SECURITY NOW!

Transcript of Episode #660

Azure Sphere

Description: This week we discuss Drupalgeddon2 continuing to unfold right on plan. The Orangeworm takes aim at medical equipment and companies. The FDA moves forward on requiring device updates. Microsoft leads a new Cybersecurity Tech Accord. We talk about another instance of loud noises and hard drives not mixing, considerations for naming your WiFi network, the unappreciated needs of consumer routers, Google's new unencrypted messaging app push, Amazon pulling the trigger on "in-car" package delivery, the first puzzle recommendation in a long time, and Microsoft's move to secure the IoT space.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-660.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-660-lq.mp3

SHOW TEASE: It's time for Security Now! with Steve Gibson. Drupalgeddon hits the big screen. Your medical equipment needs deworming. A group of major vendors have had their own Council of Elrond to destroy the One Ring, the "ring" being security exploits. Amazon brings back the trunk money. And might Steve have something nice to say about Microsoft? Find out next on Security Now!.

FR. ROBERT BALLECER: This is Security Now! with Steve Gibson, Episode #660, recorded April 24th, 2018: Azure Sphere.

It's time for Security Now!. This is the show with Steve Gibson. He's our very own master of security, the guru of trusting no one. He's like our Rodney McKay, but without the starting gate and without destroying five eighths of a solar system. I'm Fr. Robert Ballecer, in for Leo Laporte, who's currently touring Japan, looking for plutons, I think. Pluton magma rock, Steve? Is that the thing we're doing?

Steve Gibson: Well, it's great to be with you today and next week, Padre. Yes, this is Episode 660, and our topic is Azure Sphere. Which I know that Leo and Paul and Mary Jo had a lot of fun with last week because they were like, wait a minute, Microsoft is doing Linux? What? Really? And so we will get to that after we deal with the rest of the week's news. But it is an interesting project which I have to say I'm kind of bullish about. I think that Microsoft has done something good. This came out of the Microsoft Research Group. It is 100% focused on something that we on this podcast have been wishing for, hoping for, not knowing how we could get from here to there for. And that is security for IoT devices.

FR. ROBERT: Yes.

Steve: And the best news is it's all license-free. Microsoft is essentially donating a bunch of really solid work, all the intellectual property, all the licensing, everything, just for the benefit of what this architecture would mean for IoT. So we'll talk about all of that at the end of the podcast.

But we need to talk about the ongoing drama surrounding Drupalgeddon2, which is continuing to unfold right on schedule as we had expected. Symantec had a report about an interesting multiyear campaign that they called "Orangeworm," which didn't really push me a lot except that it got so much press coverage, and so many people tweeted to me about it, I thought, well, okay, we need to talk about it a little bit. The FDA is indicating they're going to move forward on requiring device updates. Microsoft at last week's RSA conference finally closed the deal on something they had initiated at the previous year's RSA conference, which is the so-called Cybersecurity Tech Accord. And I thought it would be fun to look at who's in and who's not, sort of an interesting who's who on both sides.

Also we've run across another instance of loud noises not being good for hard drives that is just kind of a kick. Also along the same lines, some considerations for naming your WiFi network. Also the unappreciated needs of consumer routers. Actually, we've all been talking about this for a long time. But a study showed just how unappreciated those needs are and came out with a little bit of concern there. We also have, oddly enough, a brand new messaging app from Google which lacks only one arguably very important characteristic, which we'll talk about. And of course Google keeps trying to do messaging for Android and just seems unable to somehow get here from - or, wait, there from here, wherever they are. Also Amazon pulled the trigger today on something that we talked about maybe six months ago or more, which is in-car package delivery.

Also I have the first puzzle recommendation in a long time. All of our listeners know that I love puzzles. But I am extremely picky about the puzzles that I love, and consequently I'm constantly getting recommendations from our listeners. I kind of look at it and think, eh, that didn't quite hook me. I have one, finally, first puzzle in many, many, many months that just has all the right things. And then we'll do a little bit of miscellany and talk about the Azure Sphere, as Microsoft has called it. So I think a really interesting, fun couple of hours for our listeners. And for you and me.

FR. ROBERT: Now, Steve, of course there are weeks where we'll do this show, and there's some news, but not a lot of news. This is a lot of news, and it's a lot of varied news. I have no idea if we're actually going to make it all the way through that because a lot of that is juicy. Way, way juicy.

Steve: Well, we'll just do the best we can.

FR. ROBERT: Indeed, indeed. All right, Steve, guide us through it. Drupalgeddon. I love the name.

Steve: Yeah, well, okay. We've been talking about it for the last several weeks. The gang at Drupal discovered a very, I mean, like the worst possible problem in the Drupal CMS - Content Management System for websites - imaginable, where anyone who is able to access the site remotely is able to run code on that server with no authentication. I mean, just a remote code exploit that is trivial to do.

So they gave the whole world, the industry, one week's notice of the fact that this was going to happen. So this was three Wednesdays ago. Three weeks ago tomorrow they gave a one-week notice that on the following Wednesday they would be releasing an absolutely over-the-top, critical, drop everything in the middle of the day. They told us at I think it was noon Pacific time that there's going to be a patch. And it's so bad that they even did a fix for the no longer maintained v6 series of Drupal because 7 and 8 are where most of the world is. But if anyone was still on 6, they needed to fix that, too.

So one week after the announcement, on schedule, they released the patch. So that was two weeks ago tomorrow, 13 days ago. One day after that, the first proof-of-concept exploit code appeared on GitHub, which was, again, predictable, expected. It's like, okay. If they're patching something, it's easy to look at the old code and the new code and go, oh, look what they changed, and then back that out and figure out what it was that they were trying to prevent.

So last week we were one week downstream; and, yes, right on schedule there were problems. First of all, security companies shortly after the release, like within hours, began reporting massive scans of the Internet for vulnerable Drupal candidate servers. And Drupal is, I think, number two in the CMS world. I think that WordPress is number one, and Drupal's number two. I knew a couple weeks ago when we talked about it. I think that's what the numbers are.

FR. ROBERT: Yeah.

Steve: And in fact TWiT is all Drupal based, also. So I made sure that Leo and Leo's team were all up to speed. And when he checked, it's like, oh, yeah, yeah, we know, we know. Because of course the Drupal guys sent out email and blog posts, I mean, they really wanted to not have the community hurt by this, although what we also know is that there will be, as is always the case, a dispiriting percentage of sites that don't update, that never update. They're just going to be victims of this.

And so this is called Drupalgeddon2 because in 2014 there was a very bad SQL problem that was similarly exploitable, and that was Drupalgeddon with a one implied because it was the first one. So here we are now, almost two weeks downstream of the release of the patch. We have lots of malicious activity. Coin miners are being installed. PHP backdoors are being installed. Perlbots are being installed. There are several instances of a very large botnet called Tsunami which has added Drupalgeddon2 awareness so that it's able to jump to and exploit those servers in addition to everything else it was already doing.

I got a kick out of, and I don't mean to be critical of Ars Technica at all, they do great reporting and provide a lot of great coverage. And oftentimes the person who writes the article doesn't do the headlines, I know from my own having written a column for eight years in InfoWorld. Sometimes I would write something very carefully, and the headline would mischaracterize what I had said because it was more catchy, which used to annoy me. Anyway, the subhead on Ars coverage said "Bug patched in March is still being exploited to take full control of servers." And I thought, still?

FR. ROBERT: Wait, wait, yeah.

Steve: It's never not going to be exploited. I mean, unfortunately, we still have Code Red and Nimda worms that are out there roaming around. I coined the term many, many years ago, IBR, Internet Background Radiation. That's what all this is. It's just background radiation on the Internet, just agents out there that are just looking around for old things, systems that have never been rebooted, that have installed themselves and so forth. And as if this wasn't bad enough, one week after the patch, another different problem was found. And it's funny that this got very little coverage. I ran across it, and then I was looking for it again, and I had to go to the Drupal.org site and check the security announcements because I found very little coverage in the press.

I'm not sure how this got by because it's also a critical error. There's a JavaScript library in the Drupal core called CKEditor, which is a rich text editor that is very popular. It's built into Drupal. It's often used. There's some question about whether the default instance of it is vulnerable. But anyway, it has a cross-site scripting vulnerability which Drupal called "moderately critical," although it also allows you to run HTML and JavaScript code in the victim's browser to gain access to sensitive information.

FR. ROBERT: Yeah, and I didn't get that because, I mean, anything that allows for cross-site scripting, that's not moderately critical, that's critical. That's about as bad as it can get because I can now run arbitrary code. So I don't understand that classification.

Steve: Right. The only thing I could think was that it was just fatigue from Drupalgeddon2.

FR. ROBERT: Compared to what just happened, this is moderate.

Steve: Exactly. It's like, oh, yeah, we really, really don't want to do this again, do we? So let's just, like, fix this please. So I did want to let our listeners know that you may need to be updating yourself again, even if you just did, if you're a Drupal site. And CKEditor, if that's part of what you're using, there's a plugin with an image tag, enhanced image plugin in that particular version. It does not affect Drupal 7, only the Drupal 8 line.

