Calm Before the Storm

Description: This week, while waiting for news from the upcoming Black Hat and DEF CON conventions, we discuss another terrific security eBook bundle offer, a Net Neutrality follow-up, a MySpace account recovery surprise, another new feature coming to Win10, the wrong-headedness of paste-blocking web forms, Australia versus the laws of math, does an implanted pacemaker meet the self-incrimination exemption, an updated worst-case crypto future model, a surprising find at a flea market, another example of the consumer as the product, a SQRL technology update, and some closing-the-loop feedback from our terrific listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-620.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-620-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with lots of security news. Next week, of course, we'll have Black Hat. This week we're just getting ready for it. We'll talk about all sorts of problems and patches, questions from our audience, and a whole lot more. Here's a question: Do ones weigh more than zeroes when it comes to hard drives? It's coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 620, recorded Tuesday, July 18th, 2017: The Calm Before the Storm.

It's time for Security Now!, the show where we protect you and your loved ones, your privacy, your security, help you understand how technology works, throw in a little sci-fi and games for fun, and that's all because of this guy right here. This show really is Steve Gibson's show from GRC.com. Hi, Steve.

Steve Gibson: Leo, great to be with you again, as always.

Leo: Nice to have you. We should call this just The Steve Gibson Show. I think it would have done better, frankly, had we.

Steve: We didn't know nearly 12 years ago - actually, nearly 13 years ago. You realize we're coming up on, we're closing in on the end of year 12 at the end of next month, end of August is when that happens. So, yeah, we didn't know how it was going to evolve. And of course it's become, well, many people's go-to weekly hit on what happened

during the week.

I titled today's episode, which is No. 620, "Calm Before Storm" because nothing earthshaking happened. But toward the end of the month, as we mentioned last week, we've got Black Hat and DEF CON conventions occurring one after the other in Las Vegas. And they always produce a bunch of really interesting news. And so there is sort of a sense of - you know how all the water disappears from the beach, and people go, where did the water go? Well, yes, that's because the tsunami is approaching.

Leo: It seems so calm.

Steve: So we're going to discuss another terrific security-related eBook bundle from that Humble Bundle that we've discussed before. I tweeted it to our listeners and already got a ton of good feedback, so I want to make sure that the rest of our listeners who are not Twitter users know about it.

I've got a little bit of a Net Neutrality follow-up from all of last week's events, just sort of a non-partisan take on what I think needs to happen. There was a MySpace account recovery surprise, and not in a good way. Another new feature coming to Windows 10 Creators Edition later this year, but it has appeared now in the latest builds. We're going to talk about the wrongheadedness of paste-blocking web forms, which is something that's been going on for years. Our listeners have, like, asked me what I thought, and I've just never gotten a moment to talk about it. And so I thought, okay, it's reached critical mass. We're going to do that.

Also we have Australia versus the laws of math. Does an implanted pacemaker meet the self-incrimination exemption? An update on the worst-case crypto future model, which occurred to me following some other news. It's surprising what one can find at a flea market. Another example of the consumer as the product, and a little quick SQRL technology update to tell our listeners where I am. And then some closing-the-loop feedback from people who listen to the podcast. So I think another great couple hours.

So our Picture of the Week, we've actually seen this before years ago, but it is one of these memes that just deserves to never die. And the caption that I saw it with this time just really closes the deal. So the caption reads: "We have patched that vulnerability you reported."

Leo: I should show the picture here. Let me show it to you so, for people watching at home, you can see it. Oh, that's a nice patch you did there.

Steve: Anyway, so for those who are listening, this shows a, I don't know, a walk path or a bike path. It's a paved asphalt strip that's got lawn on both sides, extending off into infinity on both sides. And in the middle of this asphalt path, it looks like a recently installed gate. It's bright yellow. And where the gate is the asphalt's removed, and there's a strip of concrete, so it looks like someone took out the asphalt, poured some concrete, anchored this yellow gate in. And, I mean, you cannot go through that gate. But it's completely open on both sides. And frankly, the lawn doesn't look like it's in great shape on the sides, and you wonder if that's just because everyone goes around. Anyway, it's just a classic, you know, "We have patched that vulnerability you reported." Yes, you said we needed a gate, and we gave you a gate to block any foot traffic.

Leo: No foot traffic allowed.

Steve: Or bicycles or whatever. Ugh, wonderful. Okay. So I put this number one because this offering of security-related books is breathtaking. The link is in the show notes. The show notes are already posted on GRC.com/sn for Episode 620, so you can immediately get them. But it's also HumbleBundle.com/books/cybersecurity-wiley. And the lineup is amazing. There was a previous, a couple years ago, I think it was O'Reilly who was making these available. This, as the URL indicates, is Wiley as the publisher.

So we've got, okay, for a dollar or more, that is, for just a dollar, but you're invited to provide more if you wish, the book "Social Engineering: The Art of Human Hacking." Also you get "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition." And "Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation." And the fourth book, "Threat Modeling: Designing for Security." All four of those as eBooks in multiple formats with no DRM for a dollar. But give them five or something. I mean, and I should also mention that this is all a charitable donation, as well, and you can choose to which charity it goes to from a list lower down the page.

If you go to $8 or more, in addition to those four: "Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition." Also, the second edition of "The Shellcoder's Handbook: Discovering and Exploiting Security Holes." "Cryptography Engineering: Design Principles and Practical Applications." "The Art of Deception: Controlling the Human Element of Security." And "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory." Those five books, in addition to the first four, for $8.

And two of Schneier's books are in the final set. There's an additional five for $15 or more: "The Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code." "Unauthorized Access: Physical Penetration Testing for IT Security Firms." And one of the first two of Bruce's books: "Secrets and Lies: Digital Security in a Networked World, 15th Anniversary Edition." Also "CEH v9: Certified Ethical Hacker Version 9 Study Guide." And, finally, the book - and I've got two copies behind me. When I was looking at this, I turned around. One is a hardback, and one is softcover. And that is "Applied Cryptography: Protocols, Algorithms, and Source Code in C, the 20th Anniversary Edition." And of course "Secrets and Lies" and "Applied Cryptography" are both Bruce Schneier's books. So all eBooks. What is that?

So that's 14 eBooks, four in the first and then five in each of the two, for $15. So anyway, I wanted to make sure our listeners know about it. I've already gotten a ton of feedback from the people who saw my tweet about this yesterday as I was putting this together. And a lot of people were very impressed with the lineup. So it's for a good cause. Apparently it's doing very well. And I would say take advantage of it. When I looked yesterday, it was 13 days and some hours remaining, so I think that is an end-of-July cutoff. So it looks to me like it's good through the end of this month, the end of July.

Okay. So as we know, Wednesday, July 12, last Wednesday, was the Internet-Wide Day of Action to Save Net Neutrality, which is not really a very catchy title, but that's what it was called. And I saw, Leo, you guys went to black-and-white and had a red banner across the top of the screen. And many companies did all kinds of things. There were companies who were, like, putting up a sort of an emulated blocking banner to bring it to people's attention or to say this is what you might be greeted with if we don't have some regulation to prevent ISPs from pretty much doing anything they want to with the

bandwidth that you're purchasing from them.

So yesterday, that is, Monday, just yesterday, major tech companies clashed with Internet service providers over whether this Net Neutrality law, this order that the Obama administration put into effect in 2015 which barred the blocking or slowing of web content, should be scrapped by the U.S. Federal Communications Commission, which is what the concern is now. So the Internet Association is on the side of we need to preserve Net Neutrality and this existing legislation. They represent the major technology firms, including Alphabet, which of course is Google, Facebook, Amazon, Microsoft, Netflix, Twitter, Snap, and many others. All collectively urge the FCC to abandon its tentative plans to rescind the rules barring Internet service providers from hindering consumer access to web content or offering paid fast lanes. And in the Internet Association submission they wrote that dismantling the rules "will create significant uncertainty in the market and upset the balance that has led to the current virtuous circle," as they put it, "of innovation in the broadband ecosystem."

