Mobile & IoT Nightmares

Description: Leo and I discuss this week's major dynamic duo stories: Samy Kamkar is back with a weaponized $5 Raspberry Pi, and el cheapo Android phones bring new meaning to "phoning it in." Another big unrelated Android problem; watching a webcam getting taken over; Bruce Schneier speaks to Congress about the Internet; another iPhone lock screen bypass and another iPhone lockup link; ransomware author asks a security researcher for help fixing their broken crypto; Britain finally passed that very extreme surveillance law; some more fun miscellany, and more.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-587.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-587-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got a response from the LessPass guy. We're going to talk about some amazing wild hacks, as always, in IoT and mobile, and a breakthrough in space travel. Or is it? It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 587, recorded Tuesday, November 22nd, 2016: Mobile and IoT Nightmares.

It's time for Security Now!, the show where we protect your security, now, with this guy, Steve Gibson. He's the security guru.

Steve Gibson: Little distracted.

Leo: What are you looking at? What are you looking at over there? Bandwidth?

Steve: Well, yeah. So I was talking to you before the show. I wanted to, for what it's worth, apologize to our listeners for the crappy audio that we had last week. And video, for those of you who also saw that. I don't know that it's going to be any better. We can hope. Last week our traffic was being relayed through Microsoft. And in fact, on the first page of the show notes I show four different sets of traffic that arose. The bulk of it was, in that first line, 60 megabytes, or maybe that's megabits. I'm not sure what their designations are there. But it was all being bounced through, I mean, at my end the traffic was going to Redmond. Then there was a brief attempt to send it to Rio de Janeiro at Telemar Norte Leste in South America.

Leo: What?

Steve: Then there was an attempt to send it to Microsoft in Washington, Virginia; and then another one to Microsoft in Chicago, Illinois. So the problem is this is a proprietary teleconferencing system. This is not our own. We're completely victims to what Skype decides to do. And, unfortunately this week, I'm looking at the technical information here, and UDP relay is up again. It used to say "direct connect." I'm telling Skype to use a port, like to specifically bind to a specific port, and that's mapped out to the Internet, and Skype knows that.

So I have a listening port on my network that allows you guys, even if you didn't have port mapping statically port-mapped, it allows you to reach me directly. And so what we've traditionally had was a direct connection between you and me. And so the good news is then we're only dependent upon our systems at each end and the network between us. But with a UDP relay, all of our traffic, yours coming to me and mine coming to you, bounces through Redmond. And so if they hit a rough patch, we suffer. And I can't see anything at my end that I can do differently or that you can do differently.

They did announce, Microsoft did say about a year ago that they were going to be abandoning the peer-to-peerness of Skype. And, I mean, among other things, this does allow them, if they needed to, to monitor their Skype conferences. In a direct connection, they can't monitor for law enforcement reasons. This gives them the ability to do so. So anyway, I don't know how long it's been relaying. I've heard some of our listeners say that, oh, like for the last eight weeks, I mean, they were quoting which episode it was, like 580, where it began to be a problem. So let's hope it's better this time.

Leo: Yeah. That's all we can do.

Steve: Yeah. So this was going to be a Q&A. And once again - and I have so many good comments from our listeners. I just keep pushing them down because this was another week - I hope the hackers take Thanksgiving off. Just, you know, hackers, just stop. We've got too much. So this podcast, 587, I decided I had to title "Mobile & IoT Nightmares" because there's just too much that happened that we need to talk about. The top two stories of the week is our old friend Samy Kamkar, whom we've discussed. He's a hacker of some repute. He's back with a weaponized $5 Raspberry Pi that actually follows up on a story we covered a couple months ago, in September.

Then we've got the problem of el cheapo Android phones bringing new meaning to the term "phoning it in." There's a different big unrelated Android problem. Rob Graham, our friend from Errata Security, who was the original author of the BlackICE IDE firewall, watched his webcam getting taken over and has some interesting feedback about that. Bruce Schneier spoke to Congress about the sorry state of the Internet. And despite being an anti-government, almost an activist, you know, we've sort of seen Bruce almost kind of get radicalized after the Snowden stuff, it's a little frightening to hear what he has to say.

Yet another iPhone lock screen bypass, and an iPhone lockup from a link. A weird instance of a ransomware author asking a security researcher for help in fixing their not-quite-right crypto, and the ethical dilemma that's put him in, which I'll explain. We've got legislation that has been looming in Britain passed, and some miscellany, and more. So I think another great couple hours of podcast.

Leo: Sounds good to me. All right. Now that you have resumed your normal size on the screen behind me, let's get going.

Steve: Yeah. So we'll keep our fingers crossed about the quality of the connection. I wanted to follow up, in sort of a heartwarming fashion, about this guy who I kind of beat up on last week, the author of LessPass.

Leo: Yeah, I was wondering, if he was listening, how he was going to feel about that.

Steve: Yeah. So he was listening. And in fact we made about a 10-minute snippet of the podcast, a TWiT Bit, titled by your guys, or maybe I said it and they just used the title, I don't remember, but it's on YouTube, "The Horror of LessPass."

Leo: Oh, I'm so sorry. But, well, I mean, frankly, it wasn't inappropriate.

Steve: No. And so, but I'm so impressed with the nature of his response. And there are some good security lessons in here, too. So someone named @numerodix tweeted to Vincent - that's the first name of the author - and me, "That's the first time I've seen a code review in a podcast. Pretty cool." Speaking of, you know, my explaining as I did last week, where the week before was here's the problems with the concept, with the user interface; and then Adam, one of our listeners, shot me a note saying, "Did you look at the code?" And that's, of course, what we talked about last week, was how broken this was as a generator of high-entropy passwords, which it isn't because by design its decisions made it predictable. So then Vincent replied, so he must be following me because he would have seen that - oh, no, actually this @numerodix did mention him. So it went to him, too.

Leo: Yeah. We get, you know, the thing is, even if people don't listen to the show, there are plenty of people on Twitter who will tattle on us. So I assume that anything we say about anybody will get back to that person via Twitter.

Steve: So he responds: "Yes, I'm obviously not happy with this video, but I'm glad that people are studying the code in depth." Okay, well, now, that's, like, remarkably right for him to say. And then he tweeted to me the link to "The Horror of LessPass" on the TWiT netcast network. And he sent me a link to the GitHub thread where he's completely explained his position. And so he wrote, "The interview went to says," and so he's probably a non-English speaker, so he meant "went on to say." And then he quoted me saying, "Your goal is to make your password as random as possible, so anything that reduces randomness or entropy is going to reduce the effectiveness of your password and is going to increase its brute-forcibility."

And then he said: "Understanding our mistakes: We use patterns to create passwords with complex rules like no consecutive vowels or can't start with a number. We made two mistakes," he wrote. "First, we did not understand at the beginning that the entropy of the generated password increased the brute-forcibility of the master password." Okay, and he doesn't quite understand the problem there, but that's okay. "I took the idea of

password templates from Master Password algorithm. We misunderstood and took for granted what we read." Then he said: "Then it was to define as template by default consonants, vowels, et cetera, instead of a more random one as X with the full character set." So he does understand what the requirement is for a high-entropy password.

And then, on the topic of open source, he wrote: "And for anyone who thinks they do well at first, or who think that open source does not help, on the contrary, we believe that nobody does well at first; and, thanks to the community scrutiny and critical studies of the code, this kind of tool becomes more robust the longer it lives."

Then he said, under how it feels: "The video is obviously a setback for us, especially after the euphoric past week where we went from about 100 to 1,600-plus stars. But we are glad that people review our code in depth, and this came up early on." And then, finally, actions: "We will use the full alphabet in the next version by default. We will probably increase the default length of generated passwords. So in the future we will describe, with drawings, the future algorithm and its implementation. We will simplify the code to help everyone understand how it works. And we hope you will keep your eyes peeled for mistakes and stay critical to the code."

So to all that I say bravo. I mean, we know that's all good news. The lesson, of course, is - and I think this is an important takeaway for our listeners, who were all excited about the appearance of this new interesting password generator. And so the takeaway is, looks nice on the surface. I immediately saw reasons why, on the surface, it would be impractical to use. And then what we discovered is, again, thanks to it being open source - although, as I also said last week, if you generated three or four passwords with it you'd quickly notice that they were all the same in terms of what characters were appearing where, and it was only the choice of characters that were changing. So even its behavior would have been quite clear. And as I said last week, I mean, we have essentially a security and cryptography amateur who's writing code. There's nothing wrong with that except that 1600-plus stars indicated that lots of people grabbed it and said, "Oh, what a fabulous idea, I love this," and they're off and running.

Now, in the thread that followed, some other people noted, well, you know, if you change your algorithm, that's going to change the passwords generated with the same parameters that Version 1 generated, so you're going to break everyone's Version 1 passwords. And so he's planning to have them both available for some overlap period and try to migrate people. Anyway, it's a mess. But I have to tip my hat to Vincent. His attitude is terrific.

