going to be search engines.

Leo: Yes.

Steve: That so many people get to stuff through search engines, I mean, it is our index to the Internet, that that is going to be what they try to attack, is say search engines should not return results to questionable sites. It's like, okay, well, good luck with that fight.

Leo: Heh heh heh heh. Samuel Lundmark in Sweden wonders about public key strength. He says: I have some thoughts about PKI strength. We both know that the public and private keys are prime numbers which are multiplied, and that the strength of the system derives from the difficulty of then factoring the result back into the two primes that composed it. And we know that it takes a lot of computing power to create prime numbers in the first place - actually it doesn't, but anyway - which doubtless slows down the process of testing for prime factors. So why can't someone create a database of all the prime numbers that exist in 1024 bits? How many would that be? For example, 1, 3, 5, 7, 11, 13, et cetera. If someone created a rainbow table of primes, how big would that file be? How vulnerable is PKI to rainbow tables of prime numbers? Steve?

Steve: Well, it's an interesting idea. When I was...

Leo: Such things do exist. I've seen such things. Yes?

Steve: Well, yes. And the sense we have, it turns out to be erroneous that there aren't many prime numbers, that is, that they're scarce. Since the prime is by definition divisible only by one and itself, that is, it has no other factors, that immediately rules out all even numbers, all numbers that are divisible by three, and in fact by all other primes up to itself, of course. And so that says, well, if you eliminate even numbers, you got rid of half. If you eliminate every third number, then you've gotten rid of another two thirds, or another one third that you didn't get rid of with the first half. And of course anything divisible by five, you've gotten rid of that. Anything divisible by seven and so forth. So intuitively you think, wow, that must mean that primes are kind of rarefied.

It turns out it's not the case. I saw this myself when I was developing the code for that ultra-high - for GRC's ultra-high entropy random number generator because the algorithm that I used required something called a "safe prime," which is a special kind of prime. A safe prime is a prime number which you would define as 2P+1, where "P" is also prime; and the converse of that, where that prime "P" is called a Sophie Germain prime. And so I needed one which was as big as it could be, that was just less than 2^21 bits. So I needed something that would fit in a 21-bit value for this ultra-high entropy pseudorandom number generator that I developed, which is the technology that underlies the whole - behind the whole Off The Grid system.

So I wrote my own - I wrote some code to go find that prime. And it started at one and spit out safe primes. And I watched it just spit them out, day and night, doot de doot de doot de doot, just kind of marched along. In fact, I got tired because there were so many of them that, instead of starting at one, I started up near where I wanted to finish. And I saw firsthand, to my surprise, how many primes there are. And in fact you can imagine lots of number theory has gone into this. And you can do some Googling in Wikipedia and see that in fact there's just tons of primes. And 1024 bits is such a ridiculously large number that, even if the high bit was always on, then you have 1023 bits of combinations.

And it turns out that there is just absolutely no problem just jumping into the middle somewhere and looking for a prime. Basically what they do is they do prime number tests. They take a number and say "test this to see whether it's prime," which is the strategy that I was using. And there's lots of research that's been done. As you said, Leo, it's not overly compute-intensive to find primes. But the other side is there are way too many of them to build a rainbow table. That is, I mean, you can, and you just - you'll never stop.

Leo: Well, and it wouldn't solve...

Steve: You'll never finish that job.

Leo: It wouldn't really solve the problem, either; would it? Because don't we - we need two primes. What we need is two primes multiplied together to give a larger number. And just because you had a rainbow table of primes doesn't mean it'd be easier to factor that larger number; would it? The issue is what makes it hard is factoring a very, very large number into two primes, the product of two primes into

two primes. So what you'd need is a rainbow table, not of primes, but a rainbow table of numbers created by two primes multiplied together. That would be vast.

Steve: Well, what you could do, if you had the...

Leo: The original rainbow table, I guess, you could in fact multiply them all together; right?