And of course on the other side the major ISPs - AT&T, Comcast, Charter Communications, and Verizon - all urge the FCC to reverse the existing rules, which were enacted by the Obama administration, while vowing not to hinder Internet access. That is, they were saying, we will voluntarily agree not to break the spirit of Net Neutrality, but we don't want to be forced to. And one of them even went as far as to say, well, there are some instances where we think everyone would agree that it's a good thing. So it's like, yeah, okay, right.

So the FCC, for their part, said that - oh, I'm sorry. AT&T said that the FCC in 2015, when this was initially put in place, quote, "grossly exaggerated the need for public utility-style regulation, while ignoring its costs." And so of course what has started all this is that, two months ago, the month before last, in May, the FCC voted two to one to advance the FCC Chairman Ajit Pai's plan to withdraw that previous administration's order reclassifying Internet service providers as if they were utilities.

The problem is, in my opinion, access to the Internet has evolved from what was originally sort of an optional luxury to being a near necessity. And in every meaningful way, its provision is, I would argue, no different from electricity. When I purchase electricity from, in my case, Southern California Edison, I pay the same price and the electricity flows just as well to my air conditioner as to my coffeepot. And this is true, even if Southern California Edison happened to own their own air conditioning company. They're not permitted to charge me a higher rate if I use a competitor's air conditioner. But you can imagine that in such a situation they would love to, if they could, to subsidize their own private interests at the expense of the competition and, ultimately, at the expense of the public.

So the FCC Chairman argues that the Obama order unnecessarily harms jobs and investment and has not committed to retaining any rules, saying that he favors an "open Internet," of course meaning a completely unregulated Internet. And as a proud capitalist myself, I would be happy to have that if we also had choice among providers, I mean true competition. But as I have said when we've had problems with the bandwidth on this podcast, I have no choice. I mean, there is absolutely no true practical choice for me in broadband providers. In my area of Orange County in Southern California, Cox Cable is my sole source of broadband.

And of course this has been deliberately arranged over time. And years ago we were covering the mergers of these major providers as they were purchasing each other, dramatically reducing effective competition in the market. And some of the big ones were paused or backed off on or stopped. But there's clearly a tendency for monopolies to

form. And I would argue that, unless you have true competition, then you have to have some regulation. And there isn't today actual competition so that a consumer can easily jump from one broadband provider to another, at least not in all markets. Not in mine. So anyway, 12 state attorneys general, including from Illinois and California, have urged the FCC not to overturn the Obama rules.

More than, now, I don't know what this number means, but 8.4 million public comments have been filed on the proposal. And the reason we don't know what it means is it would be nice to know whether that number was bot-filtered or not because we know that there were lots of shenanigans played with that site that wasn't preventing somewhat specious submissions from being made.

So my nonpartisan observation is that mostly I'm troubled that we're seeing such an expanded use of executive orders in place of congressional legislation. It's true that Congress moves slowly and with great deliberation, when it moves at all. But that's the way it was designed to function. The inertia means that things change gradually, only after being examined and debated at length, and that they can be tuned and tweaked as needed over time. But when issues like this become politically partisan, and when the party holding the office of the executive bounces back and forth between parties as this country experiments with different leadership styles, we wind up creating a climate of tremendous uncertainty, which is arguably the worst of all possible worlds because then no one is able to plan. No one is able to rely on what the future is going to look like.

So in this case President Obama's administration put this in place by executive order, and President Trump's is considering removing it. I hope that Congress finds the will to consider this, what I think is a crucially important issue, at length and will take it up once and for all and remove it from underneath the President's executive order pen, except to sign actual legislation into law that settles this once and for all because having this jump back and forth as a political football is just - it's, again, as I said, it's the worst of all possible outcomes.

Leo: Actually, I don't think it was executive order, Steve. I think it was the FCC that decided to use Title II regulation. Obama encouraged them to, but he did not say so. The FCC said so, and that is in their mandate.

Steve: So it's political appointments to the FCC, then.

Leo: Well, it's appropriate for them to do it. And the FCC, you may remember, tried to enforce Net Neutrality without Title II regulation, and it went to the courts because they were sued immediately by Verizon.

Steve: Right.

Leo: And the judge said, look, you can't do this. You don't have sufficient congressional mandate.

Steve: Ah, okay.

Leo: And pointed them at Title II of the Telecommunications Act saying, however, if you...

Steve: Under Title II.

Leo: If you were to declare Internet service providers as utilities, under Title II you could do this. You haven't up to now. You said they're telecommunications or something. But if you were to declare them utilities, you could do this. In effect, the judge said, "But if you wanted to, you could do it."

Steve: Yes, I do remember that.

Leo: Yeah. And then Tom Wheeler decided, after extensive comment, and that was really the thing that was interesting about this is the Internet weighed in heavily. And while I think Wheeler was reluctant to use Title II, was convinced to do so by millions of comments from the Internet last year. So that's why Ajit Pai can reverse it, because it's an FCC rule. But you're right, though, and this is what AT&T, which kind of jokingly, in my opinion, said we support the Internet Freedom Day because we believe in Net Neutrality, too, but we believe Congress should do it. And so they're saying the same thing as you. And the reason is the telecommunications industry - actually, not even that. If you just look at Comcast, Verizon, and AT&T...

Steve: Strong lobbying power.

Leo: ...poured more than half a trillion dollars into lobbying in the last 10 years, $574 billion. So they know that if they go to Congress, they will win. So I agree with you. I think really Congress is the right answer to this. But at this point it is within the FCC's purview to choose Title II and, in this case, to stop using Title II to regulate it because Congress did give them that tool in the Telecommunications Act.

Steve: And so then I guess the conclusion is that money wins.

Leo: Money wins in everything. But it does, certainly in Congress, especially since the Citizens United decision has allowed a huge influx of dark money into politics, it's gotten worse. And remember Larry Lessig, the Harvard constitutional lawyer, brilliant guy, created Creative Commons? For a long time he was fighting against copy protection, DRM. And then he gave up. He said, you know what, I can't win this battle because, before we win this battle, we have to change how election financing works in this country.

Steve: Right.

Leo: We have to get the influence of big money out of...

Steve: And return control to the electorate.

Leo: To the people. And in fact that was Larry's - Larry ran for President. And his entire platform was elect me because you're never going to get elected representatives to do this, so elect me. I'll choose a really great vice president.

Steve: Exactly.

Leo: I will do this one thing and then resign.

Steve: Yes.

Leo: Remember that?

Steve: I remember exactly that. It was wonderful.

Leo: He didn't get very far after that because of the power of money.

Steve: People were saying, "Larry who?"

Leo: The only thing I'd say about that is the only reason money is valuable in politics is to win votes. And so ultimately it is still in the hands of the voter. And we just have to vote. And we have to make our voices heard. Call your members of Congress. That scares the pants off them. That's far worse than anything, than Citizens United or the NRA or the Koch Brothers.

Steve: Yes, the idea that they might not get reelected.

Leo: That's what scares them. And the reason it works right now is because most of the congresspeople who support this are Republicans facing easy reelection, but difficult primaries should the Koch Brothers and others decide to finance opponents in the primaries. They're worried about the primaries, not the elections. They're in safe Republican seats.

Steve: Right.

Leo: So if people - I think if people started to take it seriously and vote and make their voice be heard, there would be a shot at this. That's the only way. And I don't think we're going to change, have campaign finance reform.

Steve: And of course, as we've discussed, we finally have - it's taken us as techies this

long to actually understand what the term means.

Leo: Right.