But this should be a lesson to us, sort of amplifying on what I said last week, that this stuff, and in fact the whole content of this podcast, is demonstration of this stuff is hard. And there are certainly malicious actors that hide what they're doing, or use crypto for malicious purposes. Then there are people like Vincent, who has clearly the best of intentions, but shouldn't be offering to the public something that hasn't been tested and looked at. And I think that's probably the responsible thing to do. He should use it for himself and maybe solicit some feedback in a more controlled fashion before just putting it out there and saying, "Here's a free password generator, have fun." So anyway, again, I just wanted to say, you know, I think his heart is in the right place. But that isn't enough. You actually have to understand a lot in order to do this right.

Now, speaking of understanding a lot, as you said, Leo, you're going to have Samy Kamkar on, which I think will be great. He is a real character. And, I mean, and a class-act hacker. I have a video, he's produced a video of what he has done recently that was up there as one of the top two stories of this past week, just in terms of our listeners making sure I knew about it. He's created something he calls "Poison Tap." And it's

exploiting locked computers over USB. And he went public with this last Wednesday.

Now, if you ask yourself, why does that sound familiar, it's because this is a weaponized extension of the exploit we discussed in early September, a different hacker named Rob Fuller. And we gave it full coverage in the beginning of September. He created a posting, "Snagging Creds from Locked Machines." And at the time he was using a much more expensive, I think it was $155 computer-based USB dongle. And the idea is, and we discussed it then, that when you stick a USB into a machine that is on, even if it's locked, if the lid's closed, if it's, like, inaccessible, if that USB device claims through the USB enumeration to be a network adapter, unfortunately, it instantly gets all kinds of unquestioned privilege.

And so Rob showed us early in September how he was able to take a USB Ethernet device and exploit some features of DHCP, the dynamic host configuration protocol, with another person's responder software, in order to essentially get the password hashes from the system and then perform an offline brute-force attack in order to crack the passwords. And this is a problem that Windows has had for a long time. Their earlier, especially their earlier password hashing was not very good, you know, the old LANMAN. We were talking about that a lot a decade ago.

So that was then. Now Samy came along and said, "Oh, that's interesting." And he rolled up his sleeves and just went to town. So this thing, he calls it "applied hacking" is sort of his banner. And so Poison Tap siphons cookies, exposes the internal router, and installs web backdoors on locked computers. It produces a cascading effect by exploiting the existing trust, as he describes it, in various mechanisms of a machine and network, including USB or Thunderbolt, DHCP, DNS, and HTTP, to produce a snowball effect of information exfiltration, network access, and installation of semi-permanent backdoors - using a $5 weaponized Raspberry Pi Zero.

So essentially the problem is, when a network interface spontaneously appears, the operating system enumerates it, says, oh, you know, the user must want to get on that network. And so the first thing that happens is it receives a DHCP query. Well, DHCP is very powerful. And we've talked about it extensively in the past. The minimum thing that it does is give you an IP address. It can also give you DNS. And it can also declare various routing parameters, that is, DHCP is way more than just IP and DNS. There's an extensive vocabulary of what it's able to offer.

So by leveraging the fact that an innocent computer made the mistake of querying a very powerful malicious DHCP server - which nothing prevents, essentially - he's able to roll that into, sort of incrementally, by gaining a foothold, doing something, and then pushing it further, and then substantiating that position, basically just walk into your computer and take it over, ending up, for example, rerouting all of the traffic that the machine is sending on a valid interface through it. So it's able to, if you're not using HTTPS to strip headers, to prevent security provisions that are by default available in HTTPS because of course the tunnel is unencrypted. So by intercepting the traffic he's able to - basically this is a full exploit by somebody who knows what he's doing, very creative, to completely compromise the browser aspect of web surfing on that machine, even to the point of leaving some stuff behind, which continues to have an effect.

So it's a breathtaking compromise, all based on this idea that a USB device which should not be trusted might be a network, and the fact that our systems at the moment, they don't pop up a dialogue. They don't make you click okay to confirm that you want to enumerate this newly appeared network device. They just do it across the board.

So he says, for features: "Emulates an Ethernet device over USB; hijacks all Internet

traffic from the machine despite being a low priority, unknown network interface; siphons and stores HTTP cookies and sessions from the web browser for the Alexa top one million websites." Now, he does that because, remember, any time your browser responds to a request from one of those sites, it will send whatever cookies it has. So Samy injects a million tiny hidden iFrames into the page. Each of those makes a query to one of a million websites. And that query will contain all the cookies they have. He intercepts that and grabs them. So he has all the cookies that your browser has for Alexa's top one million sites.

And if any of your sessions are statically logged on, like you click the box "Remember me" so you don't have to reauthenticate every time, well, that means that that cookie represents you for your logged-on session. And that's then exfiltrated, which his technology also does. A remote hacker could then immediately jump on, authenticating as you on that site. Just like you open, you know, just like you went to the site fresh, and it remembered that you had been logged on before, and you said don't ask me anymore.

He's able to expose the internal router - that is, your internal router that you're connecting to the Internet by - to an external attacker, making it accessible remotely via an outbound WebSocket and DNS spoofing. He can install a persistent web-based backdoor for HTTP cached objects for hundreds of thousands of domains. He even poisons JavaScript libraries being sent by major content delivery networks; does not require the machine to be unlocked. And these backdoors and remote access persist even after the device is removed and the attacker, as he puts it, "sashays away." So it's a great video. I'm delighted that he's going to be on Know How because I'm sure - and I would give our listeners a pointer to that, Leo.

Leo: Oh, yeah. Oh, yeah.

Steve: Because I'm sure they will get a kick out of it

Leo: I'm not sure what week. But, yeah, it'll be fun, yeah. And then we will, the following - as soon as they tape that, we'll put a bit of it into New Screen Savers. But, I mean, it's one of those things where I think we want to spend some significant time with him, demonstrating the whole thing.

Steve: Yeah, well, and for securing against it, notice that everything I was talking about, that is, in terms of traffic capture, since he isn't and probably can't mess with cookies, I mean, I'm sorry, mess with certificates, there's no way for him - and he says that all of this is HTTP. So for servers to secure against this, the only thing servers can do is use HTTPS exclusively; use HSTS, the Strict Transport Security, to allow browsers - because when users don't put HTTPS into the browser, they typically just www.

And we've talked about how unfortunate it is that browsers still try HTTP as the default protocol. It'll be interesting to see when that changes. I wouldn't be surprised if that's something that we see Google lead with, with Chrome, when their tests have demonstrated that it won't break too many things. Because it would sure be nice if at some point browsers, instead of defaulting to HTTP, first tried HTTPS, or maybe tried them both at once and used the more secure, the HTTPS, if it also succeeds, when they haven't been told one way or the other.

And then, finally, remember that cookies, when cookies are set, they can have a secure

flag set which prohibits the browser from sending them with its queries over a non-HTTPS connection. So if all the cookies, like session cookies, for example, which are sensitive, if those had the secure flag set, then they would not be exposed in an HTTP attack. And on the desktop side, he says, you know, that's fine for the servers. On the desktop side, Samy suggests, as he put it, "Adding cement to your USB and Thunderbolt ports can be effective."

Leo: Not on my new MacBook, no way.

Steve: No. And he says: "Closing your browser" - that is, shutting the browser down. "Closing your browser every time you walk away from your machine can work, but," he says, "is practically impractical. Disabling USB or Thunderbolt ports is also effective, though also impractical." And he says: "Locking your computer has no effect, as the network and USB stacks operate while the machine is locked."

Leo: Oh, that's interesting.

Steve: Yeah, it is. "However, going into an encrypted sleep mode," meaning, you know, where it writes the RAM out and encrypts it...

Leo: Hibernation.

Steve: Hibernation, right, he calls it "encrypted sleep," "...where a key is required to decrypt the memory" - and he says, for example, FileVault 2 and deep sleep - "solves most of the issues as your browser will no longer make requests, even if woken up." And for all this, the source code is on GitHub. So, and this is not, I mean, there's no one to disclose this to responsibly. This we knew about in early September. He's just taken it to its logical extent, that is, oh, wow, you mean I can get a - the machine is going to make a DHCP query of my own little custom DHCP server when I plug it into USB? Oh, I know what I can do with that.

And so here's another instance, as we often said, that attacks never get worse, they only get better. And so this is three months' worth of evolution of a problem. And again, this isn't exploiting any vulnerability. There's nothing to fix anywhere except, maybe, if a machine is locked and closed, you might wonder why the OS would default to enumerating and bringing that port online. And maybe even the default option should be always prompt before recognizing a new network connection to this machine because, as we're seeing, network connections are dangerous. They just get up to too much mischief.

Now, the second biggest story, or equally big, but the other one of the top two of the week was the discovery of very widespread and clearly deliberate malware installed in low-end, low-cost Android mobile devices. A company or a group we've never discussed before, I don't remember us mentioning them, Kryptowire with a "K," discovered mobile phone firmware that was transmitting what they say throughout here, PII is the acronym that we've used before, Personally Identifiable Information, without users' consent or disclosure.

Kryptowire, and this was last Tuesday, and so a week ago, while we were doing the podcast, "identified several models of Android mobile devices that contained firmware

that collected sensitive personal data about their users and transmitted this sensitive data to third-party servers without disclosure or the users' consent. These devices were available through" - and "were" seems to be the operative term there, as I'll explain in a second - "through major U.S.-based online retailers like Amazon and Best Buy and included popular smartphones such as the BLU R1 HD."