Steve: Well, and if you had the product of the two primes, then you would take the value from the rainbow table, divide it by that, and see if you get a prime out.

Leo: Okay.

Steve: So that would be the approach you could take.

Leo: In fact, that's probably the brute force attack. But that takes a long time.

Steve: Exactly. Exactly.

Leo: Right, that's the point.

Steve: And if there were "not that many primes," then it would work. But the fact is there are just - there's no limit. Well, there is a limit, but it's a huge, huge, number. And, I mean, which is counterintuitive. You would think that, since the definition is it can't be divisible by all those other numbers down below it, and it's up there so high, it turns out there's just still a gazillion of them up there.

Leo: Yeah, that's the issue. There's just so many of them. Andre Cassiram in Winnipeg, Manitoba, Canada wonders about chkdsk and defrag: Steve, I just finished listening to 336, a Q&A episode - our previous Q&A episode, as a matter of fact - and a question popped into my head about hard drives. I've been using computers since MS-DOS, when I developed a habit of performing a disk error scan, a "chkdsk" scan, and defrag at the beginning of every month. I started doing this to minimize disk errors and reduce the chance of disk failure. Probably just increased it, but that's all right.

While I've experienced a hard disk failure, they have been few and far between. I suspect it's because of this habit. I'd like your opinion on this habit and whether there's any need to continue with my perceived preventative measure. Also I've heard that solid-state drives do not require defragging. This may actually harm the drive. Why is that? I'd like to close by complimenting you and Leo on your excellent podcast. Regular user, no computer security credentials, I find your friendly, understandable style a real joy, blah blah blah, keep up the good work, accents, blah

blah. Steve and Leo, thanks for all you do. I skip through that stuff, all the praise. I blush.

Steve: I sometimes want to cut it out, but I think, well, then I'm not really posting the question, so...

Leo: Well, yeah. But it's...

Steve: Okay. Okay.

Leo: But anyway, that is great. I've wanted to ask you this for ages.

Steve: I would call running a chkdsk and a defrag a "poor man's SpinRite."

Leo: Yeah.

Steve: It actually is useful. Remember that - and the reason he was put in mind of this is it was two weeks ago that I explained what it was that SpinRite does in answer to one of our listener's questions, who said you keep talking about it, but you never talk about what it actually does. The value is in making the drive read its own data because that's when it discovers that it's got problems with a sector. It doesn't know unless it tries to read it that it's got a problem. And error correction is employed all the time now because the densities are so high, the drives are depending upon it. It's when the problem gets near the point when it might not be able to correct it if it gets any worse that it then says, ooh, relocates it to a good spot, and marks that sector bad.

So the fact is, if you did a chkdsk, which thrashes around the drive and reads the metadata, the file system data, and a defrag, which has the effect of pretty much moving everything around by visiting everywhere, picking stuff up and moving it, I call that a "poor man's SpinRite" because you are essentially telling your drive to read pretty much all of the disk and write it back down again.

Leo: You're trying to break it, basically.

Steve: Yeah.

Leo: But doesn't it - now, I'll be honest. People often talk about defrag, and on modern operating systems defrag doesn't have any real purpose. And doesn't it thrash the drive? I mean, aren't you really thrashing the drive in that case? Defrag is different from chkdsk, or SpinRite, where you read-write, read-write, or maybe don't write, just read read read read read. Defrag's moving stuff around like crazy. It's doing a lot of drive access.

Steve: Yeah. I'm not a big fan of defragging any longer, for exactly that reason.

Leo: You don't need it anymore, yeah.

Steve: And to answer Andre's question about why SSDs should not be defragged, and he is correct, remember that SSDs, first of all, being non-physical, there's absolutely no wear-and-tear if files become fragmented. That is, arguably, if you had a really badly fragmented hard drive, and you were reading those fragmented files, then it is more work for that drive to have its head jumping all over the place, following the path of a single file which has been fragmented, than if it were defragged, and the head was able to just stay in one place and just slowly click along through cylinders as it reads a long file. So SSDs don't have that problem, being completely solid-state. They do have the problem that they are fatigued by writing. So you do not want to defrag, exactly as you said, Leo, an SSD. Not only is there zero benefit, but it is actually detrimental because they don't like to be written.