So anyway, I just sort of wanted to check in on Drupalgeddon2. As I said, everything unfortunately is proceeding according to plan. This having come out, unfortunately, the nature of it, of Drupal, is that it was very simple for this to be reverse-engineered. It's not like Microsoft burying some changes inside of binary DLLs that are all mixed around and recompiled into a blob where you'd have to really do reverse-engineering. Drupal just isn't delivered that way. So it was easy for bad guys to find this. And unfortunately it's exploitable by anyone who accesses the server. And as we've been talking about, due to this crazy popularity of coin miners, malicious cryptocurrency mining is now the big get for servers because they tend to have good connectivity and lots of CPU power behind them. So, yeah, unfortunately it's on track.

FR. ROBERT: Now, Steve, it's interesting because Drupal actually seemed to have handled this quite well. They gave people advance warning.

Steve: Yes.

FR. ROBERT: Because they understood - this didn't always used to be true. But they understood that the minute they released the patches, that every black and white hat would be going through the code, as you mentioned, to find what had changed. And then they would be able to backwards engineer a proof-of-concept exploit within hours, if not minutes.

Steve: Yeah, unfortunately this is the world we're in now, I mean, it's almost a malware ecosystem of bad guys really interested in taking advantage of any vulnerabilities. And it's weird, too, when you step back a little bit, we now just sort of take this for granted. I mean, it's like, okay, this is what's going to happen. I mean, we knew it beforehand. And even in covering it it's like, okay, yeah. Unfortunately, this is going according to plan.

And I think part of the reason is that now with cryptocurrency creating a new pressure to get mining software onto hardware, there's a new reason to do this. I mean, for years we've had viruses, and I used to comment often on this podcast to Leo that isn't it interesting that the virus just seems to want to propagate and not do anything really dastardly. And it's a good thing, but it was sort of like a hobby, hobbyists or hackers who just wanted to see what would happen. Like the original Morris worm, for example. No malicious intent, it's just like, ooh, this would be cool. Can I write something that can propagate itself? Wham. Yes. Unfortunately...

FR. ROBERT: I was going to say that malware grows up. I mean, when malware was started, as you mentioned, it was mostly an oddity. It was a curiosity to see if it would actually work. From there you moved into, okay, well, maybe you infect a couple of systems. You've got an advanced persistent threat inside of a network. Maybe that might pay off financially down the line. Then it moved to, well, we can create botnets, and we can do crazy things and horrible things with botnets, and we can shake people down that way. I think, yeah, this cryptocurrency mining malware is a new generation because it's no longer waiting for a payoff. It's the minute I start infecting machines, I get paid.

Steve: Yes. And we could argue that there was sort of another stage which we went through the last couple years which was the encryption of people's data in order to try to then extort money from them. But there was something wrong with that model. Many people couldn't afford to pay. Many people had backups. Many people just sort of shrug and go, oh, I'll just get another computer. Like there was just not anything there of tremendous value. So that was a problem, but that's largely been supplanted now, exactly as you say, by this notion that, oh, I can actually create something that is going to start dribbling cash into my purse.

FR. ROBERT: Right. Well, I mean, all those previous generations you did something that would affect the performance of the machines that you were infecting, and therefore it caused an annoyance that had people pushing back. The cryptocurrency malware, not necessarily so.

Steve: Yes, especially if it's designed not to take up too much resource.

FR. ROBERT: Precisely.

Steve: It can sit there purring away in the background.

FR. ROBERT: Yeah. And this just adds to that background noise radiation, the background radiation that you talked about, which I would see every time we brought up the big network for Interop. There would always be a steady stream of attacks from really, really old malware, but they were on devices that have been long forgotten. We've gone from having datacenters full of servers and devices that we've forgotten about to now having an entire world filled with IoT devices and virtualized machines that have been forgotten about. As you mentioned, we know for a fact there's a huge component of Drupal machines that will never be patched.

Steve: Never.

FR. ROBERT: Because they've been abandoned.

Steve: Yup.

FR. ROBERT: Okay, well, luckily whenever I do this show you always bring me good news. It uplifts me, Steve.

Steve: Okay, well, we will look for some of that.

FR. ROBERT: Oh, you know what I just - someone pointed out that I actually made you skip the Pic of the Day.

Steve: Well, we did, but I have the picture again in the show notes later where we'll be talking about it. So I thought, okay, well, yeah.

FR. ROBERT: Yeah, we'll do that.

Steve: So Symantec released a report where, as they do, they've got threat intelligence groups that are looking around, tracking what's going on. In early 2015, in January, they began seeing evidence of some group which was mostly and quietly targeting medical organizations. And the press coverage that I mentioned sort of took an interesting spin. All of the headlines talked about high-tech imaging devices like X-rays and MRI machines being infected. And so that's like, oh, my god.

But it turns out, again, that's not really what was going on. In reading into this more carefully, Symantec has dubbed this thing "Orangeworm," stating that an unknown hacking group had been found installing a wormable trojan on machines hosting software used for controlling X-rays and MRI machines, as well as machines used to assist patients in completing consent forms. And in some of the little more carefully assembled coverage, the presumption was that maybe this group was targeting medical organizations because you got much richer personal information content from collecting medical records and reselling them than you did somebody's shopping records, if you managed to compromise some retailer.

So what Symantec has seen is that the preponderance of attacks is in the U.S. I think it's 17% in the U.S. Then they had a 10% pie slice of where they were unable to determine where the attacks were. Then I think 7% was, or maybe it was 10% was in Israel. And then it just sort of ran around through the pie, with each slice getting successively smaller. But global. So this appears to be a focus on global attacks. I would imagine perhaps that there's a preponderance in the U.S., just because of the systems in place and probably, unfortunately, lack of security that lets them get in. It's not just medical organizations. It's also suppliers to them. So it might be that, for example, if a medical organization has an IT relationship with some of their higher end suppliers, that that's a way into the medical organization.

And we've seen this famously in several places. I think it was the Target credit card breach that was famous a few years ago. It was actually a contractor of Target's, an HVAC manufacturer that had the vulnerability. And so the bad guys were able to get into Target through their HVAC supplier as a consequence. So that sort of thing. So there's a trojan called the Kwampirs, K-W-A-M-P-I-R-S, which is largely in the healthcare sector in the U.S. and Europe and Asia, now in its third year.

So this is one of the so-called, I don't know if it would be an APT, but it's an advanced persistent intent, so an API, I guess. And they're calling it a "supply chain attack" because it is also sort of upstream of the victims. But definitely seems focused on medical suppliers, pharmaceuticals, the healthcare industry. And they don't think it's a nation-state actor. They say that it has the fingerprints of somebody who probably wants maybe rich patient data from healthcare providers. So that may just be something that they're in the resale business of that kind of detailed personal information for who knows what purpose. So, interesting.

FR. ROBERT: Right. Now, what I found fascinating about the story is they're not going after the MRI machines themselves. I mean, that's what gets the headlines. That makes it sound spectacular.

Steve: Right, exactly, exactly.

FR. ROBERT: Because an MRI machine is still sort of a fanciful device in hospitals that miraculously gives you a diagnosis. But instead, they're going for the control systems. They're not going after the embedded systems, but they're going for the control systems. And I think it's because, if you look at most hospital networks, since I've worked with a couple of our hospitals, you can pretty much guess what they're going to be connected to because MRI machines are very specific types of devices. They will always be connected to one or two networks that you'd really want access to.

So I see this as an attempt to pivot. They want to be in on a machine that they know is going to be connected to networks that they want. And then they can just turn that and say, okay, now I'm going to attack the patient network database. Or I'm going to go after their billing database. That's, I mean, that just shows a level of forethought that I guess it's now common for malware, but didn't used to be.

Steve: Yeah. And I think it also suggests, again, a focused intent. They're not out there spraying, looking for arbitrary ways in. They're saying we're going to go after this particular profile of company and, as you said, identifying some typical ways in. And probably, once they've succeeded a few times, they start thinking, hey, going after the large control system for these large machines seems to be a successful strategy. And so they're just sort of refining a strategy over the course of three years because we're now - it was all of 2015, all of 2016 and 2017, and now we're in 2018. So it was first seen in January of 2015. So some long-term focus for whatever reason.

FR. ROBERT: And you thought that hackers were just nerds in the basement.

Steve: Now, you were looking for some good news.

FR. ROBERT: Yes.

Steve: We do have some good news. There have been, again, very much the headline grabbing are things like insulin pump can be taken over remotely, and your pacemaker can be reprogrammed, and this whole concern over hacking medical devices is headline grabbing.

The good news is that the FDA is getting ready, they're gearing up to take some action on medical devices, including eventually - bureaucracies don't do anything quickly. But they understand, someone understands there, based on the most recent medical device safety action plan - I have a PDF in our show notes if anyone is interested - they recognize that cybersecurity is no longer optional and is exactly the kind of thing that FDA regulation can require and enforce as part of the oversight and verification of the safety of devices. So the idea being that device safety, the definition is being extended to require after-market, after-sale, long-term security maintenance, not just battery maintenance and making sure the leads don't get corroded. But there needs to be an ongoing management of device safety. And I think that's just all for the best.

