The Internet of Troubles

Description: This week we continue following the continuing agony surrounding this month's increasingly troubled Window Update. We examine several significant failures which have befallen Windows 10 users after applying the month's "fixes," which have had the tendency of breaking things that weren't broken in the first place. We look at the danger presented by a very popular GDPR-compliance add-in for WordPress sites. We look at an eye-opening report about the stresses that CISOs are being subjected to, and also today's pilot test of Microsoft's new ElectionGuard voting system. We then touch on some SQRL and SpinRite news before taking a close look at two newly revealed IoT - Internet of Troubles - security worries.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-754.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-754-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here. Yes, more woes. And this time, not just Windows 7; Windows 10, too. We will talk about the troubling life of a CISO. If you're one, we have the deepest sympathy for you. And then the trouble with the Internet of Things, including a new Bluetooth flaw named after the son of Harald Bluetooth. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 754, recorded Tuesday, February 18th, 2020: The Internet of Troubles.

It's time for Security Now!, the show where we cover the latest security and privacy updates with this guy right here. He's the man in charge at the GRC, the Gibson Research Corporation. I give you Steve Gibson. Hello, Steve.

Steve Gibson: Leo. You have said that 754 times.

Leo: Holy cow. I don't know, I think that intro isn't quite as old as the show is.

Steve: That is actually true. I was thinking the same thing. So this was one of those weeks where initially, as I pulled everything together, nothing really stood out badly until I did some digging into a couple of the stories, and I thought, okay. So we've got two very worrisome IoT things. So this podcast this week is the Internet of Troubles.

Leo: Oy.

Steve: We're going to continue following the continuing agony surrounding this month's increasingly troubled Windows Update, in this case affecting Windows 10 people because Windows 7 people, they had their problems in January. Now it's Windows 10's turn in February. The monthly fixes have had a tendency to break things that were not broken in the first place. So we're going to take a look at that.

We're going to look at the danger presented by a very popular GDPR compliance add-on for WordPress. Also we're going to take a look, as I was talking to you before we began recording, at an eye-opening report about the stresses that are being subjected or that CISOs are being subjected to. It turns out the average employment duration is, I think, well, the report says it's 26 months because, I mean, it's just so bad being a CISO.

Leo: The time to breach.

Steve: Yeah. And then it's your fault.

Leo: It's your fault. Goodbye.

Steve: Yeah. Also today it's Tuesday, as you know. As is often said, if it's Tuesday, somewhere there's an election. Well, it turns out that during today there is a pilot test of Microsoft's new ElectionGuard voting system. I had no expectation it was going to happen this quickly. And in fact, it's as a consequence of the concerns over voting security that this thing has just, like it fast-tracked itself into existence. So we've got some fun things to talk about there. We're also going to briefly touch on a little bit of SQRL news; some SpinRite news; and then, as I said, take a close look at two newly revealed Internet of Troubles security worries. So I think I can promise our listeners another great episode.

Leo: And a completely incomprehensible Picture of the Week.

Steve: Yes.

Leo: You're going to explain it to us.

Steve: Yes.

Leo: It'll all make sense when Steve is done. And that's actually kind of the motto of the show. It'll all make sense.

Steve: So I cannot really describe our Picture of the Week.

Leo: I can't, either.

Steve: And when it was sent to me, I thought, okay, wait a minute. You know how like sometimes photos are rotated 90 degrees. I thought, okay, wait. Is that the floor? Or is that the ceiling?

Leo: What the hell is this?

Steve: And then I saw like the drop ceiling with the bars, so I figured, okay, that's got to be the ceiling. So that means that's the wall that meets the ceiling. The clincher was down in the distance there's like an emergency battery backup lighting thing on the wall.

Leo: Yeah. So this is the upright wall. And coming out of the ceiling is a cable bundle and a track, a fairly hefty cable bundle. It looks like a monitor mount or something on the wall. But then what's this thing sticking out that has its own power supply and a plug just dropping down to the floor? Whatever it is, it's not pretty.

Steve: No, it's a catastrophe. So that black bracket that has been attached to the wall...

Leo: Yeah.

Steve: ...is a small, it looks like maybe, what, maybe like a 4U high 19-inch rack thing.

Leo: Oh, I get it. There was no room to put the rack unit in the rack.

Steve: Correct, because the rack that they had...

Leo: Was too shallow.

Steve: ...was too shallow. It looks like maybe eight inches deep or something.

Leo: Oh, I'm getting it now, yeah.

Steve: So some, dare I say "enterprising" techie thought, well, that's not a problem. And this must be a switch or, you know, it's some sort of an appliance, a network appliance.

Leo: It could be a UDP. There's all sorts of things it could be.