Leo: And they're random access. So optimization doesn't make any sense.

Steve: Correct.

Leo: It's a meaningless idea.

Steve: It is the case, however, that running a SpinRite Level 1 pass over an SSD is good for it.

Leo: Oh, this is good to know. This is new information. Tell us about that.

Steve: This is new. I have never said before. But in reading Andre's note and thinking about it, I thought, oh. And thinking about what I said two weeks ago, SSDs also have error correction. SSDs, as we know, develop problems over time. And just like with a hard drive, you need to read the data from the SSD in order to show it that it has a problem. So SpinRite's Level 1 is a read-only scan, and doing that on an SSD makes a lot of sense. Do a read-only scan of an SSD, it'll show the SSD's controller that it's got a problem reading a sector, and then it'll map that out or rewrite it in order to strengthen that sector, if possible. So that ends up being a value for SpinRite on solid-state drives.

Leo: And the reason solid-state drives wear out is writes, not reads; right? You can read it indefinitely.

Steve: Yes.

Leo: It's just the writes that are a problem.

Steve: It's because the technology is a small conductor which carries an electrostatic charge. So there's, like, electrons stranded out on this little conductive island. And the technology is able to sense the charge so that you're able to sense the charge without doing any work. But in order to drain the charge, since this little island, this little floating island of conductive material with electrons, you need to break down the insulative barrier. And you use high voltage to do that. There's actually what's called a "charge pump" in SSDs where they actually pump themselves up to a much greater voltage than the five volts they run on, and then they use that voltage to break through and essentially break the resistance of this barrier, break the insulation, and pull the electrons off when they want to set it to zero. And similarly, they break through it to push electrons on.

What happens is that's the problem, is over time breaking through that insulation fatigues the insulation, and it starts leaking a little bit. And so the SSD will detect it and go, whoops, we've got a problem. And that's where it'll take that out of service and map in some spare space. So it's the writing that does fatigue the actual storage mechanism of the SSD, which is not a problem that hard drives have.

Leo: Right. Tom Walker, Littleton, Colorado wants to know about the WPS button: I listened to the entire show - by the way, Steve, great podcast - listened to the entire show about the WPS PIN vulnerability. Seems to me this vulnerability would be present only on routers that don't have a button, but still have WPS. Isn't the purpose of the button to temporarily turn on WPS? How can a hacker in the apartment next door hack my WPS PIN if he can't press the button to enable the two-minute WPS access? That's a good point; right?

Steve: Wouldn't it be wonderful if that were so.

Leo: Oh.

Steve: I only addressed one aspect of WPS when we've been talking about it, which was the Reaver-oriented, PIN-hacking remote exploit. There are, in the WPS spec, a number of other ways for WPS to work. There's actually already a near field technology defined for WPS, where, for example, at some point in the future, when our smart phones have near field technology in them, my new BlackBerry Bold does, and when our access points have near field technology, you'll literally be able to just knock your phone against a spot on the access point and instantly configure its WiFi. That's in the spec already.

There's also what they call "out of band synchronization," for example, using USB, where you would briefly connect your device through USB, and there's a WPS support for USB protocol to send the information through the USB channel, so it's not going through the air. That's another means of configuring WPS, already in the spec, just waiting for somebody to use it. The fourth approach, skipping the WPS approach we now know of, the fixed-PIN approach, the fourth approach is the pushbutton approach. And that works without a PIN. So it isn't that it enables the PIN, it is PIN-free, which makes it troubling for a whole 'nother set of reasons.

Leo: But you're only vulnerable for two minutes.