In this document, after you get way down into it, point number four - I've skipped all the other ones. Under "Advance Medical Device Cybersecurity" it reads: "The FDA plans to consider potential new premarket authorities to require firms on the front end, to, one, build in capability to update and patch device security into a product's design and to provide appropriate data regarding this capability to the FDA as part of the device's premarket submission; and, two, to develop" - what they're calling, and I don't know what this means - "a 'Software Bill of Materials' that must be provided to the FDA as part of a premarket submission and made available to medical device customers and users so that they can better manage their networked assets and be aware of which devices in their inventory or use may be subject to vulnerabilities. In addition, availability of a [again] 'Software Bill of Materials' will enable streamlining of timely post-market mitigations."

So that sounds like they're saying the FDA is going to require that these things no longer be allowed to remain black boxes, where there's no visibility into them. In the future, you're going to have to disclose what the moving parts are in there, in this so-called "Software Bill of Materials," so that if a vulnerability is discovered, it's possible to check that against your bill of materials and say, oh, you're using this version of SSL or this build or distro of Linux in your embedded thing, and the world just found a problem with that.

FR. ROBERT: Right.

Steve: So essentially creating accountability where there's been absolutely none, and where it's been feasible for this sort of black box concept to reign. And of course we know one other place where it would be fabulous to see the same sort of management, and that is voting machines because the model is very much the same as it is for medical devices. It's a black box where Diebold is just allowed to say, oh, yeah, we have the best security.

FR. ROBERT: And that bill of materials is actually a big part of this because it means, if you find something wrong with a component, it's not just that you know, okay, it's that component. It means you can now search your database and say, what other products are using that component? That's huge. That has not existed before. They used to have to go device by device by device. Now it's, oh, we found this software component and this hardware component combine to make a vulnerability. Any devices use those same two components? And you can do a quick search.

The other part about this, Steve, is the FDA actually got a lot of pushback. I don't think some people understand how big this actually is of a change. Manufacturers came back to the FDA, when the FDA was first starting to look at this.

Steve: Oh, you can imagine, yes.

FR. ROBERT: They were pushing hard, and they were basically saying, look, the FDA, you only care about the medical efficacy of a treatment, a device, a medication. You shouldn't be telling us how to build the devices and how to provide security.

Steve: So the argument was that the FDA was overstepping their boundaries.

FR. ROBERT: Right, exactly. This is not your area of regulation. And the FDA, they must have consulted some tech-savvy people, came back and said, wait a minute.

Steve: If not us, then who?

FR. ROBERT: If the tech is broken, that affects the medical efficacy. That's exactly your charter.

Steve: Yup.

FR. ROBERT: But I think you're right. I think federal agencies need to start doing this, this whole "security forward" view, where security is part of the first discussion, not something that you tack onto the end, which we both know that that's sort of been the M.O., not just for medical or voting machines, but from pretty much everything. Security is, after you get the thing working, then you can secure it.

Steve: Well, IoT. It's like, oh, yes, everything's connected to everything. And it's like, wait a minute, you know...

FR. ROBERT: Oh, yeah, we'll throw a password on it somewhere. Don't worry about it. It's okay. It's okay.

Steve: Yeah, yeah, [crosstalk].

FR. ROBERT: So that is good news. So when I do eventually have to have a pacemaker installed because I'm still eating way too much high-fat foods, at least I know that, A, it won't be as easy to hack me; and, B, I will have the right to actually look at the data coming off my pacemaker.

Steve: Yes. And you alone will know how to do that.

FR. ROBERT: No, I'm going to put it on the Internet. It'll be on my Twitter feed.

Steve: Okay. So at last year's RSA conference, Microsoft's Chief Legal Officer, Brad Smith, started talking about what he called the Cybersecurity Tech Accord. And apparently he's been doing - he/they, Microsoft seems to be the leader here - has been doing a year's worth of behind-the-scenes meetings and conversations and committees and the stuff that big companies do that just puts me to sleep. But it was successful such that, at last week's RSA conference, a little over a year later - the previous one was in February as opposed to early April - the Cyber Tech Accord was announced. It's got a domain, CyberTechAccord.org. And essentially this is a voluntary membership of companies who want to say they're going to team up and agree to profile their behavior in a certain way. So there's, like, four primary tenets to this accord.

Strong defense: Tech companies should do their best to protect users from any type of cyberattack, regardless of source or the user's native country. No offensive development: Tech companies should never provide material support to government-backed cyberattacks. Third is capacity building: Companies should build and provide customers with the necessary tools to protect their data and themselves from state-sponsored attacks. And, finally, collective action: Companies will collaborate with each other to share data on attacks and disclose attacks to affected users.

So this isn't a big deal. I mean, it's sort of nice to see. It feels very bureaucratic to me. But certainly it demonstrates, for companies that are wanting to be part of the accord, that they've got their heart in the right place, I guess, if nothing else. In the announcement a couple people who are members were quoted. Kevin Simzer, who's the COO of Trend Micro, who of course we all know, said: "The real world consequences of cyber threats have been repeatedly proven. As an industry we must band together to fight cybercriminals and stop future attacks from causing even more damage."

And then Carolyn Herzog, who is the general counsel for ARM, said: "The Tech Accord will help to protect the integrity of the one trillion connected devices we expect to see deployed within the next 20 years. It aligns the resources, expertise, and thinking of some of the world's most important technology companies to help to build a trusted foundation for technology users who will benefit immensely from a more secure connected world." So again, yeah, yeah, yeah. I mean, I guess it's not like it's forcing anyone to do anything. But it does feel like a good thing to have. And maybe within the umbrella this creates communications channels. It allows companies that wouldn't otherwise be grouped together to share things.

Okay. So 34 tech companies that are very familiar to us are in the Accord as of the announcement last week: Arm, Avast, Bitdefender, BT, CA Technologies, Cisco, Cloudflare, DataStax, Dell, DocuSign, Facebook, Fastly, FireEye, F-Secure, GitHub, Guardtime, HP, Intuit, Juniper Networks, LinkedIn, Microsoft, Nokia, Oracle, RSA, SAP, Stripe, Symantec, Telefonica, Tenable, Trend Micro, and VMware. I don't know why Amazon, Apple, Google, and Intel are not on that list. They had to have been approached. It seems odd that any company would say we don't want to do this, or we don't want to have our name listed. Maybe they're not joiners. I don't know.

FR. ROBERT: It's probably the "collective action" bullet point because those companies do make part of their living off of having unique security and marketable security.

Steve: And unshared security.

FR. ROBERT: Correct, correct.

Steve: Ah, okay.

FR. ROBERT: The other thing about this is I like this. I mean, I love the fact that companies are willing to throw their hat into the ring. So I don't want to take any of that away. And I've learned to not say "but." So instead I'll say "and." And there is a problem. And the problem is that second bullet point. I mean, yes, I could do strong defense. Yes, I can do capacity building so I'll continue to have strong defense. Yes. Maybe I'm even up for collective action.

But the no offensive development clause is problematic because if the - I'm going to use my country because that's where we live. If the United States government comes to you and says we want this, it's very hard to say no, especially now since we've just had a law passed that essentially says they can do it anyways. Because what is material support? Material support might just be credentials that they're looking for. And they now have the ability to go into any server that a U.S. company controls and take what they want.

Steve: Well, and I wonder if material support means involuntary support. I mean, because in the U.S. we have court orders; and companies need to be able, I mean, they can fight them. But ultimately our courts decide ultimately, I mean, even if it goes all the way up to the Supreme Court, whether a company is allowed to say no or not.

FR. ROBERT: Yeah. And I get it. Look. There's going to be people who look at this, and they're going to say, this is just security theater. These companies, there's nothing in this accord that actually tells them what they have to do. But if you join enough of these, it tells you what people actually want out of your company. Remember when Microsoft first started releasing some of their products into open source, and people thought, oh, this is all just a big show. This is just Microsoft wanting to cozy up with those that they later intend to backstab. It turned out that, no, that was not a one-shot deal. Microsoft has actually been pushing more and more of their innovation into open source, and they've been [crosstalk].

Steve: Oh, we're about to talk about that at the end, yes.

FR. ROBERT: So, yeah, say what you want about it, I still think this is a net positive.

Steve: No, I agree, yeah.

FR. ROBERT: All right, Steve. So we've got two good pieces of news. My pacemaker won't be hacked quite as easily, and we've got vendors who are jumping on the security bandwagon. But what I really want to know is if I should stop screaming at my hard drives because I do it all night. I mean, they're in my NAS, and I'm just looking at them, and I'm saying, you know, you're just dirty. You're all dirty.