Steve: You have been saying it's not the Internet that needs regulation, it's the ISPs. And that finally clarified the issue in a way that, you know, "Net Neutrality" has got to be the worst term anyone has ever come up with for something that's arguably very important.

Leo: It's a terrible term. That's part of the problem; right? What the hell does that mean?

Steve: Yeah, gosh. And so here we have the world, or at least the U.S., going to be significantly impacted by the outcome. And most people just, I mean, you know, we care, and our listeners care. But we're not the electorate at large. So, yeah, I don't know what chance it has.

Leo: I agree.

Steve: In May 2016 we discussed, a little over a year ago, the fact that MySpace had lost control of 427 million passwords, which were being offered in aggregate to buyers for $2,800. And at the time we said, okay, if you were ever a MySpace user, go do something. Delete your account. Change your password. Back then, if you were using the same password for all of your logins, then remember what that MySpace password was and make sure you're not using it anywhere else. And it was just like, it was a disaster. Yesterday...

Leo: By the way, I changed my MySpace password when that happens. Didn't want anybody using my account.

Steve: No. Yesterday, get this, a frustrated security researcher at a firm named Positive Technologies - the researcher's name was Leigh-Anne Galloway - finally publicly disclosed a troubling vulnerability she had uncovered after first responsibly disclosing the problem to MySpace nearly three months ago, in reaction to which MySpace was irresponsibly silent. She never got any acknowledgement or response of any sort. Gave them 90 days, nearly, and just said, okay, fine. So she described, in the coverage of this, MySpace as being an enormous graveyard of personal data.

And in fact I was reminded of the term "zombie data," that is, like places where we have personal data that we've sort of wandered off from, and it's zombie data. It is our data, and it's never going to die, but it's sort of just there and not being kept current. So she noted that companies have a duty of care to their users, both present and past. And in some coverage of this, Leigh-Anne told Motherboard, who reported on this, that when she discovered the flaw, she was horrified and shocked by the complete lack of due diligence on MySpace's part.

Okay. So what's the problem? Unlike nearly ever other password recovery system, which

is at least anchored to a user-controlled email address, MySpace offers an account recovery process for people who have even lost access to their email account. And I remember discussing this before, that is, this policy has been in place for a while. It's a little unnerving because basically they're saying, oh, you've lost your email, like your email provider went away, or you forgot your email login or whatever. So MySpace implemented a system that would even forgive you if you could not receive a password recovery email.

Now, at first glance, what they're doing doesn't look too bad. I've got a link here in the show notes for anyone who's interested. Since what MySpace presents you with is a comprehensive and somewhat intimidating form asking for a great many of an individual's details, with a whole bunch of them marked with asterisks saying "required information must be provided."

So the form states that all of the following information must be provided, which includes the email address associated with the profile - okay, so right off the bat it's like, wait a minute. If you know your email address - so maybe it's email address, but you can't actually retrieve email from it. Okay. Your date of birth. The zip code listed on the account. Your full name listed on the account. The city and state of the account owner. And there's a bunch of other stuff which is optional. But all those things, red asterisk-starred, must be provided. However, what Leigh-Anne found is that it appears that some heuristic logic operating behind the scenes processes the form's data so as to minimize their support costs.

Leo: [Chuckling]

Steve: I know.

Leo: Just keep listening, folks. You're not going to believe this.

Steve: So it likely has an "if any three or more are valid" in the whole...

Leo: They don't have to be right.

Steve: ...in the whole form acceptance threshold. So unfortunately, when you look this over, and consequently what Leigh-Anne discovered and reported, and which MySpace has ignored, and Motherboard then confirmed, was that anyone having only the MySpace user's name, the account username, and their data of birth, only those three pieces of information is able to establish themselves as the new owner of any existing MySpace account.

Leo: So changing my password did nothing.

Steve: No.

Leo: I should change my birth date, is what I should do.

Steve: In their reporting, Motherboard verified this, writing: "Once we finished the recovery process, we had full access to two accounts. We could write new posts, read old messages, and basically do whatever the account owner could." And then they said in parens, "(Thanks again to the two brave volunteers who let us break into their old MySpace accounts.)"

Leo: Unbelievable. Unbelievable.

Steve: It is. Now, that form, which is readily hackable even by its owner, does have a dropdown list box selection of whether you want to recover access or delete your account permanently. And I've got links in the show notes here. There's a different "Delete Your Profile" link and process. So essentially this ups the ante. We already recommended in the past that our listeners should proactively remove any residual MySpace accounts.

So if nothing else, this is a reminder that doing so then was an even better idea than we knew at the time because this has probably always been the way this worked. And it just took somebody poking at it to see how little of the form's data actually had to be correct. And Leigh-Anne discovered, uh, not much. And why? It's because they don't want to get support calls. It's like, if you just kind of - fuzzy logic. If you sort of seem like maybe you might be the person who used to be using this MySpace account, eh, that's fine. We'll give it to you. So, yeah. Zombie data. If you were ever a MySpace user, it's worth taking a minute to just wipe your data clear because otherwise somebody could easily decide they want to impersonate you. And it's just not difficult to do.

And speaking of account recovery, the Windows 10 Fall Creators Update will be adding what is apparently a much requested feature. They will be adding an "I forgot my password" option to the Windows 10 login lock screen. So where you are prompted for a password, there will be a "I forgot it" link, which there has not been until now. People who are configured to use Windows Hello mode or a PIN will also be able to access the new password reset option right from the lock screen.

Once the password reset process has been started by clicking that link, Cortana pops up and will guide the user through the reset process, which essentially amounts to providing some means of verifying yourself with a secondary email address, receiving a test SMS message, or using the Authenticator app in order to prove who you are; and, once verified, the user will be allowed to reset their password. So Microsoft continues to listen to feedback and is adding the things that people want. And I updated my Win10 machine last night to see if I could actually get that, and maybe I have to use the wrong password a few times for it to show up. I was afraid of getting myself locked out or something. So I didn't see it. And I did get - I am on the Creator track, so I think I've got the latest. But it may not have been there yesterday, but it is on the way.

And speaking of passwords, a listener's tweet reminded me that one thing we haven't discussed ever is the bizarre and sort of counter, what I think is a counterproductive practice, which some, I mean, brain-dead websites have been adopting now for several years of blocking form-fill automation. And I've received tweets about this probably for several years. Not in great number, or it would have made it onto the radar and onto the podcast before now. But the problem, of course, is that this fights against password managers.

The idea is that there is technology on a website which is proactively blocking the automation of form fill, which our password managers use in order to conveniently provide a unique password for every site that we visit, assuming that that's the way we've taken the trouble to set them up. And they're even manually - they're even blocking manual copy and paste. So even if you weren't using a password manager, but say that, like, years ago you started a text file or an Excel file or something, where you just sort of had your own ad hoc database in order to help you remember which password you use for which site, where you're used to copying that from your little ad hoc database and then selecting the password field and hitting ctrl-v to paste, but this site won't let you do it. So it essentially forces you to press keys on your keyboard - and you can sort of imagine Scotty on Star Trek saying, "How quaint" - in order to actually have to manually enter the password.

So this makes no sense to me, and I could not see any rational, right-thinking justification for the practice. But it is somewhat widespread. I mean, I'm not encountering it, but in researching it on the 'Net I found lots of instances of it, specific sites that were doing it. And so I dug around to see whether there was some hidden benefit that hadn't occurred to me.

And I did run across a posting, a blog posting by Troy Hunt, who's a well-known, and we quote him on this podcast from time to time, security researcher who writes a widely read blog. His short bio states that he creates courses for Pluralsight, is a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals. He examined this question a little over three years ago, so it's been around for a while, under the heading on his blog of "The Cobra Effect," which was a fun anecdote about the mistake that the British apparently made way back when they were in a conquering mood. They encountered a problem on the subcontinent of India, and that was cobras, which were numerous at the time. It turns out there were a lot of them wandering around and taking bites out of the British.