Steve: Well, it's got all of that networking plugged into it.

Leo: Right, right. Could be a switch, right, yeah.

Steve: And so, you know, yeah, it's got to be like a big switch. So whoever did this screwed it to the rack so that it's sticking out with no support out into the air. And then of course the power plugs into the back of it. So the power cord is hanging straight down in the walkway path. And I think this thing, this other beige thing must be a power outlet box because it looks like there's maybe something plugged into it. I mean, it just is like - anyway. So our topic, one of the things we're going to talk about is the dilemma that CISOs are in. And if a CISO did this, well, I guess they deserve whatever stress they're feeling because this looks like it's going to just...

Leo: This is just jerry-rigged. They put it in backwards. It's just crazy.

Steve: Really is bad.

Leo: That's hysterical.

Steve: So don't try this, not only at home, but at work.

Leo: Anywhere, especially at work.

Steve: Anywhere. Never do this.

Leo: I could see that in my house, but not at work, no.

Steve: Yeah. So, and we have had some pictures of wiring closets from hell in the past. So where, like, the network cables are used to hang socks that are drying and similar things.

So anyway, it turns out that the Windows 7 "You don't have permission to shut down Windows" is not restricted to Windows 7 after all. Windows 10 users have also been receiving the same permission denial. We have a picture of a Windows 10 dialog saying "You don't have permission to shut down and restart this computer."

Leo: Crazy.

Steve: So as are many weird things that only affect some subset of Windows users when they're triggered by a Windows Update, this also, this whole problem, this whole "You don't have permission to shut down Windows," whether it's hitting a Windows 7 user or a Windows 10 user, turns out to be a subtle interaction with some third-party software, which of course explains why it only affects a percentage of the population. In this case, the culprits are background services installed by Adobe's Creative Cloud.

Leo: Oh.

Steve: Yup, so it's only people who have Adobe's Creative Cloud that in some weird way collided with a Windows Update at the beginning of the year to cause a denial of permission to shut down and restart the computer.

Bleeping Computer provided some comprehensive coverage of the situation. They wrote: "Windows 10 users are reporting being affected by a bug that prevents them from shutting down their devices without logging out first, an issue that we previously" - we the industry - "thought only Windows 7 customers were experiencing. On February 6th, Windows 7 users started reporting encountering 'You don't have permission to shut down this computer.' Since then," they wrote, "this error has been reported by several Windows 10 users, too, one of them saying that he saw the error pop up on a recently installed device running Adobe Creative Cloud," as initially reported by some guy named Gnter Born.

Others also confirmed that the issue was impacting their Windows 10 Home edition devices, as well as multiple Windows 10 installations in an environment where Windows 7 devices were also experiencing shutdown issues, naturally because in that environment Adobe Creative Cloud had been installed both on Windows 7 and Windows 10 systems.

They wrote: "There are currently hundreds of user comments in Reddit threads, as well as on the Microsoft Answers forums and Twitter. While the shutdown issues aren't as widespread on Windows 10 as they are on 7, all reports point at the same error and the same underlying bug being behind the problems."

Then last Thursday, on February 13th, a Microsoft employee posted: "We've identified and resolved the issue, which was related to a recent Adobe Genuine update that impacted a small number of Windows 7 users. Adobe has fully rolled back the update automatically for all impacted customers. No action is needed by customers. If you're experiencing the issue, it will be resolved shortly via an automatic update from Adobe."

Leo: This kind of makes sense because it felt like something, some background process was blocking; right?

Steve: Yup, right, right. And then, finally, Bleeping Computer added: "While Adobe has already rolled back the update for Windows 7 customers, Windows 10 users are out of luck until the bug is also acknowledged for their platform and a fix is provided by either Adobe or Microsoft."

So it turns out that what Adobe - and I guess at some point Adobe will do that, but they hadn't as of when this most recent report was rolled out. However, Bleeping Computer said until then, you can disable - well, first of all, you can log out and then shut down, although that's kind of a pain. You can disable the Adobe services which are triggering the bug which, you know, go into Manage Windows into Services. You'll then find Adobe Genuine Monitor Service, Adobe Genuine Software Integrity Service, and Adobe Update. You could just halt those, stop them, disable them, whatever, and then later turn them back on after Adobe fixes the problem, or after you learn that it does.

In yet another problem, bizarrely, Windows 10 One Button PC Reset turns out to fail after this month's Patch Tuesday. The regular monthly rollup is KB4524244. And so it turns out - and, you know, this is not likely to affect lots of people. The Windows 10 One Button PC Reset, for those who have never encountered it, is a means, is something that's offered in Windows 10 which, if for some reason you want to just return your Windows 10 machine to factory settings, meaning a complete reset of the system, you know, there is like a Windows recovery partition compressed and hidden on a Windows 10 machine. And by jumping through some hoops, and you can get to it through menus,

I've had occasion to do it myself, you can get to this option that allows you to completely return your system to sort of like new condition.