Steve: So we've covered this a couple times, and there's a famous - it's become famous - video on YouTube of some guy literally at the top of his lungs screaming at a large RAID array of drives, or a large drive array, and causing trouble. Which initially surprised people until we realized that of course sound is acoustics, which is mechanical. And today's state-of-the-art hard drives are still the storage medium of choice when you need ultra high-density in datacenters because, yes, solid state is coming online. But still, in terms of dollars per byte, where you absolutely have to have the highest densities and the lowest cost because you need so much storage, spinning media is still the way to do it.

In order to get the level of storage density that today's drives offer, the track spacing, I mean, the term "spacing," or the term "track spacing" is an oxymoron. There is no space between tracks. I mean, it's just - it's ridiculous what the TPI, the Tracks Per Inch is now. And so what that suggests is, since drives are still mechanical, that suggests that external vibration applied to the outside of the drive will translate into some motion that the heads, which are tightly controlled but are on a pivot, need to deal with. So all of the drives have a servo control system which maintains the heads on track. But it's already fighting that job, the job of maintaining the heads with essentially absolutely no tolerance. I mean, if there was any tolerance, the engineers would have removed it in order to get higher density. So you can't have any higher density, or they already would.

So against that existing challenge, you then essentially twist the drive. Not a lot, just a little. And that causes the heads to go off track. So that's why vibration is a modern hard drive's worst enemy, and sound is vibration. So in this famous YouTube video there was some - I think they were performing reads from the drive and intermittently screaming at these drives. And sure enough, the read rate dropped because the heads were driven off track by the screaming vibration. And the drive knew that it was off track. It's like, whoops, where did that sector go that I was looking for? And so it would have to go around again, another revolution of the drive, in order to retry that sector read. Consequently, the reading rate dropped.

And of course we've talked about SpinRite often where people talk about how their drive, their system is still working, but it's slower. And so what's happening is the drives are having to - the problems are beginning to be uncorrectable by the software algorithm. So the drive sort of shrugs internally and says, well, let's just try again. And so it waits for the sector to circle back around, and then it reads it, and it's able to correct it. SpinRite, of course, is able to work with the drive in order to fix the problem, in order to make the sector readable in a single revolution rather than taking multiple one or more retries. And as a consequence of that, people often find that, after running SpinRite, their computer boots again fast. It's like it used to be.

And in fact a couple weeks ago we talked about a story where someone's mom had lost her sequel to her first novel, couldn't read it any longer. And she'd been noticing that her computer had been slowing down, but she figured, well, that's what happens. Run

SpinRite, and she got her data back, and it was fast again. Oh, good, and now you're showing the video, yes.

FR. ROBERT: So he's got a big array, a RAID array of drives in a datacenter, and he's just screaming at it. And then they go to the status screen. And on the status screen you can see what's happening to the throughput because the error correction kicks up. And on so many levels this totally makes sense. It's a mechanical device. Vibrations are going to affect a mechanical device.

Steve: Yup.

FR. ROBERT: And by the way, thank you, Aneroid, for giving us that link.

Steve: Yes, thank you. And so what happened last week, last Wednesday in the early hours of April 18th at a Swedish datacenter, was actually something that we had talked about maybe a year ago. I think a year ago it was a test of the fire suppression system, as I recall. This time it was just an anomalous misfiring of the fire suppression system. These big datacenters, of course, have to protect their systems from any sort of fire. It's uncommon, but you could have some power supply blows up in a server and catches on fire. Okay, you need to put that out. So they use very high-pressure inert gas, which they need to get out of the tanks and into the atmosphere as quickly as possible. Sometimes, if these systems are not tuned, they are incredibly loud.

And so in the news coverage of this, it turns out that on April 18th the loud sound emitted by the high-pressure release of inert gas used in this datacenter's fire suppression system destroyed the hard drives of a Swedish datacenter, taking down the NASDAQ Stock Exchange operations - it was Nordic NASDAQ - across Northern Europe. And you might say, wait a minute, how could it destroy the drive? Well, if you are writing when this happens, that will destroy the drive because essentially writing occurs in bursts.

After you encounter the beginning of the sector you say, okay, we're on track. We're good to go. Basically you turn on a big electromagnet, which is very powerful now because it needs to write very small bits very fast. And it's assuming that, between now and when it gets done writing the sector, everything is going to be okay. But if something happens to that drive mechanically, you then cross-write, you're writing on a diagonal across adjacent tracks, and you can destroy the drive to the point where it's unrecoverable.

FR. ROBERT: Now, Steve, I'm thinking it didn't actually destroy the drive because our audience would pick up on this. The mechanical drive would be okay because the heads didn't crash.

Steve: Actually, it would have destroyed the low-level formatting, which is no longer something that you're able to correct.

FR. ROBERT: Right, you can't do that anymore.

Steve: Right.

FR. ROBERT: Because as the head moves it would bounce across tracks, and you're just writing a swath of destruction across a rapidly spinning drive, and there's no way to correct that anymore because you can't do that low level.

Steve: No.

FR. ROBERT: Wow, okay. Wow, I guess you do destroy the hardware.

Steve: So for what it's worth, anyone who's working with hard drives, pay attention to vibration. Vibration is not a hard drive's friend, especially these days, where the track density is just ridiculous.

FR. ROBERT: And just so you know, anytime here at TWiT we start having glitches with our servers, we're just going to blame it on Patrick Delahanty in the datacenter yelling at the hard drives.

Steve: Oh, yes, you want to get somebody who walks softly.

FR. ROBERT: Nobody here. Literally nobody here.

Steve: So, okay. So this is a weird story, but I thought it was worth discussing because we all know, especially this audience, that the SSID of a WiFi network, the name we give our WiFi network is, unless you make it private, that is, unless you tell it not to respond to beacon requests and to broadcast itself, it's public. And anyone these days who opens up their wireless monitor is sometimes entertained by the names that their neighbors have given their WiFi network. I have a buddy who his is like NORAD West Probe Station or something like that. It's like, oh, okay. I tend to be a little less creative, but it's often entertaining to see what people have called their WiFi networks.

Recently, Michigan police were called to a Planet Fitness Gym, and that was earlier this month, to investigate what was considered a bomb threat because somebody who was at the gym had named their WiFi network Remote Detonator. Which is probably not in this day and age a good idea.

FR. ROBERT: Not smart, no.

Steve: A different gym patron at Planet Fitness gym spotted what they considered to be a worrisome WiFi network name and called the police. And apparently that was in accord to the gym's normal procedures. The gym was closed down and reopened three hours later after bomb-sniffing dogs swept the building without finding any trace of explosive devices. And so I would argue that, while somebody might have thought it was a cute prank to name their WiFi Remote Detonator, even they were regretting the fact that their gym that they were trying to work out in was closed for three hours.

Saginaw Township Police Chief Donald Pussehl told a local paper that everything was legal from the police's standpoint. There was no crime, and no actual threat was made. No one called saying there was a bomb. It was just somebody who passively noted that one of the SSIDs, one of the available WiFi networks was named Remote Detonator. And apparently this is considered protected speech under the First Amendment. Now, there have been instances of this causing problems in the past. In 2016 a passenger on a Qantas Airline flight had named their WiFi hotspot Mobile Detonation Device. Again...

FR. ROBERT: Yeah, maybe just don't do that.

Steve: Not a good idea when you're getting on a plane. That grounded the flight for hours before it was cleared to take off. And again, I'm sure that passenger wasn't happy that the flight was grounded. Who knows what connections were missed. And sitting on the tarmac or being unable to leave the gate while people figure out what Mobile

Detonation Device is on a plane, that's going to be an inconvenience. And a year later, in 2017, a Turkish Airlines airplane made an emergency landing in Sudan after somebody onboard looked at the WiFi networks available and saw Bomb On Board was actually what someone had set their SSID to.

So anyway, I guess this takes the form of a public service announcement. That's probably, I mean, it's not technically illegal. Maybe it's a function of where you are in the U.S. First Amendment apparently covers this. You're not actively screaming "Fire" in a theater and doing something where you could argue that you have breached your First Amendment rights. But really, think twice before naming your SSID something inflammatory which, depending upon where you are, really could cause a lot of discomfiture to people around you.

FR. ROBERT: And here's the thing. I mean, we can go back and forth. This is not TWiL. This is not This Week in Law.

Steve: You are broadcasting something, after all.

FR. ROBERT: You are broadcasting. And remember that, even under the constitutional protections given to us, fighting words and words that are clear and present danger to the public safety are not protected speech. That's why you can't yell "Fire" in a crowded theater, and that's why me telling you that I'm going to kill you and your family is not protected either because those are fighting words. You could go back and forth on this because this is more passive. This wasn't someone threatening to blow something up or challenging someone. It was just someone being very stupid about what they call a publicly broadcasting device. And so let's not get into that. Let's just say, how about this, don't be that guy. Just don't be that guy. I think we can all be like that; right? Unless you want to be that guy, and you're okay with being that guy, don't be that guy.

Steve: Well, yes. Okay. How about be creative? Certainly there are a whole bunch of other really fun things that you could get up to.