Steve: Yes. So the idea there is you press the button on the router, and you walk over - remember I did mention it briefly, they call it the "walk time." You then walk to the device you want to configure, and you press its button, or its equivalent, and both devices then are supposed to see each other and automatically synchronize themselves, automatically pair, but only if neither of them sees anybody else. And so that's the protection against...

Leo: Ah, that's clever.

Steve: It is clever. And it, like, still gives me the creeps because it's like, oh, that doesn't seem very safe. So, yes, just disable WPS if you can. Oh, and I should mention, Cisco has provided an update to all of their Linksys owners, not firmware, but news of when that will happen.

Leo: Yeah, yeah.

Steve: Some time in March.

Leo: It's ID 25154 on the Cisco Knowledge Base. And they say the first firmware will be to disable WPS. Not to fix it, just to disable it. And they say there is a workaround. You can disable WiFi. So...

Steve: Do they really?

Leo: Yeah. Workarounds. It says, "Not all workarounds are available or practical for all customers."

Steve: You could also unplug it. Just pull the plug.

Leo: Yeah. It says "Disable wireless radio. For customers not using the wireless function, disabling the WiFi radio will alleviate exposure."

Steve: Well, that's a good point, I guess.

Leo: Yeah, yeah. Moving along.

Steve: True enough.

Leo: True enough.

Steve: And don't let anybody press the button. Don't let any strangers come into your

house...

Leo: And press your button.

Steve: ...and press the button and then leave.

Leo: And then walk away.

Steve: That'd be bad, too.

Leo: Thomas Paulson in Nordland, Norway asks: So, is WPA cracked? Steve and Leo, longtime listener of Security Now!. I regard your expertise as my one-stop shop of all things security related. I'm sure you get a ton of email, if email has weight, about cracking this and that. I'll try to make this brief, interesting, and to the point.

In online forums I hear a lot of people claim, greatly convinced, that WPA and WPA2 have been cracked and are insecure. But I haven't had anyone produce any convincing evidence. I searched the 'Net, couldn't find any reliable resources. Searched YouTube, found a lot of videos showing how they supposedly cracked WPA by using a few Linux commands, but a video is easily faked. I remember 170, November 2008, where the TKIP hack was dissected. Since then I have not heard anything about WPA in fact being cracked. Did I miss it? Are people wrong in assuming that WPA/WPA2 is vulnerable/cracked?

I mean, as far as I know, the only way to crack my WPA2 secured WiFi network would be a brute force attack, which would take just about forever given a passphrase of significant size. I ran mine through your Password Haystacks. And even in the "Massive Cracking Array Scenario," it would take 1.91 million trillion centuries - I'm sorry, underestimated it. 1.91 million trillion trillion centuries to guess.

If it's broke, I would think the Internet would be swamped with news stories and high-profile security experts such as yourself confirming the fact. But I don't see that, and I won't believe it till I hear it from you. Thanks for creating the wonderful show. If my life were limited to a single podcast, it would be Security Now!. Best regards Thomas Paulson, Norway.

Steve: You know, I saw this, and I wanted to include it because I see the same nonsense.

Leo: Again and again.

Steve: I know, in forums. And I saw it in the last couple of weeks when I was doing research on the WPS stuff, these anonymous weenies, who I guess impress their family members...

Leo: I cracked it, heh, heh.

Steve: Yeah, with their supposed knowledge. And they just sit back there and say, oh, WPA's been cracked, hah hah hah.

Leo: That's what it really is. It's kind of this know-it-all thing. Oh, yeah, no, I know that.

Steve: Yeah.

Leo: I read that in an article once.