Now, who's Kryptowire? Well, first of all, they're the real deal. Kryptowire was jumpstarted by the Defense Advanced Research Projects Agency.

Leo: Oh, wow.

Steve: Also known as DARPA, and also the Father of the Internet; and the U.S. Department of Homeland Security. Kryptowire provides mobile application security analysis tools, anti-piracy technologies, mobile app marketplace security analytics, and Enterprise Mobility Management solutions. Kryptowire was founded five years ago, in 2011, and is based in Fairfax, Virginia.

Leo: Oh. Oh.

Steve: And has a customer base ranging from government agencies to national cable TV companies.

Leo: Huh.

Steve: So, yes, not some obscure little group somewhere. These guys are connected. So, first of all, I wanted to substantiate that this wasn't some random obscure phone that five people had. In August this year, so five months ago, or four months ago, Ars Technica reviewed this BLU R1 HD under the title: "A $60" - and actually it's 50. Maybe the price has dropped since then. It's zero now - "A $60 Amazon phone that's way better than Amazon's actual phone."

Leo: Mm-hmm. Yeah, we've talked about these BLU phones before. They also make a Windows phone. They're just cheap phones.

Steve: Right, they're just cheap phones. And then, you know, "Selling your lock screen to Amazon," writes Ars, "cuts the cheap phone's price in half." And it's funny because on the - oh, and BLU stands for Bold Like Us. Yeah.

Leo: Oh, I didn't know that.

Steve: Yeah. On their site they proudly boast - "The Rebel in You" is their slogan - starting at $49.95, exclusively on Amazon. Now, if you go to that link, Amazon says "currently unavailable." But it has 3,202 reviews. So again, not obscure.

PC Magazine looked at it this summer. They said the pros, in their summary:

"Inexpensive, study build, solid battery life, latest Android software, dual SIM card slots, and expandable storage." Cons was "Prime-subsidized phone includes Amazon bloatware and advertising and" - as we're about to find out - "and a lot more." And they were unimpressed by the camera. But they said, as their bottom line: "The BLU R1 HD is an unlocked Android phone with a good balance of performance for the price, making it a fantastic value for Amazon Prime users and regular customers alike."

And even Wired, in July, I mean, so everybody was covering this, saying, wow, 50 bucks for a completely workable phone. And we know that many people are price-based shoppers. They're price-sensitive. And so if there's, like, this well-reviewed phone, it may have some limits, okay, so it's not a great camera, but otherwise, oh, Android, you know, everybody else that I know has one of those, so what the heck?

Anyway, so Kryptowire continues, saying these devices - so this is what they were getting up to that they found - actively transmitted user and device information, including the full body of text messages, contact lists, call history with telephone numbers, unique device identifiers including the IMSI, the International Mobile Subscriber Identity, and the IMEI, the International Mobile Equipment Identity. "The firmware could target specific users as text messages matched remotely defined keywords." So, I mean, this isn't casual. This is seriously weaponized malware.

"The firmware also collected and transmitted information about the use of applications installed on the monitored device, bypassed the Android permission model, executed remote commands with escalated system privileges, and was able to remotely reprogram the devices. The firmware that shipped with the mobile devices and subsequent updates allowed for remote installation of applications without the users' consent and, in some versions of the software, the transmission of fine-grained device location information.

"The core of the monitoring activities took place using a commercial Firmware Over The Air update system that was shipped with the Android devices we tested and were managed by a company named Shanghai Adups [A-D-U-P-S] Technology Co., Ltd. Our findings," they write, "are based on both code and network analysis of the firmware." So they reverse-engineered the code and intercepted and looked at the actual traffic that the phones were generating.

"The user and device information was collected automatically by this firmware and transmitted periodically without the users' consent or knowledge. The collected information was encrypted with multiple layers of encryption and then transmitted over secure web protocols to a server located in Shanghai. This software and behavior bypasses the detection of modern anti-virus tools because they assume that software that ships with the device is not malware [by definition] and thus is whitelisted.

"In September 2016, Adups claimed on its website to have a worldwide presence with over 700 million active users, and a market share exceeding 70% across over 150 countries and regions with offices in Shanghai, Shenzhen, Beijing, Tokyo, New Delhi, and Miami." They're also in Florida, is actually where their U.S. headquarters is. "The Adups website also stated that it produces firmware that is integrated in more than 400 leading mobile operators, semiconductor vendors" - oh, help us - "and device manufacturers spanning from wearable and remote devices to cars and televisions."

And then, in a chart in their description, Kryptowire compares this with something that you and I, Leo, talked about. You'll remember five years ago there was this spyware called "Carrier IQ" which was discovered in some phones that was an early version, I mean, basically it was them, their sort of analytics system installed by a third party with the carrier's, you know, at the carrier's behest so that they could collect data on their

users. Once that came to light, of course, it was removed. So in their chart, basically, they go through an AB comparison with checkboxes and red X's about which features this thing supports and which features Carrier IQ - it was more sanctioned, even though it raised a lot of concerns at the time.

Leo: Oh, it was installed by carriers at the time; right?

Steve: Correct. Correct.

Leo: And I have a feeling these both have the same purpose, which is not for government snooping, but for advertising, right, to get information about you so they can serve you ads. That was the purpose of the Carrier IQ, as well.

Steve: Yeah. Although this is, I mean, this was - I guess the question would be who knew about this.

Leo: Right. BLU says they didn't.

Steve: Correct.

Leo: Right.

Steve: Correct. So anyway, basically we have a huge number of very inexpensive phones that, across the board, are, I mean, they are pocket spyware machines. Everything that is going on is being reported back to the mothership over these phones. Now, Amazon, of course, immediately took it off the market. And I hope this will be, I mean, I hope there's some downstream lesson to be learned by the likes of Amazon because, of course, their reputation is there. They lowered the price, cut it in half in order to have an Amazon-populated lock screen. So they bear some responsibility, I would imagine. And I hope that a lot of customers are going to have to say or will say, you know, I've had this for six months, but you're taking it back because, you know...

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

Steve: ...I bought this, and it's got spyware in it. Wow. And I don't know what this means. Amazon tried to do their own phone, which was a colossal failure. So this has been their new approach.

Leo: Well, they do this with a lot of phones, including flagship phones and stuff. They just subsidize them and sell them.

Steve: Right, right.

Leo: I don't, yeah, I mean, I don't really blame them for this. It'd be hard, I mean, nobody knew about it; right?

Steve: Yeah. I mean, yeah. And they're also selling webcams that are being exploited by the Mirai botnet and other malware. So we'll get to what Bruce Schneier says about this and where the world is heading pretty soon.

So right on this topic, too, another company, AnubisNetworks, found another Android phone - well, and unfortunately it's also one of these BLU phones, the BLU group. Their over-the-air update mechanism was extremely vulnerable to attack. And Anubis wrote: "In this article, we will be detailing an issue we discovered affecting a number of low-cost devices. It allowed for adversaries to remotely execute commands on the devices as a privileged user, if they were in a position to conduct a man-in-the-middle attack. The binary responsible appears to be an insecure implementation of an over-the-air mechanism for device updates associated to the software company Ragentek Group in China. All transactions from the binary to the third-party endpoint" - get this - "occur over an unencrypted channel."

Leo: Uh-oh. And we know why that's a problem.

Steve: So you've got unprotected, unencrypted, which means unauthenticated, thus a man-in-the-middle, over-the-air update of the phone's firmware. I mean, it's malpractice. And they say, "...which not only exposes user-specific information during these communications" - so there is that, too; PII is exfiltrating - "but would allow an adversary to issue commands supported by the protocol. One of these commands allows the execution of system commands. This issue affected devices out of the box." So no additional vulnerabilities to install, no compromise, just clean out-of-the-box. So again, designed this way. Now, I'm going to skip over a lot of the details here because there was one that just jumped out at me, which is where the term "malpractice" came from.

They said: "We acquired one of the affected devices, a BLU Studio G, from Best Buy. After building a passive network traffic-capturing system" - so they just tapped and listened - "an unencrypted transaction to the Ragentek head-end" - at the domain oyag[.]lhzbdvm[.]com, which that's just random gibberish. So they just made up some domain name so that, you know, and they probably registered it with some really bottom-of-the barrel registrar so they didn't have to pay anything. So just a garbage domain name was observed, that is, traffic, unencrypted transaction was observed "not long after proceeding through the Android first-use setup process on the device."

Now, get this: "The device then attempted to contact two other pre-configured domains, which were previously unregistered until AnubisNetworks acquired them. This gave us immediate visibility into the larger population of affected devices, which are detailed later in this article. We were able to associate the network transactions back to specific binaries on the device which were the ones investigated as part of this analysis." So they watched the device do a DNS query to this oyag[.]lhabdm[.]com. Then they saw two additional DNS queries to the same oyag dot, but then prugskh[.]net and .com. When they looked those up, the domains weren't even registered. So they registered them.

Leo: Oh, my god. You don't even need a man in the middle.

Steve: No.

Leo: Oh.

Steve: Oh, it's unbelievable. I mean, this is where I said this is malpractice. And so somebody in China...