FR. ROBERT: I've got one. So I've been doing a lot of time in planes over the last couple of months. In fact, I added it up the other day. Since the first of this year, I've spent a total of, is it 72 hours over the Atlantic? That's just over the Atlantic. So that's fun. That was, like, nine trips.

Steve: Wow, yeah.

FR. ROBERT: But on one of the trips, just for giggles because I had my gear with me, I set up a hotspot on my laptop, and it was Starbucks Free WiFi. And I used the exact same SSID that they use in every single Starbucks coffee store. I had 40 connections to that. So people obviously had not put their phones into airplane mode. But I'm thinking there were at least a few who were thinking, oh, Starbucks on a plane? Yeah, that's probably true. That's probably right.

Steve: Or if their phone had previously joined to that...

FR. ROBERT: Precisely, it would auto join.

Steve: Yes, then it's just going to auto join. It's going to go, oh, hey, I can...

FR. ROBERT: Which it shouldn't because they're supposed to be in airplane mode. But, eh, well, whatever.

Steve: That's very true.

FR. ROBERT: Try that, folks. And actually that's harmless. Try that the next time. Even if you only have an Android phone with a hotspot function, turn it on and just watch the client list and see how many will connect. So Starbucks WiFi is one that I use. The other is Free Airport WiFi. There's a bunch that use that. Just see what auto connects.

Steve: That's a very good point. It does demonstrate that we're not in airplane mode.

FR. ROBERT: Yes, yes. All right.

Steve: Okay. So the trouble with our consumer routers. We've spent a lot of time over the last few months especially because the typical consumer router is a purchase-and-drop-in, sort of a plug-and-go. The router comes out of the box able to function. You plug the WAN end into your cable modem or to your DSL modem. It uses DHCP to acquire the IP that your ISP has given it. You plug your wired devices in over on the LAN side. It has a DHCP server that does the same thing, giving everybody an IP. You obviously have to give it a password in order to set up your LAN, and give it an SSID, give it a name. And unfortunately, at that point, that is the last time most people ever think about their router. It's basically plug it in, make it work, walk away.

A publication in the U.K., Broadband Genie, out of curiosity, conducted a survey of a little over 2,200 of their readers of age greater than 18. So, okay, I guess you'd expect a certain level of maturity and responsibility and so forth. What we know is that routers can have security problems, have historically had problems, have had manufacturer-implanted backdoors with fixed passwords. There are worms on the 'Net that are checking routers for vulnerabilities. There's Universal Plug and Play that is enabled by default. My own ASUS, a recent ASUS router that I purchased, I was very impressed. It had "Respond to ICMP ping request" disabled on the LAN, but UPnP enabled on the WAN.

FR. ROBERT: Oh, so close.

Steve: And it's like, guys, why?

FR. ROBERT: Why? Why?

Steve: Why UPnP? What possible reason to have Universal Plug and Play enabled on the WAN interface?

FR. ROBERT: And ASUS is actually one of the better ones.

Steve: Yes, yes. It's an impressive router. It's got four guest networks and all bells and whistles and dynamic free DDNS and everything you could ask for. And Universal Plug and Play enabled. I just - I can't understand it.

And I guess it's because they also have remote - oh, it even has Let's Encrypt. It builds and binds a Let's Encrypt SSL cert to your router for you, so you're able to do an HTTPS external connection to it. So it's amazing. But Universal Plug and Play enabled. And maybe it's so that you're able to open ports and get to it, unfortunately. Or at least as a mixed blessing.

Anyway, the point is this was the Picture of the Week at the top of the show notes. I have it here again in our show notes. This Broadband Genie survey asked 2,200 people about their router history. How many have ever updated their router's firmware? Answer:

14%.

FR. ROBERT: Wow.

Steve: Yup. How many ever changed their network name? I mean, okay, now, I'm like, how do you not do that? I guess it must come with some - in fact, I guess I know because I remember looking at a list of available WiFi just a couple days ago, and there were, like, four Linksyses. That's all it said, "Linksys."

FR. ROBERT: Or Comcast.

Steve: How do you know it's...

FR. ROBERT: They will give you the SSID and the password on a piece of paper, as well as on the modem itself. So most people don't even change it. They'll go, oh, okay, guess that's what I'm going to use. They don't even know how to get into the management page.

Steve: And 18%, only 18% had ever changed their WiFi network name. That same 18% had ever changed the admin password. Meaning that the default admin password for, what, 82% of all WiFi routers among this population has never been changed.

FR. ROBERT: And if the default was also to allow remote login, that's a problem.

Steve: Yup, exactly. If WAN admin is enabled, as it sometimes is on routers, you're hosed. You will have somebody, even if there's no known vulnerability that lets a worm get into your router, if somebody has any interest in you, they can get in and start browsing around your network. So, wow. And we know, for example, that Universal Plug and Play can be used, we were talking about it last week, to turn your router into a public proxy in order to use you as a waypoint for malicious traffic bouncing around the Internet. Which is not how you want your bandwidth used.

FR. ROBERT: No, not really, not really.

Steve: Only 30% of router owners ever check to see what devices are connected to the network. So they're just like, oh, you know. I mean, famously in the old days, of course, everyone's neighbors were using their WiFi. Now everybody's neighbors has their own WiFi. Once upon a time that was, you know, it was like, oh, yeah, I'm just using my neighbor's WiFi because he doesn't care. It's like, okay.

And only 31% had ever changed their WiFi password. So it's exactly as you said, Father. It's like, okay, 69% just took what was written down and typed it in. Hopefully it was secure. Wow. And half the people, none of the above. Half the people none.

FR. ROBERT: Of course. Well, half of the people don't even know that they should do that. That's the thing. That's the real issue. It's not malicious. It's not, oh, yeah, I should do that, but I'm not going to. It's a device, and they figure that they bought the device from the provider - Comcast, Cox, whatever it's going to be. And the provider's going to take care of it, which of course we know, of course they're not going to do that. But they don't know that. They don't know better.

Steve: These things are sold as appliances that you plug in and you do nothing with. And so we're going to talk about here at the end of this podcast today Microsoft's initiative for potentially changing this. And it's the reason, as I said at the top of the show, I'm very bullish about this. We have to as a, well, more than as a society, as a global community, we need to change the way we do this. It has to be that moving forward this device takes care of itself.

This device, I mean, we don't need to change anyone's behavior. It can be fine that they buy something and plug it in and set it up. But it has to be able to take responsibility for managing itself. And I'm somewhat dumbstruck that that hasn't already happened, that it's still - like, for example, if I log into my ASUS router's admin page, there's like a flashing yellow exclamation point telling me that, oh, look, you need to check to see if you've got updated firmware. And often there is new firmware. It's like, okay. Why doesn't it just do this? Why doesn't it wait until 2:00 a.m. and download and reinstall firmware for me?

FR. ROBERT: I actually asked that. So my router of choice right now is the Synology series. They make the 1900 and the 2600. I like them because they're Linux based, and they are very good about firmware because they also do NASes, and they're always updating the firmware for the NASes, and they share components between the operating systems. But the one thing that's always bothered me is the router will, by default, look for updated firmware and download it so it's ready to go. But it won't pull the trigger.

And I asked my Synology guys, why not pull the trigger? And they said it's actually a legal thing because, if something happens, we're in trouble. It's like, okay, then that's a piece of law that we need to fix because, like you said, most people are not the audience of Security Now!. Most people...

Steve: Never, never, never going to.

FR. ROBERT: Never going to. They think of it as an appliance, so it needs to work like an appliance. I don't think about updating my refrigerator's firmware, so I shouldn't have to think about updating my router's firmware. And we need to make it okay for companies like ASUS and Synology and even Linksys to turn that switch and say, you know what, we're just going to take care of this for you. When it's a weird time and no one's using it, I'm going to go down for 10 minutes so I can update my firmware. And then of course when that happens, and that's going to be wonderful, there'll be people like me who are screaming, "Why did you choose 3:00 a.m. to update? Of course I'm working at 3:00 a.m. You're horrible."

Steve: Right, right.

FR. ROBERT: It's a no-win.

Steve: So there was, again, a lot of interesting news about Google's announcement of a new messaging system for their Android platform. It was funny, I think it was on Saturday Megan and Jason covered this. They didn't cover the angle that we take on this podcast. But they were, I mean - and of course Jason is Mr. Android. They did talk about all the attempts that Google has made through the years at messaging. And nothing they do gets traction. iMessage is still sort of the industry standard for it just works. It does everything people want. If you're an iOS user you get the blue balloons, and the two friends that you have that are on Android, they get green because they have to use SMS.

Well, what the press picked up on is an interesting flaw that exists and has a lot of the press scratching their head. First of all, Google calls it "Chat." And what it is, is a standards-based extension of the existing SMS and MMS, using something called RCS, which is Rich Communication Services. And within RCS there's this notion of a universal profile which is sort of the set of detailed interactions and specifications within RCS to allow everything to interact so that, if all the carriers supported the universal profile of RCS, then everybody would be able to interact.