So ingenious as the Brits were, they decided to offer a bounty on cobras in the hopes that the indigenous inhabitants of India would round up the cobras in return for cash. But of course this turned cobras into a form of currency that could be bred. So cobra breeding became a thing.

Leo: That's a hoot.

Steve: Oh, yeah. And after the British saw the error of their ways and terminated the bounty, the excess cobras were all released.

Leo: Were released into the wild.

Steve: Back into the wild.

Leo: You get a net gain in cobras. Whoops.

Steve: Yeah, that's what happens. Which of course resulted in more cobras than there were originally.

Leo: Oh, my gosh.

Steve: So of course the law of unintended consequences. So anyway, but I digress. Troy's analogy was meant to make the point that sometimes trying to fix something to make it better actually has the reverse effect. And all of us who use password managers would argue that a site which fights against very secure, difficult to enter, and even hopefully unknowable passwords, is lowering your security.

And so, okay, now I understand why this didn't occur to me. It turns out that the blocking of login automation is apparently, and this is what Troy determined, a completely wrongheaded attempt to prevent automated brute-force login attempts presumably being made by something that's using a web page's automation for brute-force login guessing. Like some sort of a, I don't know, a form-fill-in robot which fills in the form and then submits the page over and over and over. Okay.

But anyone who understands how the web actually works knows that the web browser page is merely a frontend which puts a pretty face onto an eventual HTTP form query, an HTTP POST verb query. So no sane brute-force attacker is going to automate the form. They're going to bypass that completely and directly submit the form's data to the remote web server for its approval or rejection. So it's not the way brute-forcing works, which some lame person somewhere thought, oh, I'll be clever, and I'm going to prevent anyone from pasting data into the password field, which will prevent bots from doing that. But that's not what bots do. Anyway, another way to say this...

Leo: Calm down, Steve. It's okay.

Steve: It's not possible to robustly prevent brute-forcing in the web browser client because the browser is trivially bypassed by making direct server queries.

Leo: I see that also you see places that won't let you paste into the field. Do you think that's the same misguided, you know, just cut/paste.

Steve: Yes, that's the same, yes.

Leo: Yeah, well, that's not...

Steve: And apparently, like, when companies have been asked, they've said, oh, we'll lose our certification if we allow pasting into the password field. It's like, what? Anyway, it's something that's been around us for a few years, and I've been meaning to just say, okay.

Leo: Stop it. Knock it off.

Steve: To dig in - well, yes, yes, exactly.

Leo: Please knock it off.

Steve: In the same way that the NIST has now changed their guidelines to say there is no point in forcing people...

Leo: Yeah, there's a good one.

Steve: ...to change their password every month. Please, there is no benefit to blocking pasting into password fields. It doesn't prevent any actual attack on your server because it's only the web page which no bot is going to fill in.

Leo: Right, right. It'll do a POST.

Steve: It's going to issue - exactly.

Leo: It'll POST the data.

Steve: Exactly.

Leo: It's much faster. Why would - I'm going to type it in. I have written a special automated typing system.

Steve: Oh, lord. So yesterday, while I was putting the show together, going back through all the submissions from our listeners over the past week, I kept seeing this link. And it was about some insanity in Australia. And I thought, okay, we talked about this last week. And so I kind of just kept pushing past it, saying, yeah, yeah, yeah. Finally, someone sent me a tweet with a couple quotes which did stop me cold. And I said, wait, what?

So, okay. The headline on this piece in the Guardian was of little surprise. It read: "New Law Would Force Facebook and Google to Give Police Access to Encrypted Messages." Okay, yeah. That's what we've been talking about. The subheading: "Under government plan, Internet companies would be obliged to give law enforcement agencies warranted access." Okay, yeah. Still no surprise.

Malcolm Turnbull said on Friday - and he's the guy that we quoted last week when we were talking about Australia weighing in, or maybe it was the week before. The law would be modeled on Britain's Investigatory - that's the word I always have a hard time getting around - Investigatory Powers Act, passed last November, which gave intelligence agencies some of the most extensive surveillance powers in the Western world.

Under the law, Internet companies would have the same obligations as telephone companies to help law enforcement agencies, you know, for example, in telephone wiretaps back in the good old days. Police would need warrants to access the communications. Turnbull said the legislation was necessary to keep pace with advances

in technology that could facilitate crime. He said: "We need to ensure that the Internet is not used as a dark place for bad people to hide their criminal activities from the law."

Okay. Now, here it comes. Here it comes. He says, asked by reporters, the Guardian reports, how legislation would prevent users simply moving to encryption software not controlled by tech companies - you know, yay to the reporters for asking the question; right? - Turnbull responds that Australian law overrode the laws of mathematics.

Leo: What?

Steve: Oh, yes. He said, quote, and I'm not kidding: "The laws of Australia prevail in Australia."

Leo: I didn't know you could do that. That's awesome.

Steve: Oh, they've got some powerful laws there, Leo. He said: "I can assure you of that." I'm still quoting. "The laws of mathematics are very commendable," he said.

Leo: Yes, they're commendable.

Steve: Yes. "But the only laws that apply in Australia is the law of Australia." Now, I don't know about the law of gravity because that's handy to have. Okay.

Leo: What a moron.

Steve: Yes, the people handling the legislation for us. Also, Turnbull denied that the government's plan involved the use of a backdoor into programs to allow access to encrypted messages on platforms such as WhatsApp and Telegram. He said, and I'm quoting again: "A backdoor is typically a flaw in a software program that perhaps the developer of the software program is not aware of, and that somebody who knows about it can exploit." Still quoting. "If there are flaws in software programs, obviously, that's why you get updates on your phone and your computer all the time. So we're not talking about that. We're talking about lawful access."

So, okay. Translation: Apparently, if it's a lawful backdoor, then by definition it's not a backdoor. It's a handy new feature. Then, pressed on whether the government's plans meant it would ask companies such as Facebook and Apple to keep a copy of encryption keys used by customers, Turnbull said: "I'm not a cryptographer." Uh-huh, yeah, surprise. "But we are seeking," he said, "what we are seeking to do is to secure their assistance," that is, the assistance of actual cryptographers, although I would argue that it's less seeking their assistance then compelling their assistance. Anyway, he said: "They have to face up to their responsibility. They can't just wash their hands of it and say it's got nothing to do with them."

So, yeah. Attorney General George Brandis said the legislation would, quote, "impose an obligation upon device manufacturers and service providers to provide appropriate assistance to intelligence and law enforcement on a warranted basis." Anyway, so again,

I just - the idea that they're saying, sorry, the laws of mathematics will be bent to suit the laws of Australia, which will prevail. It's like, okay. Now I understand why our listeners thought I had to see this, and I thank them for bringing it to my attention because it was good for a good laugh.

And it's going to be really interesting to see how this all shakes out. I think probably, what, next year I would imagine we'll begin to see this. They're saying that this will be put in front of their Parliament by November of this year, and saying that it would allow courts to order tech companies to quickly unlock communications. Of course, now, the technology we have in place now has been designed not to allow that.

And so there'll have to be some - the legislation will have to incorporate a period of time, well, I mean, we'll have to see how this all comes out. But if it does happen, it'll have to incorporate some leeway to allow the technology to be changed to accommodate warranted intercept. And we'll have to see whether it's, like, from some point forward, or past communications, after the fact, I mean, this is going to - it's going to be a mess because, without legislation, we've been covering for years the huge strides the crypto industry has made, arguably spurred by the Snowden revelations, adding things like perfect forward secrecy, where future disclosure of a key does not allow you, by design, to go back and decrypt previous conversations. That's what perfect forward secrecy means. And the best protocols we're using today now support that.