Leo: They forgot. They forgot.

Steve: I mean, like, maybe they thought, well, you know, we'll register a couple more in case we ever need them for some reason. And so they thought, well, but, you know, no reason to have a DNS server there because the primary one is there. But the devices are still querying. So Anubis registered those two wacky domains. Then the devices started querying them. And then they were able to respond and become part of the network, and thus enumerate what was going on.

They write: "We have observed over 2.8 million distinct devices, across roughly 55 reported device models, which have checked into our sinkholes since we registered the extraneous domains. In some cases, we have not been able to translate the provided device model into a reference to the real-world device." You know, I mean, they're being passive. They don't want to, like, reach in and figure out what's going on because that would be breaking laws. So they're just passively monitoring traffic in, as they call it, in their sinkholes or their honeypots.

They write: "These are the devices captured in the 'Others' category." Oh, and on their page they show a big pie chart, and less than a quarter were BLU devices, and almost a half of the pie was "Other." And then there were some small chunks, like three or four other manufacturers that they were able to identify the models. And, you know, they're not big names. They're people who chose to use Ragentek's firmware for whatever reason, and Ragentek didn't bother to even register the domains that their firmware was querying. Just, you know, maybe they would need them some day in the future. So, boy.

Leo: Wow.

Steve: In their conclusion they said: "This analysis revealed two critical discoveries: First, the vulnerability described above allows for users to be subjected to significant attacks in positions where an adversary can perform a man-in-the-middle attack. Secondly, this over-the-air binary was distributed with a set of domains preconfigured in the software. Only one of these domains was registered at the time of the discovery of this issue. If an adversary had noticed this" - I mean, and here we're glad that Anubis were the ones who found this. "If an adversary had noticed this and registered these two domains, they would've instantly had access to perform arbitrary attacks on almost three million devices without the need" - as you immediately saw, Leo - "to perform a man-in-the-middle attack. AnubisNetworks now controls these two extraneous domains to prevent such an attack from occurring in the future for this particular case."

And again, our lesson here is spend a little more money and buy yourself some more security, if that's something that you're interested in. And I would imagine anyone within the sound of this podcast is interested in security. So, wow. And maybe you know people

who have these low-end phones, and you can let them know or find out what make and model they are and whether they might be vulnerable to this. Yikes.

Leo: Really kind of stunning.

Steve: Oh, gosh. It is.

Leo: It's just it all feels kind of half-assed; you know?

Steve: Yeah, it is. I mean, it absolutely is. And this is where we are. Here we're looking at the mobile side. We'll get to IoT in a second. But in weeks recently we've been talking about this disaster in IoT. And what's happened is, and Bruce addresses this a little bit later in his presentation to Congress, it's a weird situation where we've got serious technology being mass-produced and used with no oversight. And, now, and imagine if you're a U.S. government person who's responsible for the safety of the networks in this country, and you're reading this, that some Chinese firmware manufacturer has been selling phones in millions to citizens in the United States, and that these phones are all reporting back to Shanghai, and any of them can be taken over remotely. That's a concern.

Leo: Yeah.

Steve: Wow.

Leo: Wow.

Steve: And this is not science fiction. I mean, it sounds like, you know, 10 years ago this would have just been infeasible. This is recent history now. Incredible.

So the 'Net has been reporting, and in fact Christina Warren did a nice piece in Gizmodo on Friday on yet another iPhone lock screen bypass. And these are crazy complicated now. I mean, that's the good news. The bad news is they exist. So Christina wrote, her piece was titled: "This Weird Trick Apparently Lets You Bypass Any iPhone's Lock Screen." And in fact she had a bunch of people at Gizmodo try it on a range of phones, and they were successful.

She says: "First, you need to call the phone you want to gain access to. If you don't know the number, you can ask Siri, 'Who am I?' to get it." And then she says: "A FaceTime call will work as well. Then, from the incoming call screen" - and I'm going through this because I want people to understand how crazy this is. "From the incoming call screen, choose the 'Message' option and choose 'Custom.' That opens up a screen to reply to the call with a message. From here, you need to enable Voice Over mode" - and so this is really where the gotcha is, is in the interaction of Siri and the Voice Over mode - "by invoking Siri and saying, 'Turn on Voice Over.' This will enable an accessibility feature that will read out items on the screen." And I just hit the spacebar and lost my place. On the screen.

"This is where it gets really tricky," as if that wasn't already. "Then you need to double tap on the recipient filed on the message," that is, the name, "while also tapping on a random key on the keyboard. This should open up a 'to' field on the SMS that will then let you search through contacts already on the phone." And then she says in parens, "(You'll know you've gotten the bug to work when you see the tools pop up next to the compose message box.)

"At this point, you've already broken into the phone to a certain degree because you can see all of the contacts. Pressing on an 'i' icon next to a contact should show details about the contact, which will then allow the user to create a new contact. This is where the exploit really becomes useful. Tapping on the 'new contact' button, a user can opt to add in a photo, and doing that will allow access to all the photos on the camera roll. This basically means a skilled person could browse all of your photos without you knowing.

She writes: "Tricks that let hackers bypass any iPhone's lock screen are hardly new, and they typically take a little bit of skill and luck. And although the iDeviceHelp video and others like it are cropping up all over YouTube, it's always safe to remain skeptical about how dangerous these tricks might be. As far as bugs go, this one feels fairly innocuous since it requires prolonged physical access to a device." Although, you know, you can imagine law enforcement would love to know about this. "And although you can access photos, actually doing anything with that data is a different story."

And all over the 'Net where this is being covered, the advice is simple. If you disable Siri on the lock screen and Hey Siri, this stops the security hole. If you do that, then at least you'll have some safety until Apple issues a proper fix. And so my takeaway is somewhat different. It's that, you know, here's a classic example of this all getting too complicated. As we know, and as I often say on this podcast, complexity is the enemy of security. And so Apple keeps adding this or that convenience.

And look at what Samy did, taking a simple concept of a USB device can be a network adapter, which he got from Rob in September when Rob noticed there was a way to exploit that, and how innocuous features, otherwise innocuous features can then use that entry point in order to exploit more. That's exactly what this is. So, and this is the problem is that certainly Apple doesn't want this to happen. They're not happy because here they are all touting they're the best in security available anywhere. And it turns out you can browse the pictures of somebody on a locked phone by cleverly winding your way through a bunch of incrementally revealed capabilities that somebody clever worked out. It's hard to defend that this kind of behavior exists. Yikes.

And Charlie Miller on 9to5Mac reports that - and just for what it's worth to our listeners, there is another iPhone-locking link going around. This doesn't appear to do anything other than bring phones to a crawl and then finally resulting in them locking up. It's an MP4 video. Nobody technical has yet reverse-engineered this and figured out what's happening. So what's happening is people are sending links around to each other, or posting them on Twitter, in a hah hah hah, you know. And then the good news is you do - the bad news is you have to do a full restart of your phone, the power off cold boot, by holding the power button and the home button down, or on the iPhone 7 I think it's the power button and the volume up button. That'll get you back. So if anyone does get bit by that, just doing a - I would imagine ultimately all our listeners would say, okay, I guess I just have to do a hard reset to get back up.

Leo: Why do you think it happens?

Steve: I mean, it could be anything. This is probably a flaw in the MP4 file format interpreter. And this is why it's a concern. Right now all it's doing is messing up your phone. For example, it could be a flaw that ends up consuming memory. So it slowly burns up all of your memory. The phone slows down until finally it just dies in a complete memory consumption, essentially a denial of service of your phone. But this is also the kind of thing that, if not fixed in a week or two, we'll be reading about it having been weaponized. Somebody will figure out what the flaw is because a hacker will go, oh, you know, I mean, they know that this is the way these things begin.

Leo: It's like StageFright. It's something in the media player. And just as with StageFright, they'll figure it out.

Steve: Exactly.

Leo: It's funny why media players seem to have a lot of problems. I guess, but, you know, we go back to the issues that Microsoft had with playing back - with Metafile, Windows Metafile and stuff like that. It's these renderers in Adobe Acrobat and [crosstalk]...

Steve: Yes, the interpreters.

Leo: These renderers, interpreters are really running code when they're looking at the data file.

Steve: Right.

Leo: In effect; right?

Steve: Right, yeah. Our advanced formats now have, you know, they require interpretation in order to execute. Even, I mean, even a decompressor is an interpreter. It's reading instructions embedded in the stream and interpreting how to decompress the file to its original form based on what was there. And so, you know, compressors, compression and decompression is everywhere. And the takeaway is this stuff is hard.

Leo: Yup.

Steve: I got a nice note from a listener, Ben Aylett, in Perth, Western Australia. And his subject was, "Finally!" He said: "I'm a regular technology guest on a local radio talkback station in Perth, Western Australia, and I had a caller tell me about problems he was having with his hard drive. Of course I went right to my favorite hard drive tool - which, of course, was SpinRite. Thanks for making a great tool that I use at least once a month to help out others. It usually brings drives back from the dead, and occasionally confirms my suspicions that the drive is beyond salvation. Either way, I'm proud to share GRC and all your good work with my listeners and clients when I can." So, Ben, thanks for sharing your success.