And to Google's immense credit, what they have somehow managed to do, and it's phenomenal, actually, is they've gotten, I think it's 34 carriers, 11 somethings, and two OEMs, maybe it's 11 OEMs and two manufacturers, to all agree and all support the universal profile for RCS. What this means is that the forthcoming Google Chat for Android will be universally interoperable globally.

And it was Verizon and one other, I can't remember, two final major carriers, even they went with it. They dropped this notion of trying to differentiate themselves and go their own way. It's like, you know, no. We're going to do this new chat app which is going to use RCS. And sure enough, on the surface, it delivers an experience like iMessage. You know, multimedia, return receipts, group messaging, a lot of the things that have not been available before. However, it misses one arguably important feature. There's no encryption.

FR. ROBERT: Wah-wah.

Steve: Now, thinking about this, I guess I can kind of understand that maybe Google can't solve this problem. Apple can because they manage the keys. They're the closed ecosystem, and you're tied into Apple and iOS, and they're pushing versions and everything. And again, stated simply, they manage the keys. We've just been talking about how Telegram has been recently and incrementally, but now completely, pushed out of Russia, and previously was pushed out of China. Well, Google doesn't want their chat app to be outlawed by major segments of the globe. You know, China is big. And Russia is huge.

So I guess they probably decided, okay, we're going to finally come up with a way to give our Android users the features they want and not battle, not do this encryption battle which is brewing, just not have that be our problem. If individual users want encryption, they can use Signal. They can use Telegram where it's legal. They can solve that problem one way or the other. But for most people, and it turns out that most people do - all the studies show most people use whatever is the default chat app in their Android device. Very few people bother with a third-party chat app unless they have some need or reason for it.

So I think what Google is doing is just saying, okay, we're going to, by pushing the standard to universal profile for Rich Communication Services, even though there's no encryption, we're going to give people the experience they want. And lots of people probably don't care.

FR. ROBERT: Yeah, that's true. I mean, encryption to a lot of people still sounds like hocus pocus. And as long as it does what they want it to do, they'll use it. Although, Steve, I will say this. So I just came back from Rome. I had an international meeting with my counterparts from across the world. So I had a representative from the African nations, a representative from the Asian nations, a representative from the European nations, the Latin American nations, United States, and India.

Steve: And they're all like other versions of you?

FR. ROBERT: Basically, yeah.

Steve: Okay, cool.

FR. ROBERT: I'll be the Curia counterpart, so I'm at the headquarters, and we all do the same work. But it was interesting because we were looking for a way to communicate with all of us. And we went through a couple different solutions. They didn't want to use Slack, and Hangouts was a nonstarter for them. But every single one of them except for the U.S. delegate used WhatsApp. That's the big one. And they won't go anywhere without it. So I'm thinking, unless you can offer more than what WhatsApp offers, you're not going to crack outside of the U.S. market that much. That's just a thing. So Google can make yet another client because they're really good at doing that. They've done a couple since Hangouts, and Hangouts is still around.

Steve: And Allo they also are giving up on, by the way. It's just like, okay, fine, that never happened. It just didn't get traction.

FR. ROBERT: That's why it's so hard for me to get excited about another Google Chat release because I'm thinking, well, in three years they'll come out with one, it'll be better, and maybe it'll have the things I want this time, like encryption.

Steve: Well, it is nice, and I thank them for moving the cellular industry forward beyond SMS and MMS, that had been the lowest common denominator. Essentially it was the lowest common denominator. And so, if nothing else, this has forever moved the cell industry because everyone has agreed to support it, has upped the ante now to what is arguably a more useful functional chat system as a new lowest common denominator. But as you said, at the cost of you guys, your team can't use it because you need to have some control.

FR. ROBERT: Now, Steve, next up, you know what I'd love to do? I would love nothing more than to allow Amazon to get into my car whenever they'd like to. So I want to talk about that. Want to talk about that?

Steve: What could possibly go wrong?

FR. ROBERT: What could possibly be wrong with that? So, Steve, I was really, really not comfortable with allowing Amazon into my home just by pressing a button. But I think I would totally be okay with them having a special button that just pops my trunk anytime they want.

Steve: Yeah. So they've been circling around this for about a year. There have been some pilot tests. And today, on April 24th, they announce the availability of delivery to the trunk of your car. So this is a new delivery service which they're rolling out for General Motors and Volvo vehicles initially. It's available in 37 cities starting today. So essentially what this uses, it uses, in the case of GM, the OnStar system, which is a communications system between your car and the cloud, literally, above you in the cloud. And Volvo has a similar system for a connected vehicle system. This allows them to know where your car is parked.

You use their application, the Amazon Key app, which you add your car to the Amazon Key app, and you take a picture of it so that the Amazon courier is able to identify it. They need your license plate also in order to make sure they're using the right one. And essentially the delivery person queries Amazon to get the current whereabouts of your car. It does need to be within a reasonable distance of your physical delivery address. So, for example, it can't be the other side of the country, or in a different country, or maybe even in a different state. So the idea being home or work sort of location.

And this of course is trying to solve the problem of secure delivery. Many people who are, for example, apartment dwellers don't have a convenient place where Amazon can leave packages where they have sufficient security. Or even if you are in a condo or in a community, or in a home where there's a lot of foot traffic, it can be problematical to leave boxes somewhere. So Amazon has done things like having the Amazon Lockers, where they put something, and then you go and get it. And so this is an attempt essentially to turn the trunk of your car into a semi-private locker.

The technology of OnStar and Volvo's technology allows them to unlock your car. So this is all basically - well, to locate your car and to unlock it. So it's easy to put the pieces together. The Amazon courier determines where the car is, goes there, identifies it visually, verifies the license, is standing next to it, presses a button on their app. And with the knowledge that they have a delivery, they probably have to scan the package, verify that they have it. Everything makes sense. Amazon verifies that you are expecting a package; you're expecting a trunk delivery.

And so your car spontaneously unlocks for this Amazon person, who then puts the package in the trunk, closes the trunk, relocks the car, and all of these things have to happen in order for the delivery person to have successfully delivered the package and then get their next assignment. Packages are limited to 50 pounds. They cannot weigh more than that. They cannot be larger than 26x21x16. They cannot require a signature. They cannot have a value over $1,300, nor can they be from a third-party seller. They can only be from Amazon directly.

FR. ROBERT: That's to stop scams; right. So that's to stop vendors from trying to scam through this.

Steve: Exactly. So anyway, I get the problem they're trying to solve. Maybe it's better than a drone flying overhead and dropping it on your head. Not clear on that one. And again, we immediately saw problems where, as you commented, Padre, that people were aiming a webcam at the front door, and it took, what, was it a week before all kinds of...

FR. ROBERT: It might not even have been that. I think it was, like, three days.

Steve: I think it was, before that system got hacked. So I guess, I mean, no one is going to not understand that you're giving Amazon permission, with lots of caveats, to have access to the interior of your car. Hopefully people don't have super valuable things already because we know that cars are not that secure. Locks can be jimmied. Windows can be broken and so forth. So I guess within - and I don't think it unlocks only your trunk. I think the car unlocks. All the doors pop open. I don't think it's an exclusive trunk unlock. I'm not sure. Maybe if the system can provide that, then it's just the trunk. For example, I think my car's trunk is able to unlock. I don't have any connectivity. I'm driving something old.

FR. ROBERT: I don't have any connectivity, but I can unlock my trunk without unlocking my doors. And also I have the ability to disable the lever on the inside so you can't actually pop my trunk from the cabin. You need both my key and my fob to make that work. So I have to put it in the keyhole, and I have to press the fob in order for it to pop it.

Steve: Nice.

FR. ROBERT: I know most people don't turn that on because I'm kind of paranoid. But I'm with you, Steve. I understand why they made this. And I will make fun of it mercilessly because I think it's a horrible, horrible idea. But there is an edge case or two where this would be more convenient than, say, having it delivered to an Amazon Locker that you then go to to get. So, okay, sure.

Steve: Yeah. If your car is sitting in an accessible parking structure all day, and you're at work, and you want something delivered to your trunk, and you have not left anything valuable inside, it's not as if any random Amazon employee is able to walk up to your car anytime they want to and open it. I mean, so it is as locked down as it can conceivably be, given that it has to be - you are allowing under certain requirements your car to be opened. So, yeah, okay.

FR. ROBERT: Aneroid in the chatroom brings up a good point, which is, if they could do this service while your car was in motion, then it would be worth it for the entertainment value. You're just going down the highway. Suddenly your trunk pops open and there's a guy leaning out the front of a car, just trying to drop the box in.

Steve: That's right.

FR. ROBERT: Okay, okay. That's it for the Amazon - what are they calling that, the Trunk Club?

Steve: I don't think - I didn't see a name, actually, associated with it. In-Car Delivery.

FR. ROBERT: In-Car Delivery. Do you remember those commercials, 10, 15 years ago of the trunk monkey? This kind of reminds me of that. It's just something that maybe 10 years ago people would have thought of, yeah, I'm going to allow a retailer access to my trunk? This has the same sort of feel. I'm going to allow someone to put a monkey in my trunk? I'm sorry. I might be dating myself with that.