So, boy, you know, without any legislation, the technology has shot to a point where we're using a lot of technologies which are fundamentally hostile to the kind of legislation that everybody, all of the saber-rattling that we're seeing is saying that they want. And it's quite clear that these legislators are not cryptographers. So, yeah, we live through an interesting period now, Leo.

Leo: You have to think he's - Turnbull's got to know better. He's just being cynical. He's appealing to know-nothings. It's just not so different from the law of the land in the U.K.

Steve: Correct.

Leo: So we knew this would slowly creep across the world.

Steve: Yeah. And what interests us on this podcast are the details. What is it? What is the law going to say, and what are the technological implications of that?

Leo: Right.

Steve: So, okay. First it was a smart water meter. Then a listening home audio device. Now it's a suspect's own heart rate, as recorded by his implanted pacemaker. Engadget's headline reads: "Judge Allows Pacemaker Data to Be Used in Arson Trial," with the subheading, "The subject tried and failed to get the judge to disregard his own heartbeat as evidence." Now, we covered this story at the time. It was in the latter half of last year. You'll remember this, Leo, because it was sort of bizarre even then.

Authorities in Ohio arrested a man named Ross Compton on the charge of arson and

insurance fraud based on his pacemaker data. Compton told the police that, when he saw his house burning on September 19 of last year, he packed his suitcases, threw them out his bedroom window, and carried them to his car. However...

Leo: How they got there.

Steve: Uh-huh. Since he has a serious heart condition and other medical issues that would have made it extremely difficult for him to do all of that, also in the timeframe apparent, that was apparently, like, based on the 911 call and so forth, investigators were able to secure a search warrant for his pacemaker. So there was reasonable suspicion that allowed them to get his pacemaker data. Then, according to court documents, a cardiologist reviewed his heart rate, the pacer demand, and his cardiac rhythms before, during, and after the fire, saying, quote: "It is highly improbable that Mr. Compton would have been able to collect, pack, and remove the number of items from the house, exit his bedroom window, and carry numerous large and heavy items to the front of his residence during the short period of time he has indicated, due to his medical conditions."

And as it turned out, that data became a key piece of evidence that allowed law enforcement to indict the accused, this guy Mr. Compton, although they also detected gasoline on his shoes and clothing. So, yeah, how did that get there?

Leo: He was shaky after the fire, and he had to fill his tank, I think.

Steve: He had some hokey story.

Leo: Yeah.

Steve: So I should note that the EFF is not happy about this, naturally. Stephanie Lacambra, an Electronic Frontier Foundation staff attorney, told SC Magazine in their coverage at that time that cases like this could be the canary in the coalmine concerning the larger privacy implications of using a person's medical data.

She explained: "Americans should have to make a choice" - should not, sorry. "Americans should not have to make a choice between health and privacy. We as a society," she said, "value our rights to maintain privacy over personal and medical information, and compelling citizens to turn over protected health data to law enforcement erodes those rights."

Ross's attorney, so the defense attorney, tried to convince the court to disregard that evidence, arguing that it was obtained in an illegal search. But the judge who heard the case didn't see it that way. He has decided to allow the suspect's pacemaker results to be used as evidence against him in an upcoming trial. However, something the judge said is troubling. Engadget reported that Judge Charles Pater said he does not think the data's use has bigger privacy implications. But his exact quote makes that rather murky.

He said: "There is a lot of other information about things that may characterize the inside of my body that I would much prefer to keep private rather than how my heart is beating." He said: "It is just not that big of a deal." And it's like, whoa, wait. So he's

saying that heart rate should be made publicly available, or available in this case, yet he is acknowledging there are other things about his body that he doesn't want to have available.

So it seems to me like, you know, I'll be surprised, for example, if this got appealed, if that on-the-record statement wasn't used to say, wait a minute, the judge is just making an arbitrary decision that pacemaker data is acceptable, but other things, like maybe your insulin pump data, for example, would not be. I don't know. It just seems to me that we need, again, some clear legislation about what is private and what's not. And I am glad we have the EFF watching this stuff and often stepping in on our behalf.

Techdirt has a writer, Karl Bode, who posted yesterday under the topic of the misuses of technology. And some of this is sort of already on the record for us. But it triggered some additional thinking that I wanted to share with our listeners. So I want to share his reporting and then further stretch our thinking about the possible future of Internet encryption.

So Karl wrote: "The global war against privacy tools, VPNs, and encryption continues, utterly unhinged from common sense." And, he writes: "The assault on consumer privacy remains a notably global affair. Reddit users noticed that India's fifth largest ISP, YOU" - as in Y-O-U - "Broadband, is among several of the country's ISPs that have been trying to prevent customers from using meaningful encryption. According to the company's updated terms of service, as a customer of the ISP you're supposed to avoid using encryption to allow for easier monitoring of your online behavior."

Says the Terms of Service, quote: "The customer shall not take any steps, including adopting any encryption system, that prevents or in any way hinders the company from maintaining a log of the customer or maintaining or having access to copies of all packages/data originating from the customer." And then Karl writes: "Of course, enforcement of such a requirement is largely impossible." Okay, now, this is what I will address in a minute because it's actually and significantly incorrect, as a consequence of some additional thinking I've done.

But, he writes: "YOU Broadband isn't just being randomly obtuse. And while the ISP's Terms of Service is making headlines, this effort isn't really new." He writes: "Most Indian ISPs are simply adhering to a misguided, and still not adequately updated, set of 2007 guidelines" - so 10 years old - "imposed by India's Department of Telecommunications, demanding that ISPs try to prevent their subscribers from using any encryption with greater than a 40-bit key length, if they want to do business in India."

Quoting from the Terms of Service: "The licensee shall ensure that bulk encryption is not deployed by ISPs connecting to landing station. Further, individuals/groups/organizations are permitted to use encryption up to 40-bit key length in the symmetric key algorithms or its equivalent in other algorithms without having to obtain permission from licensor. However, if encryption equipments higher than this limit are to be deployed, individuals/groups/organizations shall do so with the prior written permission of the licensor and deposit the decryption key split into two parts with the licensor." Okay.

So then Karl says: "Which in and of itself is rather hysterical, given that since 1996 or so most folks have considered a 40-bit key length to be the security equivalent of wet tissue paper." In fact, Ian Goldberg, and we talked about this at the time, or talked about it in the past, won $1,000 from RSA for breaking 40-bit encryption in just a few hours way back in 1997, saying at the time: "This is the final proof of what we've known for years: 40-bit encryption technology is obsolete."

So first of all, on the question of is this possible, well, what we know of the way web browsers and servers establish their connection is that by necessity there is a plaintext handshake which occurs between the client and the server, or any endpoints in a secure TLS connection, before the encrypted tunnel is brought up in order to begin encrypting traffic. And we've often talked about how one of the reasons that browsers and servers have deprecated 40-bit keys and the use of 40-bit symmetric ciphers is that it was possible for an attacker to create a downgrade attack. Because that handshake is, by necessity, in the clear, the client sends a list of all the ciphers it knows to the server. And if a man in the middle were to edit that list, removing the higher security ciphers and leaving only the 40-bit ciphers, then the server would receive this sad list of available security and shrug to itself and go, well, okay, and agree to establish a 40-bit connection.

The client would think, wow - because the client wouldn't be aware that its handshake had been edited on the fly, it would think, wow, this must be a lame server. I offered all these great ciphers, and the server apparently just can only do 40 bits. Oh, well. And so they would then negotiate a 40-bit connection which we now know, if that was captured, could in a relatively short amount of time be cracked. And historically this was so-called "export-grade" encryption. The good news is, for years we suffered under the previous use of export-grade encryption. It just stayed around for the sake of backward compatibility to endpoints that couldn't do any better.