It turns out that Microsoft introduced this problem by resolving a possible security vulnerability that might be introduced by third-party UEFI boot managers which as a side effect turned out to kill Windows 10 One Button PC Reset. Yes, Leo, I can hear you, and I feel the same way. It's like, this whole thing is just beginning to collapse under its own weight. So Microsoft has pulled that update and has no plans to reissue it.

As Microsoft explained it: "You might restart into recovery with 'Choose an option' at the top of the screen with various options, or you might restart to your desktop and receive the error 'There was a problem resetting your PC.' Anyone experiencing this problem is advised to simply remove the update from their affected Windows 10 machine." So again, they're like, you know, they rescinded it, but it's unlikely to affect that many people. If it does, you can remove that update.

But get this one. This one is causing some serious concern. Ever since this Patch Tuesday, some unlucky Windows 10 users, and I've not seen any forensics on this yet, they're reporting that another of the updates in the rollup is causing an additional problem that is very worrisome. According to reports, a bug in, in this case it's KB4532693, hides their user profile and all of their user data.

Leo: This is such a nasty one.

Steve: Yes. Because, I mean, you know, Microsoft is selling Windows 10, well, or pushing it, to people who are just, you know...

Leo: To normals, yeah.

Steve: Normals, yes, exactly. And so it's being reported on Microsoft Forums, Twitter, Reddit, tech sites including AskWoody, Bleeping Computer, and BornCity. Users are reporting that, after installing the standard monthly update rollup, they're just doing their normal, you know, Microsoft makes you do it now, so okay, fine, and it doesn't take that long for a regular monthly update. However, after doing this, they can no longer view or access their original Windows 10 profile. In other words, according to these reports, after the update users are left logged into a blank default Windows 10 profile where all of their previous data is missing.

Leo: That's scary. Now, it's not actually missing. You're just logged into the wrong profile.

Steve: Right. Well, it's not deleted, essentially.

Leo: Right.

Steve: Yeah. So all installed apps, desktop wallpapers, desktop files, downloads, you know, everything that, you know, for those who don't know, your whole profile is what makes you different from someone else logging into the same machine under their own

profile. The profile is your per-user account. So as you can imagine, it's quite unsettling to just update Windows, as you're told you should, and then all your stuff is gone.

Last Wednesday Woody Leonhard tweeted: "Multiple reports that the Feb Cumulative Update for Win10 resets the desktop - custom icons missing, background set to Windows logo - and would not recognize the established logon account." He asks, "Are you seeing the same?" And then sent a link where presumably people could respond. So as you said, Leo, the good news is nothing was permanently deleted. The data's not gone. It's only been hidden.

According to a report on Bleeping Computer, the bug is caused by a faulty, as I said, KB4532693 installation procedure. The bug occurs when the Windows Update service creates a temporary profile for use by the installation procedure, but then - whoops - forgets to remove it after finishing the update installation. When the update finishes, this temporary profile remains the one that users are logged into, and all their stuff is gone.

Reports indicate that the original user profile folders are still available on disk, but that they've been renamed with a .000 or a .bak extension. And while it's technically possible to recover these sequestered profiles by renaming and relinking them, the steps required are error prone. And as you said, Leo, this is, you know, many people are just normals. They're like, where did all my stuff go?

Leo: Oh, yeah. I've had calls like this, and it's terrifying for them.

Steve: Yes.

Leo: Because it's not clear it's not gone.

Steve: Right, exactly. Well, it looks gone. And it's like any normal person would go, all my stuff is gone.

Leo: Right.

Steve: So it turns out that the best solution is to uninstall the faulty update that's part of the rollup, KB4532693. Just uninstall it. Multiple users have reported that removing the faulty update restores their old profiles. So anyway, all that said, it's obvious that not all Windows 10 users are impacted by this bug. So, yes, most users will have no problems at all. Who knows what's going on? All of my Win10 machines are current with the February rollup, and I didn't see that happen to me. But it clearly is happening to many people.

So as we know, given the problems that Microsoft is now continually having every month, the advice would be don't immediately jump on one of these rollups. What that means is you may be planning to. The good news is, if this does happen to any of our listeners, everybody who hears this will know, okay, all is not lost. Nothing is lost. You can just uninstall this 4532693, and you'll get your stuff back. But, boy, Microsoft, I don't, I mean, yeah, I don't know how we explain the continuing problems that Windows is having.