Steve: And of course, if people don't have connected cars, it's not an option.

FR. ROBERT: Right, yeah. And also I would say, if you have one of those cars that doesn't have a separate trunk from the rest of the car, I probably wouldn't do that, either.

Steve: Yes. Then your interior is accessible to somebody at the trunk.

FR. ROBERT: Also it means that someone could just watch a delivery car and then know which cars they should break into because there's a brand new box in there. There's the trunk monkey. Thank you. John Slanina, always ready with - ooh. Ooh. Actually, that might work better than the Amazon Delivery Service.

Steve: So our listeners know that I enjoy puzzles. I have an affection for clever, well-designed puzzles. And as I mentioned at the top of the show, I feel I'm very picky because our listeners who know this are sending me links to discoveries of theirs all the time, and few of them make the cut. Infinite Loop was a previous favorite of ours. The Sequence is probably the all-time blockbuster puzzle, like fan favorite or podcast favorite. The Sequence was multiplatform, and essentially it was visual programming. Your goal was to design a little visual machine which would move pucks from a source to a sink, and do it repetitively. And, oh, my goodness, fabulous. Blockwick was another, which was just a terrific take on the traditional sliding block puzzle.

The things I like have a number of features in common. There's no timer. There's no time limit. There's no [buzzer sound] bothering you. There's no rush. There's no hurry. It's meant to be enjoyable and relaxing. So you also don't need to worry about running out of anything - time or turns or attempts or choice or anything. That's not what it's about. It's about getting from the start to the finish at your own speed, making mistakes, being forgiven infinitely, and also having a sense of progress, a sense of, okay, I can see that I'm getting somewhere. It's not a sudden, like, aha sort of thing.

So with all of that preamble, I found another one, and it's on the screen. And I like it. It's not free. I paid $3 for it, I think $2.99, through iTunes. It's called Dissembler, D-I-S-S-E-M-B-L-E-R. It appeared at the end of February, and I just happened to see it by a coincidence, at a moment when I was receptive. Brand new concept, simple, original, very clean. No timer, no ads, no annoyances. You can undo things without limit. Anyway, it's got nice background music which, yes, you could turn off. There are people who don't like anything making noises or background music.

I've only spent a few hours with it, so I can't vouch for it in the long term. But it's really a nice concept. And for those people who have liked...

FR. ROBERT: But what am I trying to do here?

Steve: Oh, okay.

FR. ROBERT: Oh, I see. I get it. All right.

Steve: The idea is that you...

FR. ROBERT: Oh, it's cute, yeah.

Steve: With the Pad or the - it is available on Steam, so if you wanted to you're able to use it on any Steam-compatible platform. But essentially you have an array of colored squares in a certain pattern, and you're able to flip any pair of them. And when you do so, if you get three or more contiguously connected of the same color, then it's removed from the board.

FR. ROBERT: Oh, I love these. This is a sequence game. It's all about the sequence.

Steve: Yes.

FR. ROBERT: I love those.

Steve: Yes. It's really well done. So again, I haven't - it's been months since I found something that I could recommend. I can recommend this. I don't know where it goes in the long term. I did read some reviews before I wanted to recommend it. And there's a concern that it gets too difficult. There is, however, an infinite levels mode where you can just say, just make them up. I just enjoy solving these puzzles. I think the first 120-plus are deliberately designed and really very nice. So anyway, Dissembler, my first puzzle recommendation in a long time.

FR. ROBERT: That might be my next airplane hit because...

Steve: It would be perfect for an airplane, yup.

FR. ROBERT: Jason Howell got me onto Monument Valley, which I love.

Steve: Oh, yes, yes, yes, yes, yes.

FR. ROBERT: But it's so limited. I mean, I went through that game in 20 minutes.

Steve: Yes. You end up solving it, it's like, oh, crap.

FR. ROBERT: I need more. Give me more. So, yeah, if there's an unlimited, that could get me over the Atlantic the next time I have to go. All right.

Steve: Okay. So time to talk about Azure Sphere.

FR. ROBERT: Yes, I like.

Steve: And I'm impressed. Everybody knows I don't carry Microsoft's water ever. I'm the person who wrote Never10, so that gives you a sense for my position on Microsoft. They've done something great. There is a group known as Microsoft Research which is sufficiently disconnected from Microsoft Profit - and that's not P-R-O-P-H-E-T, that's P-R-O-F-I-T - that Microsoft Research Group are able to do good things.

What they have done with Azure Sphere is design a complete front-to-back, soup-to-nuts, open, free ecosystem for securing IoT devices. It starts with an IoT-friendly processor, a custom chip design, which is a variation of an existing MediaTek chip. Remember that ASMedia were the bad people who put the backdoor in the AMD chips. That's not these people. MediaTek are good people. One thing you can do, Padre, is google MediaTek, M-E-D-I-A-T-E-K space MT3620. In my show notes I didn't have a link. But MediaTek, it's the MT3620. That's the processor which Microsoft designed in collaboration with MediaTek. It is what we need for IoT. It has the equivalent of the Apple Secure Enclave in hardware. And that's this wacky thing they call Pluton. It's the hardware security side.

About a year ago Microsoft Research produced a document titled "Seven Properties of Highly Secure Devices." And I do have a link to the PDF in the show notes, or you can probably just google "seven properties of highly secure devices." The first property is a hardware-based root of trust, meaning that you have unforgeable cryptographic keys that are generated in and protected by hardware. Which means that they are physically resistant to side-channel attacks, and it gives the device a unique unforgeable identity that is inseparable from the hardware. This has that. Also, a small trusted computing base.

So you have private keys stored in a hardware-protected vault, inaccessible to software. Remember that that's possible. That is, you can have your private key sign something without the key itself ever being accessible. You can only ask it to do the work of signing. So this creates a division of software into self-protecting layers.

Then you have defense in depth, multiple mitigations applied against each threat. Then compartmentalization, certificate-based authentication, renewable security, and failure reporting. Those are the seven properties which Microsoft incorporated into the system. So we first have an amazing little chip that will be available for developers to play with around the middle of the year and available for MediaTek toward the end of the year. However, the intellectual property, the IP of the chip, 100% free. It is license-free. Anybody else who wants to make this chip is able to do so. This chip is a multi ARM...

FR. ROBERT: Cortex, yeah, A7.

Steve: Exactly. It has an application-level processor which is a single-core ARM Cortex-A7 running at 500MHz. Then it's got sub-processors. It has a dual core ARM Cortex-M4 with a floating point. It's got A-to-D converters, general purpose I/O, I2C, I2S serial interfaces, pulse with modulation, an SPI interface and a UART built in, both 2.4 and 5GHz WiFi ABGN, all of this on chip. And a custom Linux that is a secure Linux distro which Microsoft named Azure Sphere OS, also part of this. And, finally, a cloud-based service which is, I was stunned, not tied to Microsoft.

FR. ROBERT: Right.

Steve: It's an open cloud-based service that allows - so essentially Microsoft has designed and done all the work of creating an affordable, feasible, truly secure, cryptographically secure and enforced in hardware based chip. It has both RSA and elliptic curve technology built in, and all the hardware and other support you could want in order for making a low-cost, like consumer-cost, WiFi-connected device that knows how to identify itself to whatever cloud services somebody wants to tie it to so that it's able to essentially do exactly what we were talking about with a router.

In fact, this would be a perfect chip to use for a little router. It's got all the I/O and capabilities that a router would want and the ability to check in with a cloud for the cloud service to verify on an ongoing basis the true security and update in a secure fashion, as well. So that, for example, it's able to receive signed update packages that cannot be forged because they are signed by someone whose keys are built into this thing and that are only accessible to it. I couldn't be more stunned and delighted that Microsoft has done this.

FR. ROBERT: Just looking at the spec sheet, I mean, it is impressive. There is a question to me about how low power it is, in other words, how much does it consume, because that will determine what types of applications this will be used for. But with that many GPIO - so you've got 72 GPIO. You've got 12 PWM counters. It does I2C, SPI. Basically everything that you would want out of, say, like an Arduino training kit, all the way up to industrial automation, this looks like it could handle, which is phenomenal.

Steve: Five UART I2C and SPI interfaces, eight analog-to-digital converter inputs.

FR. ROBERT: Dual-band WiFi. That's impressive on such a small package.

Steve: Yeah.

FR. ROBERT: But, Steve, how is that key stored? Does this have some sort of equivalent of like a Secure Enclave?

Steve: Yes, yes.

FR. ROBERT: It does.

Steve: Yes, yes, yes. So that is absolutely key to it. So they call this thing Pluton (P-L-U-T-O-N) security system. And they said outside of these three end user-accessible cores - so we talked about the application core, and there's the sub-processors. There's also the WiFi has its own core that runs the WiFi. So outside of these three end user-accessible cores, they say the MT3620 contains an isolated security subsystem with its own ARM Cortex-M4F core that handles secure boot and secure system operation.