Steve: Well, so Thomas and everybody else, nothing has changed. WPA and WPA2 have not been cracked. The only little chink in the armor of WPA was exactly as Thomas remembers, which was that the TKIP, the Temporal Key Integrity Protocol was - it was very cleverly jimmied a little bit by some developers who figured out that they could decrypt very short packets only of the sort that maybe the ARP protocol would use. Nothing further ever came of it. You can't do more than that. You can't decrypt large packets. There just isn't really any practical way to leverage that. And WPA2, which uses the Advanced Encryption Standard, the AES, is absolutely, exactly as Thomas says, uncrackable. The only known exploit is going through the front door with a brute force attack and trying, exhaustively, every possible passphrase on a packet that you captured in the air. And so it is not the case that WPA and WPA2 have been cracked, despite what you see posted by weenies in forums.

Leo: So in fact we say, if you want to secure a wireless router, make it as secure as anything wired, use WPA2, right, at AES.

Steve: And the only known problem is if you used a really dumb...

Leo: And a good password.

Steve: ...password.

Leo: Yeah, don't use 1234567 as your password.

Steve: Do not.

Leo: And if you have WPS, turn that off. Nathan Agius - right? Because WPA, I mean, WPS will bypass the WPA passwords, no matter...

Steve: Right. What was so clever about WPA was that it still used the RC4 cipher. And RC4 is itself not insecure. It was that the WEP implementation of it was so poor that there were all kinds of ways to crack it. So but the problem was, back then, when we were trying to get away from WEP as fast as possible, there was a lot of old hardware that wasn't strong enough to handle a much more powerful cipher. So they used this Temporal Key Integrity Protocol, basically came up with a clever way of reusing RC4 and solving the WEP problems, but still giving us really good strength. So that was a long time ago. Now, in this day and age, everything supports WPA2. So as you said, Leo, disable WPA, everything should work just fine.

Leo: Nathan Agius in Sydney, Australia is looking for an alternative to GoDaddy: Hi, Steve and Leo. After recently listening to you and Leo complaining about GoDaddy multiple times and the fact GoDaddy was in support of SOPA, I decided to move away from them. I signed up with Hover - good, that's one of our sponsors - for some domains, and I want to move my main ones away soon.

The problem is I'm using GoDaddy's hosting on two sites, and I don't feel comfortable with just picking a new hosting company randomly. Do you have any advice? My first thought was to go with TWiT sponsor Squarespace, but unfortunately they do not allow server-side code in PHP to be uploaded by me. Can you suggest - I'm not surprised. Can you suggest any Linux-based hosting with PHP support? Thanks for your time and a great show. P.S.: For years now I've been swapping the contents of all my drives onto new media and back every six months due to bit rot. You woke me up to this years ago. Great advice. That's an interesting - I never heard of that. Did you recommend that, swapping it?

Steve: No.

Leo: But it's a good idea.

Steve: It is. I mean, you could also run SpinRite, or you could...

Leo: Yeah, same idea.

Steve: Just do something that reads the drive. Reading the drive allows it to see it's got problems.

Leo: Do you have, I mean, you have used power hosting. You do your own hosting through Level 1; right? Or something like that. What do you do?

Steve: Yeah, well, I've got my own servers at Level 3.

Leo: Right, Level 3. Level 1. Level 3, yes.

Steve: And all of my server-side stuff, of course, is in assembly language. But I didn't

know if you had somebody. But I would say DreamHost is a really strong hosting provider. And, I mean, they're a real propeller-head provider. They do, and I checked, allow you to do your own server-side PHP5 stuff. And they've got great packages. They've been around forever. And they give you a whole bunch of different plans and access to essentially virtual private servers running Linux or other OSes of your choice. So if nothing else, DreamHost. But maybe somebody in the chatroom has a recommendation, or I thought maybe you might. [BlueHost is good. Elaine]

Leo: Yeah, I like DreamHost fine. They did get hacked recently, but...

Steve: We talked about it last week.

Leo: Everybody does.

Steve: Yup, exactly. And they were as responsible about it as they could have been.