Leo: Nice. I don't have a commercial. Just keep on going.

Steve: Yeah.

Leo: I mean, if you want to have a drink, I could tap dance. I could sing a song.

Steve: Yeah, I don't think the tap dance would go well over the audio.

Leo: No. By the way, audio and video looking good.

Steve: Oh, I'm glad.

Leo: So I don't know why.

Steve: I'm going to - Mark Thompson is a Skype user. I'll make some time before next Tuesday to mess around with him because he and I can look at each other's traffic and figure out - I'd just like to see why I'm unable to get a direct connection.

Leo: Strange, yeah.

Steve: I'm glad that we're doing better.

Leo: Good.

Steve: Okay. So Robert Graham we've often spoken of. He's Errata Rob, and ErrataSec is his site on the 'Net. He's the original author of the BlackICE early firewall for PCs. He posted his analysis of deliberately hooking a camera to the 'Net. And in fact TechCrunch glued a whole bunch of his tweets together and made a better job of it. And they wrote, and this is a great story: "Here's an object lesson on the poor state of the so-called Internet of Things."

Now, this is interesting, too. They said Robert Stephens. And I thought, what? Um, okay. And they referred to him as Robert Stephens. I've spoken to him. But, I mean, maybe Graham is a pseudonym. I did a little bit of digging around. I couldn't find anything that indicates anything about a Robert Stephens. Everything I found was Robert Graham. And that's how I've always known him. So maybe they know something I don't. Anyway, they said: "Robert Stephens plugged a WiFi-connected security camera into his network, and it was compromised in 98 seconds."

Leo: Geez.

Steve: "Stephens," they wrote - we know him as Robert Graham - "a tech industry veteran" - certainly he is that - "wasn't so naive as to do this without protecting himself. It was walled off from the rest of the network and rate-limited so it couldn't participate in any DDoS attacks." Now, of course, we know from last week rate-limiting won't help necessarily because even low-rate attacks, if they're the BlackNurse - and, oh, by the way, we've heard from the people who named it, and we know why. So we'll get to that in a minute.

So, I mean, he was being as responsible as he could be. So Robert "monitored its traffic carefully, expecting to see, as others have, attempts to take over the device. But even the most jaded among us," writes TechCrunch, "probably wouldn't have guessed it would take less than two minutes." Robert wrote in one of his tweets, "Actually, it took 98 seconds for the first infection." And he wrote that on November 18.

"Ninety-eight seconds after it jumped on the WiFi, the camera was attacked by a Mirai-like worm that knew the camera's default login and password." So, now, imagine. Even with the best intentions, you hook up the camera, and of course you've got to get it on the network in order to talk to it. Before you have a chance to open up and boot your laptop and start configuring it, you've already lost control. Ninety-eight seconds, and the camera is owned. Wow. This is our world.

"The worm - its advance agent, really - checked the specs of its new home and then downloaded the rest of itself onto the device and, had Stephens not locked it down beforehand, would then be ready to participate in all manner of online shenanigans. The camera, a cheap off-brand one from a company that sells smartwatches for $12, isn't exactly best-in-class. This type of thing could be fixed with a firmware update or, in some cases, by simply changing the default password, but not everyone knows to do that." I mean, most people don't. They just plug it in and, oh, look, when they're out at the restaurant, they can see their front yard or their living room or the baby's room, whatever.

"And even the most tech-savvy people might not get that done in two minutes. Better-quality devices will almost certainly be better protected against this kind of thing" - exactly the point I've been making - "and may, for example, block all incoming traffic until they're paired with another device and set up manually. Still, this is a good reminder that it really is a jungle out there." And remember, now, also the other problem we have is that these devices were not designed for us, listeners of the podcast. They're designed for the hundreds of millions of people that want a camera, and so they buy one. And they plug it in and point it in the direction they want, and then they read the instructions that say go to this website and look at yourself. I mean, these things are just - people are installing spies, literally and figuratively, in their homes constantly now as a consequence of what has happened.

So Bruce Schneier gives Congress some sobering truth. The Daily Dot reported on this, saying: "Speaking before members of Congress, the Internet pioneer" - referring to Schneier - "made clear the dangers of the Internet of things" - now, this is what they need to hear - "saying, 'The Internet era of fun and games is over.'" The Dot wrote: "Internet pioneer Bruce Schneier issued a dire proclamation in front of the House of Representatives' Energy & Commerce Committee last Wednesday: 'It might be that the Internet era of fun and games is over because the Internet is now dangerous.'

"The meeting, which focused on the security vulnerabilities created by smart devices, came in the wake of the October 21 cyber attack on Dyn that knocked Amazon, Netflix, Spotify, and other major web services offline." Oh, and speaking of Dyn, by the way, Oracle has just bought them.

Leo: Yeah, is that a coincidence? That's weird; right?

Steve: It is weird. I was wondering if their stock was depressed as a consequence of the cyber attack, making them vulnerable to purchase.

Leo: Right.

Steve: "Schneier's opening statement provided a clear distillation of the dangers posed by connected devices." And there is a video of him, for anyone. But for the podcast we've got all of the good points pulled out.

Here's how he framed the Internet of Things, or what he later called the "world of dangerous things." So Bruce says, speaking to Congress: "As the chairman pointed out" - the chairman of the committee - "there are now computers in everything. But I want to suggest another way of thinking about it in that everything is now a computer. This is not a phone. It's a computer that makes phone calls. A refrigerator is a computer that keeps things cold. ATM machines are computers with money inside them. Your car is not a mechanical device with a computer. It's a computer with four wheels and an engine."

Leo: Yeah, especially my car, which is basically an electric - a computer on top of an electric go-cart.

Steve: And let's hope it goes forward.

Leo: Oh, my god, yeah, exactly. I mean, it's so obvious that everything is drive-by-wire on that Tesla.

Steve: Yeah.

Leo: Yeah.

Steve: And he says: "And this, gentlemen, is the Internet of Things, and this is what caused the DDoS attack we're talking about." He then outlined four truths he's learned from the world of computer security, which he said is now "everything security."

First principle, first of the four: Attack is easier than defense. And of course that's one of the principles that we live by on the podcast. Bruce said: "Complexity is the worst enemy of security. Complex systems are hard to secure for an hours' worth of reasons" - which he did not go into because they would have glazed over - "and this is especially true for computers and the Internet. The Internet is the most complex machine man has ever built by a lot, and it's hard to secure. Attackers have the advantage."

And I really like that. Think about it. We tend to look at the Internet in pieces because we deal with it in pieces, you know, things that you connect to it. But Bruce flipped this around, I think, in a really interesting way, thinking of the Internet itself as an entity and

with all of these computers on its endpoints. It is the most complex machine we have ever built by a huge margin.

His second principle: There are new vulnerabilities in the interconnections. And in fact this is exactly that iPhone lock screen point, you know, it's the way things interact. And it's the same thing with Samy's exploit of an enumerated network interface. It's the interactions of individual things that are not by themselves devastating, but they'd be combined. Bruce said: "The more we connect things to each other, the more vulnerabilities in one thing affect other things. We're talking about vulnerabilities in digital video recorders and webcams that allowed hackers to take websites. There was one story of a vulnerability in an Amazon account that allowed hackers to get to an Apple account, which allowed them to get to a Gmail account, which allowed them to get to a Twitter account." I think he's talking about Mat's.

Leo: Yeah, that's Mat Honan's attack, yeah.

Steve: Yeah. "Target Corporation, remember that attack?" he says? "That was a vulnerability in their HVAC contractor that allowed the attackers to get into Target. And vulnerabilities like this are hard to fix. No one system might be at fault. There might be two secure systems that come together to create insecurity."

Principle 3: The Internet empowers attackers. Bruce said: "Attacks scale. The Internet is a massive tool for making things more efficient. That's also true for attacking. The Internet allows attacks to scale to a degree that's impossible otherwise. We're talking about millions of devices harnessed to attack Dyn; and that code, which somebody smart wrote, has been made public. Now anybody can use it. It's in a couple dozen botnets now." Actually, it's 52, as we reported last week. "Any of you can rent time on one dark web to attack somebody else." He says, "I don't recommend it, but it can be done. And this is more dangerous as our systems get more critical. The Dyn attack was benign. A couple of websites went down. The Internet of Things affects the world in a direct and physical manner: cars, appliances, thermostats, airplanes. There's real risk to life and property. There's real catastrophic risk."

And, finally, his fourth principle: The economics don't trickle down. He says: "Our computers are secure for a bunch of reasons. The engineers at Google, Apple, Microsoft spent a lot of time on this. But that doesn't happen for these cheaper devices. These devices are a lower price margin. They're offshore. There's no teams. And a lot of them cannot be patched. Those DVRs are going to be vulnerable until someone throws them away. And that takes a while. We get security for phones because I get a new one every 18 months. Your DVR lasts five years, your car 10, your refrigerator 25. I'm going to replace my thermostat approximately never."

Leo: But you remember, I told you the story about the guy who called the radio show who had a five-year-old Samsung refrigerator with Internet access that wasn't working anymore because the API in the Google Calendar had changed? You know, this is a problem. Refrigerators last 25 years. The Internet, you know, a year or two, everything's different.