In addition, a 1x1 dual-band 802.11 a/b/g/n WiFi radio subsystem is controlled by a dedicated Andes N8 32-bit RISC core. This subsystem contains radio baseband and MAC that is designed to allow high-throughput applications with greater power efficiency. They said operation of the MT3620 security features and WiFi networking are isolated from and run independently of end-user applications. Only hardware features supported by the Azure Sphere secure IoT platform are available to 3620 end users. As such, security features and WiFi are only accessible via defined APIs and are robust to programming errors in end-user applications regardless of whether these applications run on the Cortex-A7 or the user-accessible Cortex-M4F cores.

So essentially it is hardware secure, presenting an API which allows you, for example, to ask the Secure Enclave, which is what this is, to sign a hash of something for you, but never expose the hardware, the private key, and only perform the operation, not give you access to the raw material. I mean, I'm just, it's like, yay.

FR. ROBERT: They're giving away the chip. But that part I'm gathering will work best if you're using it with Azure services because that whole idea of being able to store the key and have updates securely delivered to the chip is probably going to be a bit smoother if you're using Microsoft's web services.

Steve: Well, it's all open. Okay. So they said: "Azure Sphere Open Cloud." They said: "The Azure Sphere Security Service guards every Azure Sphere device. It renews security, identifies emerging threats, and brokers trust between device, cloud, and other endpoints." So I agree with you, Padre, that certainly they could be providing those services, and I would imagine many manufacturers, as long as Microsoft makes it affordable, would just rather turn that over to Microsoft. However, Azure Sphere, they say, gives you choice. You can connect data from any cloud, proprietary or public, or even your on-prem infrastructure, to the Azure Sphere Security Service. And I read also elsewhere that it worked with Google or AWS or any other cloud provider.

So again, they're not trying to make this about Microsoft. I mean, they look, from everything I've seen, their heart's in the right place. And it looks to me like they've done a beautiful job. Anyway, tons of links in the show notes. All of the information is available online for anyone who's interested, and a dev kit available in a couple months. And I don't know if you ran across a picture of it, but it's a cute little Arduino-looking sort of thing.

FR. ROBERT: Yeah, I couldn't find a picture.

Steve: It probably has the same - it's got the two opposing rows of headers. So I would bet that it's got Arduino-compatible pins.

FR. ROBERT: Well, Mukti in the chatroom is saying, well, what's Microsoft getting out of this? Well, that's actually really easy. Gartner came up with their magic quadrants, and by the end of 2018 they expect just the security component of the IoT to hit $1.8 billion. That's just one component of a multibillion dollar industry. So Microsoft is hoping that in doing this you will associate Microsoft with secure IoT. And if you associate Microsoft with secure IoT, it's much more likely that you're going to choose them as the vendor for your IoT solution. That's what they get out of it. There's nothing nefarious about it. There definitely a profit in store for Microsoft, if this works well.

Steve: Yeah.

FR. ROBERT: I'm excited, Steve. I mean, this has been something that we've been looking at for a while, which is a security-centric approach to the Internet of Things because no one, no one is going to be able to argue that the Internet of Things doesn't have problems. We've been seeing it since it first became a thing. And actually the Internet of Things really first started coming around when I first came onto the network. That was one of the very first things that we reported on for This Week in Enterprise Tech. And it became very rapidly, rapidly obvious that even though the devices were interesting, and they reported back interesting data, that security just was not there. And there have been so many talks over the years about how we're going to improve that, we're going to put security first. To see a big player actually do that, I like that.

Steve: Well, and the problem is everyone has traditionally approached this from here's what I want to do. Okay, here's a chip that will allow my coders to code the app that the thing does. Instead, we start with an architecture that is all and only about security, which is open, and which you then lay your software on top of. So, I mean, it turns it around where it puts security first. And I'm just like, okay, yes. I have no problem if there's competition for it, but at least now there is a solution. And I can't see a downside.

FR. ROBERT: No, I really can't. I mean, if Microsoft can give me an open piece of hardware that I can thoroughly scrutinize, I can go forward and back and look at all the different solutions, all the different components that they've included and say, okay, the hardware is secure. The communication for the firmware is secure. That gives me the confidence to then design a device that might have access to, say, oh, I don't know, medical information, or personally identifiable information. It means that when I'm designing my IoT device, I don't have to worry that it's going to be the malware vector for my network. And that changes what I think is possible with IoT because, if I'm assuming, as I am right now, that every IoT device I put on the Internet is going to get owned, it changes what I think is possible.

Steve: Well, and imagine if this acquires a reputation, if you're looking around for solutions, that is, as a consumer, and you have heard that Azure Sphere is the way to do secure IoT, then that's what you choose. So it becomes a competitive advantage for manufacturers to embed the Azure Sphere platform into their solution. We'll cross our fingers.

FR. ROBERT: Right. Well, Steve, I've gotten to the bottom of this doc here, and that's wonderful, except for the fact that I haven't heard about SpinRite at all. Don't we normally talk about SpinRite during these episodes?

Steve: Well, I did talk about shouting at drives and SpinRite. And all of our listeners know about SpinRite. And so thank you for bringing it up. I will remember to bring a story to our listeners with you next week.

FR. ROBERT: Actually, I do have a story because I knew I would be hosting this show with you.

Steve: Yay.

FR. ROBERT: So I had a little tidbit.

Steve: Cool.

FR. ROBERT: One of the things that I did for our IT at what we call the Curia - it's our worldwide headquarters, you know, and that's where I'm going to be working next year. But the last visit I made I had a meeting with their IT guy. And we always have an issue with wireless in the Curia. It's an old building. Wireless signals don't go through really well. So I told him that I would bring some of my enterprise gear, some of my enterprise wireless APs. I brought some Zero stuff, some Ubiquiti stuff, some Rocket stuff. And I told them, here, play and see what works best.

And then he said, "Well, do you have anything else in your toolkit?" because he loved the toys that I brought. And I said, "Well, there's one thing that I always have with me, and you could use it while I'm not here." And I had my copy of SpinRite. So I put it in my little folder, and I said, "Just take care of this for me." He's had it for a total of three days, and he just wrote me, and he said, "I've used it six times." And he said, "It's amazing because we had some systems that we thought were dead, and they were in the corner, and I was going to work on them when I had it. And on a whim I tried SpinRite on one of the rotating drives, and it worked perfectly, and it brought it back to life, and I've been able to copy stuff off." And he goes, "I'm now going to go through our entire inventory and see where this might help." So SpinRite is officially in the Vatican.

Steve: Yay.

FR. ROBERT: You can put that on your site.

Steve: Nice. Well, it made it to the International Space Station.

FR. ROBERT: There you go.

Steve: And so now it's in the Vatican. Very nice.

FR. ROBERT: So it made it into the hereafter and made it into the here yonder.

Steve: That's perfect.

FR. ROBERT: There you go.

Steve: Thank you for telling us, Padre. I appreciate that.

FR. ROBERT: Folks, we thank you for joining us. Of course I'm Father Robert Ballecer. That's Steve Gibson. We do this show every Friday. Now, normally it's with Leo Laporte, but I have the honor, the privilege of doing it for the next two weeks, including this week. I'm sorry, every...

Steve: Every Tuesday.

FR. ROBERT: Every Tuesday. Did I say Wednesday? I mean Tuesday at 13:30 Pacific time. I'm not going to do UTC because that's a Leo thing he's really good at. Now, Steve is always here to inject you with a healthy sense of paranoia. Folks, it is still paranoia if they're out to get you. But, you know, sometimes it makes you look better. You can find all of our shows at TWiT.tv/securitynow, including back episodes, and a place where you could subscribe if you want to get your security goodness into your device of choice every week.

We've got an audio version, a video version, and a high-definition video version, as well as versions in iTunes, Stitcher, and wherever fine podcasts are found. Don't forget that you can also get high-quality audio recordings at GRC.com, which is the home of Steve Gibson, where you'll also find his outstanding products like SpinRite, ShieldsUP!, and coming soon, SQRL.

Steve: And SpinRite is now Vatican-approved.

FR. ROBERT: And it is now Vatican-approved. You actually can put that there.

Steve: That's very nice.

FR. ROBERT: We are extraterritorial. It's been an absolute pleasure, Steve. And next week can I present a theme? Because a big fan of your show, I don't know if you know this, but David Hewlett, who played Dr. Rodney McKay in the Stargate franchise, he has watched or listened to every episode of Security Now! ever.

Steve: No kidding. Wow.

FR. ROBERT: He is a huge fan. So I'm thinking...

Steve: Well, and I'm a fan of his.

FR. ROBERT: I'm going to see if I can send you a Stargate Atlantis patch, and I'll wear one, as well. And I'll see if I can bring in my - hopefully my ZPM will be done by then. We'll go through the Stargate of Security, the Security Gate.

Steve: Nice.

FR. ROBERT: Does that sound doable?

Steve: I look forward to talk to you again next week, my friend.

FR. ROBERT: All right. Steve Gibson, Fr. Robert Ballecer, and remember that if you want to keep your data safe going into the future, you're going to need some Security Now!.