Finally, over the last few years, as we've moved forward, it has been dropped across the board. So currently that could not be done. But what could be done, if somebody wished to, would be that an ISP could first of all require their customers to use browsers with this degenerate form of encryption, or we know the ISP could themselves set themselves up as a so-called "middlebox" in order to intercept more secure connections, decrypt them on the fly, perform so-called "deep packet inspection," and then reencrypt as it goes to the server.

Now, until recently, I have been suggesting that what this would require is that we accept, "we" an ISP's customer, accept a certificate from the ISP because, for example, that's what the existing middleboxes do that are used in enterprise settings. That middlebox has its own certificate, and all of the PCs within the organization have that cert added, the public key matching the private key that the middlebox is using, have that added to their trusted root store so that their connections can be intercepted and analyzed for malware and content protection in order to help secure the corporate Intranet against the fact that now most traffic is encrypted.

So that's the way those work. But it's not - and so the other problem in terms of a practical solution is that how can an ISP ask all of their customers to do that? And what about IoT devices, which may have a non-editable fixed firmware set of root certificates, if they're even using TLS. Of course, if they're not, then it's not a problem.

But in thinking about this further, I realized that, for example, Google is able to mint their own certificates. They're able to do that because they have a certificate which they got from Global Trust which is itself a certificate authority. It's an intermediate certificate. But unlike most intermediate certificates, it has the permission bits set because it obtained them from Global Trust to itself be a certificate authority and create its own certificates.

So one scenario here is that, in the future, ISPs might be established in the same way that Google has established themselves, such that an ISP would receive a certificate which is already trusted by all of the trust stores in all of our devices. And unlike typical intermediate certificates, it would be a certificate authority certificate, allowing its

interception hardware to seamlessly intercept traffic as it's crossing their borders.

Now, I hate that idea. Don't misunderstand me. I'm not suggesting this is a good idea. But the technology exists to make that happen. Now, what would be better if something like this occurs is that, instead, an ISP could be required to reroute specific customer traffic to a law enforcement hub. That is, right now the ISPs have routers. They're routing traffic around. So imagine that, in responding to a court order, an ISP is told to route a certain customer's traffic to a specific destination. Then law enforcement could have such a certificate allowing it to seamlessly and essentially transparently intercept traffic.

And there are still some downsides to that. For example, we know that Chrome has pinned the known Google certificates. So Chrome would set off alarm bells if there was a certificate from Google that this entity was trying to intercept and create on the fly. So either those pinned certificates could be made as exceptions, or Chrome could have the law enforcement interception certificate added to essentially its permitted pinning, in order to prevent alarm bells from ringing.

So anyway, I just wanted to share some further thinking and evolution of ways that it might be possible for the structure that we have today to be matured in order to allow, at least in the U.S., with the constitutional provisions we have against unwarranted search, but the need to be able to provide search warrant supervised interception of specific traffic where a court has decided there is cause, there are technical means by which that could be done in a way that would still largely protect everyone's privacy and even protect the privacy of those who are being surveilled by centralizing that to a degree that, frankly, there are already commercial entities like Google doing exactly the same thing. Google has the ability to mint certificates. And that same capability could be provided to law enforcement under some proper terms and conditions.

A cryptography professor is wandering through a flea market and spots a typewriter for sale for 100 euros. But because he's a cryptography professor, he immediately recognizes it for what it actually is - an original Model 1 German Enigma machine.

Leo: Oh, no.

Steve: Being sold as a used typewriter.

Leo: And not a very good one, at that.

Steve: No. It's like, where do you put the paper? How do you change the ribbon on this thing?

Leo: OMG.

Steve: He buys it for 100 euros.

Leo: Hell, yeah.

Steve: So he later sold it at auction. And the only way I can explain the low price he got, although he made a pretty penny, is that maybe, I mean, the purchaser certainly knew what it was, and they made off like a bandit. He sold it for 45,000 euros, the "typewriter" that he purchased in a flea market for 100 euros. The reason, though, that was a good deal, although it must not have been in maybe super pristine condition because I think that matters. Last month the famous Christie's auction house in New York sold an Enigma machine for $547,500. So I have a feeling that was probably in mint condition, with all of its little light bulbs working, and probably fully functional. But, yes, keep an eye out at the swap meet and the flea market and the garage sales for something that looks like a funky typewriter. You never know what you're going to find.

Leo: That's wild. This was in Germany?

Steve: I think it was in - shoot, I don't think I had it here. I've got the link to - the BBC News covered it.

Leo: You've got to wonder how it got there; right?

Steve: Yeah, I know. It must have just been in somebody's garage for, you know, it's like, oh, spring cleaning.

Leo: But how did it get in their garage? I mean, it wasn't - I don't think people just have, oh, yeah, I bought an Enigma machine today.

Steve: Yeah, that's true. And there weren't - yeah, yeah.

Leo: Wow.

Steve: They're rare.

Leo: Isn't that neat.

Steve: Yeah. So speaking of typewriters, this just sort of passed by. I just wanted to note on the topic of that we are the product. We consumers are the product. The standard keyboard on the HTC 10 has begun showing ads. Reddit had a long thread of mild annoyed or mildly infuriated people just sort of shaking their heads that now, above all the keys and other little UI features, there were ads beginning to appear on the HTC 10. So, yes, the look of the...

Leo: HTC said that was a mistake, that that...

Steve: Oh, really. Oh, I'm glad you know. Okay, good, good, good.

Leo: Yeah. Just that was something went wrong.

Steve: That's freaky. I mean, I saw the screenshot of it.

Leo: Yes, no, you would [crosstalk].

Steve: And it was quite a convincing mistake.

Leo: Yeah, well.

Steve: Good. Okay. So a SQRL update. I have been working on SQRL's integrated install update and uninstall technology. It is integrated into the single EXE, so essentially the first - and our listeners will be doing this before much longer. It's getting close. I did not use a separate third-party installer because, frankly, SQRL is, I think it's 287K or something, and the installers are multiple megabytes. So the installer would be - oh, and it leaves debris behind and everything. So it just doesn't do anything that is necessary. So when you download it, you'll run it. SQRL will pop up a screen, "I notice I'm not installed." And you don't have to install. You could say no, and it'll just run from where it is. But if you install it, then you get some additional features. You have to have admin privileges.

The installer that I have written is UAC friendly, so it understands about the split tokens we've talked about in the past that appeared with Vista, and then of course with Windows 7, 8, and 10, where you need to give permission in order to do something that's privileged. By putting SQRL into the program files tree, it protects it from some level of abuse. And it establishes it so that it puts an entry in the add/remove programs in order to make uninstall easy. It gives it a presence in the Start Menu and so forth.

So I did something that was cool, though, that is an example of one of the advantages of doing my own technology for this. And that is that of course the SQRL executable itself is signed with an Authenticode certificate that of course I got from DigiCert. But that in itself, that is, just having the executable signed with a certificate doesn't itself provide the most security possible, since much of today's high-quality trusted software is signed with Authenticode certificates. It raises fewer alarm bells when somebody runs something. GRC's certificate has established a reputation. So, for example, Never 10 is signed with my DigiCert Authenticode certificate. And we've passed two million downloads. So Windows knows about stuff signed by GRC and, similarly, by Authenticode certificates.

Any random attacker could sign their own malware. So just the fact of it being signed actually doesn't provide much protection. To prevent that from happening, after downloading an updated version of the SQRL client as a temporary file, SQRL's self-updater not only validates that the new download's Authenticode signature is valid, but

also verifies that the certificate was issued to Gibson Research Corporation and that the issuer was DigiCert. So the one step above doing that would be pinning to a specific certificate fingerprint.