Steve: Yeah. And he says, "So the market really can't fix this." And this is a point that I've been making recently, too. The point being consumers don't know and may not care. And clearly the Chinese manufacturers in Shanghai who are registering domains that

their firmware is querying, but not even bothering to acquire the domain names, they don't care, either. So again, the market can't fix it. So Bruce then laid out his argument for why the government - and this is Bruce, too. I mean, this is, I mean, he's no fan of government intervention. This is a little bit like Linus Torvalds or Richard Stallman saying they want more government involvement.

So he laid out his argument for why the government should be part of the solution, and the danger of prioritizing surveillance over security. And I'm really glad they heard this. Bruce said: "It was okay when it was fun and games. But already there's stuff on this device" - and I guess he was holding, oh, he actually was, I saw a picture, he's holding up his phone - "that monitors my medical condition, controls my thermostat, talks to my car. I just crossed four regulatory agencies, and it's not even 11:00 o'clock.

"This is something that we're going to need to do something new about. And like many new agencies in the 20th Century, many new agencies were created: trains, cars, airplanes, radio, nuclear power. My guess is that the Internet is going to be one of them. And that's because this is different. This is all coming. Whether we like that the technology is coming, it's coming faster than we think. I think," Bruce said, "government involvement is coming, and I'd like to get ahead of it. I'd like to start thinking about what this would look like.

"We're now at the point where we need to start making more ethical and political decisions about how these things work. When it didn't matter - when it was Facebook, when it was Twitter, when it was email - it was okay to let programmers" - and then he interrupts himself sort of - "to give them the special right to code the world as they saw fit." And remember, Bruce is, like, industrial-strength cryptographer. I mean, you know, he did Blowfish and Twofish and the Yarrow pseudorandom number generator. I mean, he knows what he's talking about.

He says: "We were able to do that. But now that it's the world of dangerous things, and it's cars and planes and medical devices and everything else, maybe we can't do that anymore." And that's not necessarily, we know, what Bruce Schneier wants, but he recognizes its necessity. And he finishes, saying: "I don't like this. I like the world where the Internet can do whatever it wants, whenever it wants, at all times. It's fun. This is a fun device" - he was waving his phone around - "but I'm not sure we can do that anymore."

Leo: I'm not sure I agree with him. I understand the problem, but I don't think what he's proposing as a solution is...

Steve: Well, he's proposing major intervention and regulation.

Leo: A government agency called the Internet Regulation Agency.

Steve: Yeah.

Leo: Yeah, yeah, that's all well and good if you've got a benign government that understands technology.

Steve: You know, we've often talked about, in sort of musing about the trouble that our computers have, how interesting it is that in the license agreements, that the producer of the software is held harmless. You don't own the software. It's licensed to you, and we reserve the right to revoke the license. And oh, by the way, if it ever does anything wrong, well, you have no recourse. And, oh, by the way, you agree to that. And if you don't agree to it, fine, go somewhere else. We'll take somebody else's money.

Leo: Yeah, but that's why I use open source software. I mean, you know, you don't have to have those shrink-wrapped licenses. That's a strong argument for open source. But, man, I know, it's kind of a mess.

Steve: I know.

Leo: I don't know what the solution is. I really don't.

Steve: No, we all, I mean, we're in trouble. That's what this means.

Leo: And by the way, he's talking to a lame duck session of Congress which, even if they wanted to do something, couldn't and probably doesn't want to. So the whole, I mean, the FCC decided to say, well, we're not going to do anything till January. We'll just let the next administration take care of this. You saw Admiral Clapper has resigned.

Steve: Oh, my god, yes. That was the best news I've had all week.

Leo: Or is it General Clapper? I can't remember. But he, yes, but, well, that's nice news. But who's going to replace him?

Steve: Yeah.

Leo: I mean, I don't know what the answer is.

Steve: I know.

Leo: I don't think going to the government and begging for help is going to really be a good idea at this point.

Steve: Well, and the problem is I can see Bruce's position. We're in an unregulated environment. And I don't, you know, programmers don't have certifications. I mean, look at Vincent, who wrote LessPass. With good intentions. There's a perfect example. And he's able to. I encourage him to learn. Unfortunately, a lot of people started using it. And but it was irresponsible for him to make it available when he didn't know how to do it correctly. But he had the right to. And I think it's great that he's learning how to do it

right. There's just a perfect example. And we have lots of people just, you know, who say, hey, I'm going to do this.

And, I mean, you could argue that the whole front of the podcast was talking about firmware from China that is doing not only unskillful, but malicious things, and hundreds of millions of people are buying the products. I mean, we're in a, I mean, I think Bruce is absolutely right. I guess my point is not all problems have acceptable solutions, but that doesn't mean they're not problems. We have a problem.

Leo: Or that we shouldn't seek a solution.

Steve: Right.

Leo: I mean, I agree. I don't think creating a federal Internet agency is at all the right solution. We could argue about other solutions. And obviously market-based solutions haven't worked, either. So, hmm, I don't know. What, you want to really license programmers?

Steve: No.

Leo: No.

Steve: I'll hang up my shingle. No. Oh, I guess I could pass the license exam, but still no. But I guess if that comes...

Leo: Well, maybe you could.

Steve: Then comes liability insurance.

Leo: Yeah, maybe you could. You know, it's harder to become a hairdresser, a barber in California than it is to become a midwife. And, I mean, I don't have high hopes for a solution. I really think we ought to find a consumer-based, market-based solution. But I don't know what the - I don't know how to do this. I really don't.

Steve: Yeah. And I think, you know, our listeners have seen in this podcast a huge lesson, which is paying more isn't a guarantee, but it's a big start because...

Leo: We have to stop being so cheap, and we have to start paying attention to these companies.

Steve: Right.

Leo: And all we've been doing as consumers acting as a whole is driving the market to cheaper solutions.

Steve: Right.

Leo: Right? We've taken all the profit out of the business. So why should they devote any time to making it secure? That's just expensive.

Steve: Yeah, exactly. I mean, these companies have been selling this stuff like hotcakes. And so, I mean, from their standpoint, it's working.

Leo: It's working.

Steve: Wow.

Leo: Well, I think we've done a lot, and I think we'll continue to make sure to do this, not just on this show, but on all the TWiT shows, to raise awareness of these issues.

Steve: Yes. Yeah. And again, we care about the people who listen to us. I mean, I can't effect this change. And I think that's probably one of the things that I hear from feedback is people appreciate knowing. What they do with that knowledge is up to them.

Leo: Yes, yes, right, exactly. And somebody's reminding us that the Philips Hue light bulbs weren't cheap, and the ZigBee protocol is supported by big, well-known companies.

Steve: Like I said, it's no guarantee. But I guess the point is that Philips has the resources to fix the problem.

Leo: Right.

Steve: And they have a reputation cost for the problem that would allow them to say, you know, send your bulbs back. We're going to bite the bullet and replace them with updated firmware.

Leo: Right.

Steve: Whereas these phones are never going to get fixed.

Leo: No.

Steve: So this has been in the offing for quite a while. And I know we have a lot of listeners in the U.K. Britain passed what is being called "the most extreme law ever passed in a democracy." The law requires U.K. Internet providers to store browsing histories, including domains visited, for one year against the actions of their customers in case of police investigations.

And Zack Whittaker gave this some good coverage in ZDNet. He said: "The UK has just passed a massive expansion in surveillance powers, which critics have called 'terrifying' and 'dangerous.' The new law, dubbed the 'snoopers' charter,' was introduced by then-Home Secretary Theresa May in 2012." And of course we've been following this. We've talked about this for a while. And it's like, it's always sort of felt like the U.K. was going to be ahead of us. And I don't like this because I don't want them to set a precedent that the U.S. follows. But it took two attempts to get it passed into law following breakdowns in the previous coalition government.

Now, fast-forward, or slow-forward four years and a general election later. Theresa is now Prime Minister. The bill was finalized and passed last Wednesday by both houses of Parliament. "Civil liberties groups have long criticized the bill, with some arguing that the law will let the U.K. government 'document everything we do online,'" they say. "The law will force Internet providers to record every Internet customer's top-level web history in real-time for up to a year, which can be accessed by numerous government departments; force companies to decrypt data on demand, though the government has never been that clear on exactly how it forces foreign firms to do that that; and even disclose any new security features in products before they launch." To, like, ask Big Brother if it's okay.

"Not only that, the law gives intelligence agencies the power to legally hack into computers and devices of citizens" - known in the parlance as equipment interference - "although some protected professions, such as journalists and medical staff, are layered with somewhat better protection. The bill was opposed by representatives of the United Nations, all major U.K. and many leading global privacy and rights groups" - all of whom have been watching this and saying no, no, no, no, no, please - "and a host of Silicon Valley tech companies. The law will be ratified by royal assent in the coming weeks."

So, boy. I mean, think of it, too, I mean, it is, you know, it's always easy to say that you want legislation to do something. At some point the rubber has to hit the road, and it has to actually happen. So, for example, an ISP cannot see what happens inside an encrypted tunnel. They could only be able to record that you connected to an external VPN service, and that's all they could say. Now, presumably all VPN endpoints in the U.K. would then also come under this legislation and have to monitor all of the unencrypted, then, communications of their customers. It's just - it's a mess. I mean, it's sad. And maybe we should consider this a test case, see how it goes. I mean, maybe it'll get pulled back, I hope, because, boy, this is the government that wants to be able to see everything its citizens do.