Leo: Right. I mean, the truth is that's why Squarespace doesn't allow you to upload, side load PHP code. When we've been hacked - we've been hacked, what, two or three times at TWiT, and it was always PHP code. That is kind of inherently risky. You have to know what you're doing if you're writing PHP code and uploading it.

We use a company called SoftLayer for our hosting. And basically, I mean, we use it as a dedicated server hosting. So in other words, that server is all ours. We have six of them. We have a MySQL server, we have divided up - much like what you would do yourself, Steve, you have your own hardware running in your own area with bandwidth provided by Level 3. We just - our hardware we don't own. We lease it from them, and it's in their cages in Dallas and Seattle. We like the fact that it's multiple locations. We like the fact that they have gigabit and hundred megabit connections to the outside world, better than we've got. So, I mean, I don't have - I couldn't afford a gigabit connection here. We have 150Mb, but I'm not going to use that for servers.

So we just do it at SoftLayer, and they're fairly affordable, and I think they're good. They, I believe - now, one thing to describe and maybe to help people understand, there's managed and unmanaged hosting. Ours is unmanaged, which means we have our own sysadmins. They're responsible for security and maintaining it. SoftLayer doesn't look over our shoulder. They basically give you a box with a connection and say, "It's all yours. Do whatever you want." For some people, that is not what they need. They need more handholding. They might want somebody to manage it at various degrees. I'm pretty sure you can get managed hosting, as well, from SoftLayer, at a price. DreamHost is I'm sure managed. It's rare that you'll find a hosting server that's - unless you have a dedicated host, dedicated server, rather, that will say, hey, do whatever you want, because you're on the same box as a bunch of other people. So I'm sure DreamHost is managed. And for most people that's what you want.

Steve: Yeah.

Leo: Peter McDonald in Scotland - and I do, by the way, no hesitation, if you want a good company, I love SoftLayer. We don't get a deal with them. We pay full price. We pay thousands, I think 4 or 5,000 a month in server costs. But they are great. They've been very responsive whenever there's a problem, and I've been very happy with SoftLayer.com.

Peter McDonald in Scotland shares his thoughts about self-updating routers: In Security Now! 336 you said it was a shame that routers don't - or in Scotland they probably call them "rooters" - don't automatically update their firmware. I work for a major U.K. ISP who supply rebranded Thompson and 2Wire routers to their customers. Both of these routers do, in fact, automatically update their firmware. When they're plugged in for the first time, they register with the network on the ISP side. When a new firmware is released, a batch of routers are upgraded to ensure that, if there is an issue, not all are affected. Once it's been proven there are no issues, the rest of the routers get updated in large batches.

Granted, these are routers with customized firmware on them, written by the router manufacturer to our, the ISP's, specification. But there is no reason why they couldn't do the same for public routers. There are two issues, however. First, how do you handle a bricked router? If there are any issues during a firmware upgrade, the router could become unusable. If the consumer did not know of the upgrade, they may just think it malfunctioning and start rebooting midway through the upgrade. There's one way you could brick it. Secondly, some customers - and I think that's probably the best reason, because during a firmware upgrade the router will not be working. And if you rebooted it then, disaster.

Secondly, some customers really do not like the device updating itself. What can and does happen a lot is the new firmware will break some functionality that hasn't been fully tested. This results in dissatisfaction and complaints for the company. This happened recently at my work, where a firmware upgrade stopped IPSEC VPNs from working. Ouch.

Steve: Well, there is, I think, probably in the future, we're going to see routers, rooters, whatever you want to call them...

Leo: It's funny because you don't call them "rooters" in Australia because if you did, it would be dirty.

Steve: Yeah.

Leo: But we call them routers in the states, and I know in the U.K. they call them "rooters." So just so you know. I think we've covered both pronunciations by saying so.

Steve: There is longstanding technology for embedded systems where you have something called a "watchdog." And the watchdog is a hardware timer which, if the router is working correctly, in one of the router's execution loops every so often it goes and resets this timer, so that the timer is never allowed to expire. And if the timer ever expires, that tells it that there's a hang somewhere. And so in embedded systems it'll

reboot the device in order to wake it up and pull it out of this hang.