The problem with that is that certificates expire, as we know, deliberately, every few years. So pinning updates to a specific certificate would require the updates to contain the fingerprints of not-yet-valid future certificates and would force an update only for the purpose of updating the permission to update, essentially. So instead, what I've essentially done is I've pinned the certificate to the "Issued By" and the "Issued To" fields in the certificate, and there's just no way that an attacker is going to be able to arrange to get any sort of a SQRL malware spoof client signed by a valid Authenticode certificate issued to Gibson Research Corporation by DigiCert. That's not going to happen.

So anyway, and so the beauty of this is that you download the first copy of SQRL, and it will then keep a lookout for updates, notify you when there is one, and you press a button, and it updates. What happens behind the scenes is that what is downloaded not only has to be over TLS, has to be from GRC, has to be from a known location there; but, once it comes down, then it has to be validly signed, and that certificate that it's carrying has to be from me and which I got from DigiCert. And if all of that is true, then it renames itself as the new client, and that goes into use.

So a much stronger update technology than we normally see, and I just did it because I could because I was writing my own installer, updater, and remover. The install and uninstall is all finished. I'm just adding some little double-check dialogues to the updater. Then that'll get done. I'll turn it loose to the gang in the newsgroup to pound on. And then I'm down to a few little things. I've got a couple changes to the UI, and then I do have a to-do list that I've been accruing of just sort of mostly cosmetic stuff to deal with before I declare this thing finished. So we're getting very close.

Leo: Bravo. That's awesome.

Steve: Yeah. I'm excited. Naturally. And of course all of our SpinRite users are excited because once SQRL is behind me I return to work on 6.1. Which reminds me, apparently I said SpinRite last week was approaching 40 years old. I meant 30. And I saw one tweet...

Leo: Oh, that's less impressive.

Steve: Well, and I thought, how could I have said 40? And so I saw one tweet from someone who said, I think you said 40, and it must have been 30. And then I thought, I couldn't have said that. But then several other people also caught it. So clearly that was what I said. I just wanted to correct the record. Yes, 30 years old.

Leo: Shows you how much credibility you have with me because I didn't doubt it for a minute. He must have started in his 20s.

Steve: It also means that Sue has been with me for about 32 years because she has been with me from even before the days of SpinRite.

Speaking of SpinRite, I did see a nice note from Michael, who's in Glasgow, Scotland. And the subject was: "What's heavier, one ton of zeros or one ton of ones?" I thought, what? Anyway, he said: "Hey Steve. Longtime SpinRite user here. It's an amazing product that I, like many of your listeners, treasure.

"I was thinking about Oxford's question from Episode 617, on whether it's better to SpinRite before formatting a drive or after. The intuition he had about it probably making no difference is interesting. You agreed with him, of course. My question is, does SpinRite take the same amount of time in both cases? Say that there's a 1TB drive chockful of years of data and," he writes, "detritus."

Leo: Detritus, he means.

Steve: Detritus, that's right. I always - I have a problem with that word, detritus, thank you - "but in good working order with no serious problems. Will SpinRite finish working in the same amount of time as a blank, completely empty 1TB drive fresh out of the factory? I've never tried it, but I guess it must." He says: "My gigantic folder structures and sizeable data files have never felt so light." And so the answer is yes, until v7.

My plan is to do a series of point releases - 6.1, 6.2, 6.3, and I'm not sure how far it'll go. Because it's taken me so long to get SQRL finished and to get back to SpinRite, I'm going to push out a 6.1 faster than I had planned, that is, I'm going to make the changes I need to very quickly in order to get a 6.1 out. Then I'll do - and that will fully support direct hardware access to the hardware, that is, the native motherboard AHCI controller, or is it ACHI? I can't - Advanced Host Controller, AHCI, Advanced Host Controller Interface.

I think 6.2 will then add support for the native USB controllers to allow attached storage to work much faster. I did, before I paused work on 6.1 to work on SQRL, I did have the hardware running, the direct hardware interface running with a maximum size 32MB buffer, up from 32K, which is what SpinRite has always used traditionally because that's the max that could be allocated. And it was running, it would be able to do, that is, the code I have was able to do half a terabyte per hour. So it would do that one terabyte drive that Michael asks about in two hours. But none of the SpinRite 6 series knows about the file structure. SpinRite has always been a whole drive surface analyzer and data recovery tool.

With 7, I'm going to implement file level awareness to add things like rebuilding the file structure. But what that will also mean is that it will be able to do selective file recovery and, for example, to verify the integrity of the data separate from the surface. So for the moment, to answer Michael's question, it doesn't matter whether there is a file system on the drive or not, which is why many people run SpinRite on brand new drives before establishing, before even sticking it into a computer and establishing their operating system on it because it'll run on a blank drive just fine. So anyway, Mike, thanks for the question and for bringing it up.

Leo: All right. On we go. Steve Gibson, you've got some questions.

Steve: So, yeah, just a couple nice bits of feedback from our listeners. Someone whose Twitter handle is @shadyhotdog, but the name he has registered is This Is Nighthawk!, he just said: "DNSthingy is amazing." He said: "Flashed my ASUS router with their

firmware, and now I can do all sorts of cool stuff. Thanks, @SGgrc."

Leo: I think that's the Nighthawk who's a regular in our chatroom.

Steve: Oh, cool. Yeah, of course, and that's the DNSthingy that we talked about last week from the Nerds On Site guys, David Redekop, who also hangs out in the chatroom, that uses DNS in order to perform all kinds of controls over people's local Internet.

Byron Lee wrote: "Steve, my security-conscious friends won't touch my mobile Facebook Live video streams. What's a good, simple alternative?"

Leo: Ah.

Steve: And Leo, I was hoping you would have an answer to that, since I have no idea.

Leo: I wonder why their friends won't, why his friends won't.

Steve: Yeah, he says "my security-conscious friends."

Leo: Well, they just don't like Facebook, I guess.

Steve: Exactly.

Leo: Well, there are certainly many ways to stream. There's kind of, you know, we stream on Ustream. That's free. We stream on Twitch.tv. That's free. YouTube Live, that's free. But I think if his friends don't like Facebook Live, they may not like any of those. I'm not sure. All four of those allow free live streaming. I don't - it depends what his friends don't like.

Steve: Yeah. I think maybe they're just anti-Facebook. So you've just given us four good alternatives. So I think that probably answers Byron's question. Thank you.

Leo: Periscope, that's another one.

Steve: Oh, yeah, of course, yeah. Matt Warner said: "Looks like Twitter disabled two-factor authentication using authenticators and now uses SMS only. Is it better not to use two-factor authentication at all?" And I would say absolutely not. That is to say, it is better to use it. I mean, the fact that SMS is not as safe or secure as authenticator-based, time-based one-time passwords or one-time tokens, doesn't mean that it's not still better than nothing.

So, yeah, it's a little worrisome that the six-character SMS is being sent every time you need to authenticate. It would be nicer if that weren't the case. But it sure beats, you

know, but at least it's tied to your phone that's registered with your account and prevents an attacker from just being able to arbitrarily log in if they somehow guess your username and password. So absolutely, use as much two-factor authentication as you can. Any is better than none.

And Jerry Yu followed up on our discussion last week about that Broadcom exploit which was patched by Google earlier this month in Android, to note that it looks like it was also patched by Apple. Remember I said we did not know where Apple stood. It looks like it was patched in 10.3.1 because under the CVE number for that exploit, it reads: "WiFi in Apple iOS before 10.3.1 does not prevent" - and that's the CVE-2017-6556 "stack buffer overflow exploitation via a crafted access point." So that's definitely the problem we were talking about, and it looks like Apple did fix it in 10.3.1. So that's good to know, that we don't have that baseband radio problem.

Michael Rickman asked if I saw this, and he sent me a link, which was to yet another all-in-one credit card project on Indiegogo. And I just have to say, yes, and so far I think I've been burned by three of them.

Leo: I warned you about Coin.