Leo: Yeah.

Steve: And, you know, a democracy. I mean, not a repressive regime.

Leo: It's just unbelievable, yeah.

Steve: Yeah. Yeah, I mean, every domain you visit for a year is, like, going to be recorded. Wow.

Okay. Now, this is odd. This is interesting because this develops a little differently than you would expect it would. This is from a very well put-together posting on BleepingComputer. We've often referred to them. They're our go-to place for the whole ransomware environment. They were on the early cryptomalware/ransomware early on. It's a neat site, very active high-end forums.

And this is kind of an odd ethical dilemma. Fabian Wosar, who's Emsisoft's security researcher, is a frequent poster and participant in the forums. He's facing a moral dilemma like very few security researchers have faced before. Wosar has been active for a few years helping ransomware victims. And in fact we've discussed his work before. Like a few months back, remember, there was some ransomware that didn't do it right, and it was possible - and some security researchers, in this case it was Wosar, who reverse-engineered their work, realized they'd done the crypto wrong, and then published some decryption software which, if any of their users or any of their victims knew of it, would be able to get their files back.

Well, he's received a private message from a user identifying himself as one of the people who coded the Apocalypse ransomware. During their exchange, the ransomware coder has asked Wosar to, get this, help their crew fix a bug in the ransomware's encryption process that causes files to be overwritten with junk data. That is, the ransomware is buggy, so it doesn't actually correctly write the encrypted data. It writes garbage, which of course kills the actual data so that it cannot be recovered.

"In order to secure Wosar's help, the ransomware coder has appealed to the researcher's dedication to helping ransomware victims. The crook says," as this posting writes, "that if Wosar helps, they'll be able to provide a ransomware variant that doesn't destroy users' files. The ransomware author was very candid with Wosar in his request. He said that even if Wosar helps or not, money is more important to them, and they'll continue to spread their ransomware as they have been doing for the past six months."

Leo: Oh, now, this is an ethical challenge.

Steve: Yes.

Leo: How interesting.

Steve: Isn't this weird? "The only ones that will have something to gain are the ransomware victims who, if they decide to pay, will then be able to regain access to their files."

Leo: Yes, let's fix our buggy software.

Steve: If Wosar helps.

Leo: Wow.

Steve: So the exact quote of the request reads, from the ransomware authors: "Once you have written that you feel" - so, and they're not English speakers, but I want to read exactly what they wrote. "Once you have written that you feel sorry for the ransomware victims. You can help them. As you know, we now use CryptoAPI." That's actually an API in Windows. And I remember we covered this some time ago. It was being - there are instances where it can fail. But if the software doesn't catch its failure and assumes that it provided a correct result and uses that, you don't encrypt correctly. And that's what's happening here.

So they say: "As you know, now we use CryptoAPI; and, if encryption function fails, we just fill file with garbage. As a result," they write, "after the decryption some victims crying to us. We try to keep an honest business; but money is more important to us, so some of the victims lose some of their files." Well, all of them. Well, all that matter. "How you can help them? I know you are the best in cryptography, so we can send you the encryption and decryption code, and you should point us where is a bug. We will fix it, and no more fake encryptions with garbage instead of the file content." So what do you do?

Leo: Wow.

Steve: Isn't that interesting? This is just such a...

Leo: Well, you don't help them. I mean, I don't...

Steve: No. Yes, I agree. I think the idea would be that their malware would get the reputation of being a scam where, if you pay them, you don't get your files back. On the other hand, it doesn't seem like it happens all the time. So it probably happens enough that people say, oh, yeah, I did pay those cretins, and I did get my files back, the Apocalypse ransomware. Ugh.

So, yeah, I mean, it's hard to justify helping them. On the other hand, their logic is intriguing. That is, it's just going to be a matter of testing the return arguments from one API and fixing it so that they detect a failure or prevent it from failing. I can't exactly remember the details around that API call. But it is a problematic function in the Windows crypto library. And then they would at least be able to return everyone's data. On the other hand, maybe it's better if they can't. I don't know. But, wow.

Leo: No. You don't help them no matter what. I mean, oh, geez. Has he said what he's going to do?

Steve: No. He's, like, pondering. He's, like, stuck.

Leo: Geez, Louise. Wow.

Steve: So a listener of ours, Matthias Bartosik, sent me an interesting screenshot from a tweet of his. He said: "Win10 insider preview changes default browser to Edge and tries to persuade me to stay when I want to switch back to Google Chrome."

Leo: Yeah.

Steve: And he sent a picture, and I guess you probably encountered this, Leo.

Leo: Oh, yeah, everybody has, yeah.

Steve: Yeah. And so, you know, before you switch, try Microsoft Edge. It's new, it's fast, and it's built for Windows 10.

Leo: I get that all the time because I use Chrome as my default browser, yeah.

Steve: Yeah, of course. So welcome to Windows 10.

Leo: By the way, Apple does the same thing. They say, you sure you don't want to use Safari?

Steve: But constantly? Or always?

Leo: No. And I don't think this one's constant. I think you say no, and it doesn't stay that way. But when you try, when you switch the default browser, it definitely encourages you to make the proper choice.

Steve: So this is kind of odd. And this is an unsatisfying answer; but we left the question open, and I wanted to close the question. So this was on November 17th. And I don't know if they were referring to us. But the guys who named it BlackNurse said: "There seems to be some confusion/amusement/discussion going on regarding why this attack is called the 'BlackNurse.'" And again, remember that's the ICMP Class 3 Code 3 or Type 3 Code 3 that allows a single host with about 15 to 18 megabits of bandwidth, so not a lot of bandwidth, and just one, to hold many major sites. And there's a growing list of, like, major routers and firewalls, lots by Cisco, that are vulnerable to this. So it's significant. And so they said: "Also, googling 'black nurse' might not be 100% safe-for-work."

Leo: Oh, god. Which is another reason not to use that name.

Steve: Yes, exactly, a term, "...since you risk getting search results with inappropriate

videos that have nothing to do with this attack. The term 'BlackNurse,' which has been used within the TDC Security Operations Center for some time to denote the 'ICMP 3,3' attack, is actually referring to the two guys at the SOC who noticed how surprisingly effective this attack was. One of these guys" - this is why it's a little strange. "One of these guys is a former blacksmith, and the other..."

Leo: They're yanking your chain.

Steve: "...a nurse."

Leo: No one's a former blacksmith.

Steve: No, no.

Leo: Once a blacksmith, always a blacksmith.

Steve: Well, okay.

Leo: I used to shoe horses, but now I'm a code junky/jockey. Former blacksmith.

Steve: Anyway, so they explain, "the other is a nurse."

Leo: Yeah.

Steve: "Which was why a colleague of theirs jokingly came up with the name 'BlackNurse.'"

Leo: How about NurseSmith? That would have been a better name.

Steve: "However, it was first intended as a joke. The team decided to call the attack 'BlackNurse' even when going public with it."

Leo: Yeah, yeah.

Steve: It's like, eh. I agree, Leo, that seems a little farfetched. You know, a blacksmith then became a high-end security guy, and a nurse is hacking in his spare time? I don't know.

Leo: They're yanking your chain. This is the Danish sense of humor.

Steve: So I did promise everybody that the SQRL presentation slides would be online, and they are. I didn't have time, literally, as you know, Leo, I was running behind as it was, there was so much to talk about this week. But there is a link. For anyone who's interested, GRC.com/sqrl/presentation.pdf. And of course I will create a link to it, and it'll be part of the SQRL spec and so forth. But I did incorporate all the feedback from the guys that are working with me in the SQRL newsgroup. So GRC.com/sqrl/presentation.pdf. And it's about 40 slides.

And I should explain, too, it's not meant as a, I mean, I wrote this for - I created it for the presentation week before last to Yubico. So it's at a higher end. There will be other materials for users. This is more meant sort of for our audience, the people in our audience who've been following along. This is SQRL, if you'll pardon the term, in a nutshell, that is also a full-feature walkthrough.

So if you just page through this and look at it, you'll get a lot of information that's sort of put together in a nice mixture. It's way below the level of a spec, but it's above the level of the user, stuff the user never needs to know about. One of the beauties of it is that it just works. This explains a lot of how the plumbing is, you know, which the Yubico guys wanted to see. So I'm glad we have now a full-feature walkthrough of this.

I also wanted to mention, because I'm about to go out on the fringe, but before that, my discussion of this new theory of gravitation, and maybe that it eliminates a need for dark matter. I mean, I'm not an astrophysicist. I never claimed to be. I haven't even played one on television. A number of our listeners were upset that one of their pet assertions about dark matter, that is, the observation of the gravitational lensing of the bullet cluster - which, oh, of course, we all know about that - still exists, even if there's a different theory of gravitation.

And again, I'm not making any assertions about this. I was just reporting on what I thought was an interesting idea. And it would be nice if such a, like, without this theory, using even that modified theory of gravitation, that reduces the error from a factor of 10 to a factor of two. So it improves it by five, but doesn't get you there. And it's got problems with the gravitational lensing in the bullet cluster, too.