So it's entirely possible to imagine a router which would be even safe, could be made safe against this kind of vulnerability, that is, the problem of, like, being reset in the middle of a firmware update or something, by giving a watchdog timer the ability to reflash the firmware from a master copy in ROM. So there would always be a good, known, fallback firmware that the router could come back to, if in the process of getting itself updated something happened, or the new firmware was properly flashed, but then ended up having a problem and the user said, whoops, just press a button in order to fix the router.

So you can imagine workarounds. Maybe it'll never happen. Routers are so inexpensive, no one wants to add the additional cost. But we sure are seeing a situation here where it would be nice to have some means of reaching out and updating - god knows how many wireless routers have this WPS vulnerability that's just going to be there forever.

Leo: Yeah. Sigh. Rick Huebner in Melbourne, Florida shares some tips for using TrueCrypt: Steve, in Security Now! #337 you mentioned the person accused of mortgage fraud and being compelled to provide their password to decrypt their laptop. I'm an avid user of TrueCrypt, and I have my laptop drives whole-disk encrypted. For several years now TrueCrypt has offered the option of replacing their boot-time display text with your own text. This is limited to something like 30 characters, but I found that the best prompt, instead of that glaring TrueCrypt prompt, was to put in something like "Missing ntoskrnl.exe," or just a blank screen. This gives the impression that the hard drive's dead and tends to provoke a compassionate response instead of an adversarial response to an encrypted drive. I mean, come on, who sees a safe and doesn't wonder how much cash and drugs are stored in it? Remember Scarface? I think this, combined with either encrypted virtual machines or the hidden volume/operating system should provide enough deniability for all but the super spy.

Steve: I really - I like Rick's thought. And it actually mimics what I have done in the past. My feeling is you really gain nothing if your boot-up screen says "Nanny nanny nanny, you can't guess my password."

Leo: Good luck.

Steve: It's just going to piss off somebody and induce them to try, or maybe they'll just throw the machine down on the ground because they're upset or something. I really much more appreciate sort of the Aikido approach of just sort of saying, exactly as he suggests, something to indicate that the system is not functioning, like "Missing ntoskrnl" or "Missing operating system." Just say "Missing operating system." Lord knows that's the horrible message we see sometimes when we're configuring systems, and the BIOS tries to boot from the wrong drive, or we leave a USB dongle in, and the BIOS tries to boot from that. And so, I mean, it would stop somebody so that they wouldn't even go any further.

Now, it would not stop the FBI because anyone forensically looking at the boot sector would immediately recognize that this is a TrueCrypt boot sector which has been configured to display this message. So up at the high level it's not going to stop anybody. But I do, I really - I loved him saying it provokes a compassionate response, rather than

one that's adversarial. And I say, why not go for that? Do not taunt somebody who you're trying to keep out of your drive. That's just never going to have any benefit.

Leo: Finally, our last question, from Andries Strauss in Centurion, South Africa. He is wondering about cooling down phone batteries: Steve, you've shared a lot regarding phone batteries lately, which is always very interesting. I'd like to know, is it okay to mount my iPhone on the air vent of my car's air conditioner? The issue is I use my iPhone as a GPS device while driving, and I have it mounted on a suction-cup cradle, leaving it exposed to direct sunlight. It's also charging while in the car. After a while the screen goes darker, making it difficult to see the route. This, I found, was because of the phone heating up.

I then have to remove the phone from the cradle and cool it down by holding it directly in the air flow of the air conditioning, not exactly the safest operation while driving. The other option is to set the air conditioner to blow air from below the front windshield so more cool air reaches the phone - but not me. I've seen various types of cradles which will allow you to mount the phone directly on the air vent grill. Is this a good idea, though, to have the phone permanently, directly in cool air?