Steve: Yes. Kickstarter or Indiegogo. And, I mean, in fact I did finally get an email from one of the first ones where the guy, I mean, I sincerely think, I mean, I know that he did everything he could. But I remember seeing a picture of his workshop, like he was in the garage winding some coils or something.

Leo: Oh, boy.

Steve: And I remember thinking, oh, this does not look good. So the problem is these electronic all-in-one credit card things, they are seductive, but it is very difficult technology. And so this is not something I would argue anyone should fund. I'm sorry. I don't mean to pour cold water on this. But Indiegogo - and it's not universally the case that Kickstarter and Indiegogo are people in their garage. But as you know, Leo, as I have experienced, many of these projects never ship. And I will be very surprised if a small group are able to pull this off. If it's going to be done, it's going to be done by somebody, by a much larger organization that can actually make this happen.

Leo: This is the - now I want to say this is the one I want. This is the first one I've seen that uses a chip, that uses an EMV chip.

Steve: I know. Yup.

Leo: See, that makes sense to me. It's not a striped card, it's an EM - I know. But you're right, it's hard to make. They've got $2 million raised.

Steve: Good. Let somebody else pay for it.

Leo: You've learned your lesson.

Steve: I'm not doing it again, no. There's just too many things that can go wrong. So as soon as it moves to "Yes, we've actually shipped it, and it works," then it's like, okay, sign - I only use one credit card anyway. My best friend has a wallet that's probably throwing his back out, it's so thick, full of - because he travels for a business, and he's got hotel cards and airline cards and rental car cards and everything. So, yeah, I could see where for many people collapsing them into a single card would make sense. But, no.

Leo: You have to charge this one every month, too, which is kind of weird.

Steve: Yeah, exactly. I mean, there are just - there are downsides.

Leo: Yeah.

Steve: So someone named, I don't even know how to pronounce this, Qrex. It's probably something that was available on Twitter. His name is Qrex, and his Twitter handle is @qrex. He said: "Confused re SN-619 HTML5."

Leo: [Laughing]

Steve: He wrote - uh-huh. He wrote: "So privacy and security are good, unless it's media, and it's between a company and their subscribers? Explanation?"

Leo: That's a good point.

Steve: I know. That one, it gave me some pause. And so I thought, okay. Here's how I - and really, I had to think about this for a while. Privacy and security are good unless it's media, and it's between a company and their subscribers. Okay. Valid point. The MPAA, let's remember, fought mightily to completely prevent the commercialization of consumer home recording. When that inevitably failed, content providers attempted to thwart the consumers' legal right to make copies of their legally obtained media.

Early analog VHS tapes were protected with a system known as Macrovision, which deliberately messed up the automatic gain control, the AGC, of recorders, preventing the duplication of such protected content. This also lowered the delivered quality of the result. But the publishers didn't care. It also didn't work to prevent copying. Before long, Macrovision stripping boxes appeared which removed that protection. So it increased the cost of everything, reduced the quality of the result, and didn't prevent anyone who actually wanted to make a copy from doing so. Pirates continued to pirate.

In the U.S., as we know, our copyright laws provide exemption for fair use. But media DRM does not honor that right. The most famous examples are probably DVDs, whose encryption was broken long ago. And early in this podcast we talked about the problem, the fundamental problem of a DVD player needing to decrypt the encrypted disk in order

to show it to you. The decryption has to happen there, in your living room.

So yes, it can be cracked. And as of course we know, it was broken long ago, allowing owners now of those DVDs to legally, even if against the overtly restricted express wishes of the media's publisher to rip and decrypt DVDs for more convenient, and I would argue also more reliable, because we know DVDs don't last forever, storage and use. The silver oxidizes over time, and a DVD can become unplayable. But if you ripped it and stored it on a hard drive, it could last longer, potentially.

And of course more recently we have HDMI's HDCP, the High-bandwidth Digital Content Protection, which forces another significant compromise. Once upon a time it was possible to instantly switch media sources and destinations in the blink of an eye. But that smooth operation has been messed up by HDMI's HDCP. Now, when switching, it's necessary to wait for at least several seconds for the endpoints to renegotiate their secure connection. And when that fails, as it occasionally does, you have to switch away and back again and hope. And HDCP limits cable length which can be used reliably because it's the most finicky protocol in the entire system.

And HDCP also has been completely bypassed. The market is chockful of $39 Chinese HDMI HDCP decrypting capture cards, which contain all of the standardized and well-known HDCP keys and render the entire system ineffective. If pirates wish to pirate, they can and do. But in the meantime, everyone else, all legal and legitimate users suffer significantly lower quality experience because the MPAA once again won their legislative lobbying victory.

So will the web be any different? Of course not. It will be every bit as possible for pirates to decrypt and capture web-delivered media as it has been for them all along the way. You can place your bets on that right now. The people who realistically understand this know that we're going to get a fragile and unnecessarily complex system, which will be less comfortable and convenient for legitimate and legal use, while doing little to actually thwart those who are intent upon pirating the web-delivered content.

The bottom line is what the MPAA and RIAA want is simply impossible for technology to deliver. Yet the money we have paid them allows them to continually screw up, with no apparent success, their media's delivery channel. So, yeah. This is a bit different from protecting our logon, password, and session cookies. And that's our show.

Leo: Wow. Jam-packed with security goodness. Steve Gibson is at GRC.com. When you go there, check out SpinRite, the world's best hard drive maintenance and recovery utility. That's his bread and butter because everything else there is free, including copies of this show, 64Kb MP3 audio, finely written transcriptions, so you can read along as you listen, and of course all that other great stuff he puts up there for all of Steve's wide and varied interests, including SQRL and Perfect Paper Passwords and Password Haystacks. And there's a great password generator there, people keep reminding me, a great 64-character password generator.

Steve: Yup.

Leo: It's all there, GRC. It's fun to browse around, too. It's like Grampa's attic.

Steve: Grampa, wonderful.

Leo: If Grampa were a crazy security guru. Hey, we're the same age. I can say that.

Steve: Hey, no offense taken, my friend.

Leo: Uncle Steve's attic, how about that? We also have audio and video of the show, if you want to watch Steve in action and see his mug and the mug. Just go to TWiT.tv/sn. By the way, TWiT.tv/teespring for the T-shirt. The mug will be added soon. Steve gave his thumbs-up. We put, I admit, peer pressure. But that's, you know what, sometimes you have to.

Steve: It looks good.

Leo: I think it looks great. I can't wait to get one. We'll send you a few, too.

Steve: Cool.

Leo: If you go to TWiT.tv/sn you can also subscribe there, and that's what I recommend. That way you'll get every episode. There are quite a few, and many more to come. Steve's pledged to stick with us till 1,000. So a whole 380 episodes still to come. TWiT.tv/sn, or use your podcast client, whatever you use to listen to podcasts, to subscribe. We do this show every Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC, right after MacBreak Weekly So if you'd like to watch live, I encourage you to do so. TWiT.tv/live has live video streams on the services I mentioned earlier, plus audio streams, and we're on TuneIn.

You can listen on your Amazon Echo, as well. Oh, she wasn't listening, I guess. Just actually you can watch live by saying "Echo" or whatever your trigger word is, "Watch TWiT Live on TuneIn," and it will play for you. Sometimes you have to say "TWiT Live" for some reason. I'm not sure why. You can also say, "Echo, listen to Security Now! on TuneIn," and you'll get it that way. And that way you'll get the latest episode. That's kind of a fun way to listen, while you're cooking or whatever else you're doing.

Let's see. What else? Oh, if you're watching the live stream, I would invite you to visit the chatroom, irc.twit.tv, because you can play along with the home version of our show and all the crazy kids in there. Thanks for joining us. We'll see you next time - bye, Steve - on Security Now!.

Steve: Thanks, Leo. Bye.