So anyway, I hope people didn't misunderstand. I wasn't making any assertions about what I believe or know. I was just saying, hey, here's an interesting theory, and wouldn't it be nice if we didn't need dark matter. And, by the way, this whole gravitational lensing thing is way less certain that some people seem to have believed. So I got some talkback on that, and I just wanted to share it. Now, this is cool, Leo. NASA...

Leo: Oh, I know where you're going with this one. The propellant-less engine.

Steve: Yes. The reactionless space drive.

Leo: I still think this is utter nonsense, but go ahead.

Steve: It may be. However, it's interesting. You know, we know that things break down, that is, some of our concepts and theories break down at different scales. And, well, for example, Newton's theory of gravitation has no problems with apples dropping and satellites orbiting the Earth. And we understand it, and we're able to make use of it. But the problem is sometimes on different scales these things don't apply as well as they

appear to.

So a little bit of background. Back in 1999 an inventor described a reactionless propulsion system which met with a lot of skepticism. But some people began testing it. And they were reporting that it seemed to be generating some thrust. Now, once again, by "reactionless," you know, the normal way we thrust is that something is shot out of the end, and what is it, Newton's - one of the laws. The fourth law? For every action there's equal and opposite reaction.

Anyway, so I'll just share from some of the coverage: "After months of speculation and leaked documents, NASA's long-awaited EM Drive paper has finally been peer-reviewed and published. And it shows that the 'impossible' propulsion system really does appear to work. The NASA Eagleworks Laboratory team has put forward a hypothesis for how the EM Drive could produce thrust - something that seems impossible, according to our current understanding of the laws of physics.

"In case you've missed the hype, the EM Drive, or Electromagnetic Drive, is a propulsion system first proposed by British inventor Roger Shawyer back in 1999. Instead of using heavy, inefficient rocket fuel, it bounces microwaves back and forth inside a cone-shaped metal cavity to generate thrust." Inside a closed cavity to generate thrust. "According to Shawyer's calculations, the EM Drive could be so efficient that it could power us to Mars in 70 days.

"But there's a big problem with the system. It defies" - oh, it's the third law - "Newton's third law, which states that everything must have an equal and opposite reaction. According to the law, for a system to produce thrust, it has to push something out the other way. The EM Drive doesn't do this. Yet in test after test it continues to work. Last year, NASA's Eagleworks Laboratory team got their hands on an EM Drive" - oh, and it's a cool-looking thing. I don't have a picture in the show notes, but they're all over the place - "to try to figure out once and for all what was going on. And now we finally have those results.

"The peer-reviewed paper is titled 'Measurement of Impulsive Thrust from a Closed Radio-Frequency Cavity in Vacuum' and has been published online as an open-access 'article in advance' in the American Institute of Aeronautics and Astronautics, the AIAA's Journal of Propulsion and Power. It'll appear in the December print edition."

So skipping way down to the end of what was published - I've read it - the conclusions say: "A vacuum test campaign that used an updated integrated test article and optimized torsion pendulum layout was completed. The test campaign consisted of a forward thrust element that included performing testing at ambient pressure to establish and confirm good tuning, as well as subsequent power scans at 40, 60, and 80 watts, with three thrust runs performed at each power setting for a total of nine runs at vacuum. The test campaign consisted of a reverse thrust element that mirrored the forward thrust element. The test campaign included a null thrust test effort of three tests performed at vacuum at 80 watts to try and identify any mundane sources of impulsive thrust. None were identified.

"Thrust data from forward, reverse, and null suggested that the system was consistently performing at 1.20.1 millinewtons per kilowatt [mN/kW], which was very close to the average impulsive performance measured in air." I should stop and mention that previous tests done around the world had been done in air, and there was some concern or questioning whether it might have been - the microwaves might have generated heat, and so the heat acting on the air was what was producing some convection currents or something to produce some false readings of thrust.

"A number of error sources were considered and discussed. Although thermal shift was addressed to a degree with this test campaign, future testing efforts should seek to develop testing approaches that are immune to CG [center of gravity] shifts from thermal expansion. As indicated" - and then they cite a section of their report - "a modified Cavendish balance approach could be employed to definitively rule out thermal. Although this test campaign was not focused on optimizing performance and was more an exercise in existence proof, it is still useful to put the observed thrust-to-power figure of 1.2 mN/kW in context. The current state-of-the-art thrust to power for a Hall thruster" - a Hall thruster is the current best concept. It's an ion-based plasma. So you typically ionize Xenon gas, and it accelerates it out of the back of the vehicle in order to, again, that's standard Newton's Third Law. You're shooting stuff out one end, and you're generating propulsion in the other.

Anyway, so the Hall thruster "is on the order of 60 mN/kW." So as opposed to 1.2. "This is an order of magnitude higher than the test article evaluated during the course of this vacuum campaign; however, for missions with very large delta-v requirements" - meaning we need a lot of speed over time - "having a propellant consumption rate of zero" - because that's what this is. Remember, you're using up Xenon gas as you're ionizing it and blasting it out the end. So you're consuming mass in order to thrust it out the back. This system consumes no mass.

So they say: "Having a propellant consumption rate of zero could offset the higher power requirements. The 1.2 mN/kW performance parameter is over two orders of magnitude higher than other forms of 'zero-propellant' propulsion, such as light sails, laser propulsion, and photon rockets having thrust-to-power levels [on the order of] 3.33-6.67 micronewtons per kilowatt [N/kW]." So who knows? I'm not saying it's real. I'm just saying it's very cool.

And also, again, this is where, I mean, you know, this might be cold fusion. Remember back in the '80s everyone got excited because it looked like there was a way to perform fusion, not fission, but fusion in a test tube at room temperature. And some explosions were performed, and some people claimed to be getting more energy out of it than not. But here we are, decades later, and nothing ever happened. So maybe it's specious. But I think more people are going to be looking at it now, and that's a good thing.

Leo: I feel like it's - you're going to have to have something better than that to overturn Newton's Third Law of Thermodynamics. I don't know. 1.2 millinewtons.

Steve: Millinewtons per kilowatt.

Leo: Millinewtons with a plus or minus - with an error of one, plus or minus. So close to the air.

Steve: Yeah, 1.2 plus or minus...

Leo: One.

Steve: Point one.

Leo: Oh, point one.

Steve: Yeah.

Leo: All right.

Steve: Point one. Yeah.

Leo: Okay.

Steve: So it's between 1.0 and 1.3. I'm sorry, 1.1 and 1.3.

Leo: Do they have a thesis as to what's going on?

Steve: Oh, yeah, yeah. I didn't go into it. But they have a concept for - and again, this gets into the quantum physics about - and they discuss this in their paper, a theory for how this can work, how it can be that it's generating a small, non-net zero thrust in one direction.

Leo: Yeah. Which would be very valuable, obviously.

Steve: Oh, yeah. I want one.

Leo: Sounds like a perpetual motion machine.

Steve: We'll see.

Leo: We'll see.

Steve: I just thought it was cool because, I mean, reactionless drives, the aliens all have them. So, you know, we need that, too.

Leo: Somebody's got to invent one.

Steve: Yeah.

Leo: All right. I don't know, maybe I - I don't know anything about it. Why should I

be skeptical?

Steve: I'm just hopeful.

Leo: Yeah.

Steve: It's fun.

Leo: And I'm just a cynic, so there you go. My friend, we have come to the end of this fine motion picture.

Steve: And not a moment too soon. As I said, there was just too much to talk about. And I think this was a lot of good stuff to talk about, and I'm glad we did.

Leo: It's very good stuff, as always. We do this show every Tuesday, about 1:30 Pacific, 4:40 Eastern, if you want to tune in and watch live in the chatroom at irc.twit.tv. That would be 19:30 UTC, so you can do the offset from your locale. We encourage you to listen offline, as well. And Steve's got audio of every show plus a transcript that makes it a lot easier to understand what he's saying. And that's at GRC.com. While you're there, don't forget to get SpinRite, the world's best hard drive maintenance and recovery utility, plus all the other fabu things that Steve does, just for us, for free, Perfect Paper Passwords and SQRL and all of that. And the SQRL presentation is there.

If you can't make it to there, you can always go to TWiT.tv/sn. We've got audio and video. I don't know why you'd want video, but you can get it. And we have lots of other shows, too, at TWiT.tv. And you could always subscribe using your favorite device, your mobile or your desktop, and get every episode. We're everywhere. You can watch on your TV on a Roku or an Apple TV. Just make sure you don't miss an episode because, who knows, you know, next week we may be announcing that you can use water for gasoline. It could happen. Could happen. I'm just teasing. Steve, always a pleasure. Thank you, sir.

Steve: Thanks for making it possible, my friend. We'll be back next week. I'll spend a little time on the Skype stuff, although we did much better this week than we did last week, so that's good.

Leo: No problems at all. Maybe all this time it's been like this, and we just didn't notice. I don't know.

Steve: I don't know.

Leo: Right. Thanks, Steve. We'll see you...

Steve: Thanks, buddy.

Leo: ...next time on Security Now!. Bye-bye.