Steve: It is a fantastic idea.

Leo: Couldn't hurt.

Steve: And, no, actually more than that, Leo. One thing in all of our discussions that I also have meant to say, but it kept slipping my mind, is temperature. Lithium-ion batteries hate the heat. It is absolutely destructive to them, to the degree that mature technology, responsible technology will not have anything to do with a hot lithium-ion battery. It will absolutely shut down. It won't charge. It won't discharge. It'll just say we're not doing anything until this battery cools off. It is crucial that lithium-ion batteries not be allowed to get too hot. And it's something that I had forgotten to mention.

But in terms of our general sort of ongoing series on care and feeding of contemporary lithium-ion battery technology, temperature really matters. So, for example, do not leave devices sitting on your car dashboard. Obviously it's not good anyway because bad guys can see them, and that gives them an incentive to break a window and reach in and get it. But you do not want them to heat up. It will age the battery very quickly. So absolutely, keep things out of direct sunlight because that allows them to get very hot, and they don't like it.

Leo: Yeah, sunlight's bad. In fact, the iPhone has a warning, which I have seen, that will pop up. It will actually shut down and say it's overheated and will stop working.

Steve: And I've had that with my iPad, as well, yes.

Leo: Right. So, yeah, you definitely don't want to overheat that. And, hey, think about all the computers that for years sat in air-conditioned, sealed chambers. That's what they want.

Steve: Well, yeah. But even more so, chemistry wants that. I mean, our batteries are goo-filled. They've got all this chemistry going on in there. And it's that chemistry that really is heat-sensitive.

Leo: Right. Steve Gibson is not heat sensitive. But he's liable to strip down if it gets too warm. He is our...

Steve: Hey, I've done this podcast with a fever, Leo.

Leo: Yes. You know what? Let's give you some credit. Last week Steve was walking wounded, and he did not indicate in any way that he was in pain. I guess he got some food poisoning or something.

Steve: Had a 101-degree fever. I took my temperature afterwards, and I thought, whoa, well, the podcast must go on.

Leo: I'm impressed. In future, please do not do that. Just tell me. We'll reschedule. Anyway, thank you for letting us reschedule. We did this show a little bit earlier. Normally we do it Wednesdays at 11:00 a.m. Pacific, 2:00 p.m. Eastern at TWiT.tv. But you know what? We make sure that you can get it in any way you want. You can watch it on Roku. You can watch it on many devices. You can download video from iTunes or just from our site, TWiT.tv. And Steve even offers, I don't know - how many downloads? Do you have counts of downloads for 16Kb versions?

Steve: Oh, yeah. I haven't looked at them for a long time, but we get thousands of downloads.

Leo: Thousands, wow.

Steve: And I bounce them through Podtrac so that Podtrac can count them, too.

Leo: Thank you, we count them. But for those of you who really want a small file, I mean, 16Kb is about as small as you can get and still have audio. There is a text transcript, as well, which is even smaller. All of that, the bandwidth-impaired stuff you'll find at GRC.com, Steve's site. A great place, too, if you want a question on our next Q&A episode, to go: GRC.com/feedback. There's lots of free stuff at GRC.com, too, you might want to check out. But of course let's not forget SpinRite, the world's best hard drive and now solid-state drive maintenance and recovery utility. Couldn't do any recovery on there, probably, but you could exercise it in a safe way.

Steve: Well, I would imagine some future version will be in my...

Leo: Really?

Steve: Oh, yeah. We're not done.

Leo: Good on you. Yeah, because I don't want, I mean, I don't want solid-state to put Steve Gibson out of business. That would be bad.

Steve: Nope. I don't think that'll happen.

Leo: All right, Steve. Well, I'm glad you're feeling better. Don't eat at that place ever again.

Steve: Nope, not going back.

Leo: Thanks, Steve. Thanks, everybody. We'll see you next time on Security Now!.