Leaving them alone for a while, there is a very popular GDPR Cookie Consent WordPress plug-in which has a critical flaw. It's of some concern because more than 700,000 active

installations exist of this problem. So anybody who's listening, and if you know anybody who has a WordPress site, and you may know that they've got this GDPR Cookie Consent plugin installed, it needs to be updated to version 1.83 or later with high priority, due to a serious vulnerability.

As its name implies, it serves as an aid to making websites compliant with the EU's GDPR regulation. But since its February 10th update, it has also been critically, I'm sorry, until it was just updated on the 10th, so a little over a week ago, last Monday, a week ago Monday, until a week ago Monday, February 10th, it has been critically flawed in a fashion that, if exploited, could enable attackers to modify the site's content and inject malicious JavaScript into any of these 700,000 active installations.

I don't use it myself on my WordPress blog, so I wasn't able to verify whether this has automatic update technology as part of it. So what I would recommend, any of our listeners, if your WordPress site uses this GDPR Cookie Consent plugin, make sure that it is at 1.83 or later. After the developer was notified of the critical flaw by the people who found it, the plugin was removed from the WordPress.org plugin directory, saying "pending a full review," according to the plugins directory page. And now the new version, 1.83, was released by the plugin's developer Cookie Law Info, as I said, Monday before last.

The vulnerability stems from improper access controls in an endpoint used by the WordPress plugin's AJAX API. AJAX, for those who don't know, is the acronym for a technology which allows JavaScript running on a page to independently initiate its own outbound HTTP and other connections for retrieving data for use by that JavaScript. For example, I use it myself on the SQRL login page. That's what creates that magic where, without even touching the login page, after you authenticate with your smartphone, the login page that is there, that is present, spontaneously updates to show that you're logged in.

What's happening is that there's a so-called AJAX query running on that page in the background which is periodically pinging the site's server that you're logging into for a new URL for the page to jump to. AJAX scripting cannot ask for anything from anywhere, thank goodness, or we'd be in real trouble. It's constrained by same-origin rules, so it can only request additional information from a site that meets the same-origin restrictions, typically just the site that provided the page. So it's just sort of like it allows sophisticated actions. It's behind the scenes of many of the web applications that we've now grown to take for granted.

But in this case this plugin has a method "_construct" which is used by initializing code in the plugin for creating new objects. It constructs the objects. And unfortunately, this fails to implement required security checks. Because of this, that AJAX endpoint, which is only intended to be accessible to administrators, is allowing visitors to the blog to perform a number of actions that can compromise the site's security. It accepts three different values from the AJAX API.

Two of them, one of them is "save_contentdata" and the other is "autosave_contant_data," turns out can be leveraged for exploitation by an attacker. The mistakenly accessible save_contentdata allows admins to save the GDPR cookie notices to the database. However, since the method is not checked for authentication, any visitor to the site can also modify any existing page or post, meaning most of the website. And as is so often the case with HTTP, it's possible to delete or change the page's content. Injecting content then allows reformatting of text, local or remote images to be obtained, as well as hyperlinks, shortcodes. You could embed a frame that then pulls content from somewhere else and get up to all kinds of high jinks.

And then that second problem, the autosave content data, is used to save the GDPR cookie info page in the background while the admin is editing it. And it turns out it saves it into a sensitive database field, skipping any validation checks. And again, this opens it for abuse. So not surprisingly, the researchers who discovered it urge WordPress plugin users to update immediately. And it was that language that concerned me that this might not have an auto update mechanism. I may have some additional news on that by next week from people who do have it and have some experience with it. But 700,000 WordPress sites is not nothing. And this allows lots of at least defacement of WordPress blogs and probably much more malicious modification. So make sure if you're using that that you get it updated.

So it turns out the average tenure of a CISO, a C-level Information Security Officer, like a CEO and CFO and so forth, is just 26 months.

Leo: Wow.

Steve: Due to high stress and burnout.

Leo: Yup.

Steve: It turns out that the vast majority of interviewed CISO executives, 88% of the 800 that were interviewed report high levels of stress. One third report stress-caused physical health issues, and half report mental health issues. We've touched on this in the past. Information security, cybersecurity, is still a relatively new thing. It's still seen as more of a necessary evil by corporations than as an obvious profit center, like sales, marketing, or R&D. Not to mention the fact that the high priests of information security appear to speak in a strange language that makes no sense to any of the other C-suite executives who are the ones, after all, who establish the budgets and the schedules.

So as a consequence, most companies are still not ready to truly embed CISOs into their company culture and into their day-to-day operations. They're sort of like, you know, it's like that guy who hangs out in the wire closet. So today CISO jobs come with low budgets, long working hours, a lack of power on executive boards, a diminishing pool of trained professionals that they're able to hire, and a constant stress of not having done enough to secure the company's infrastructure against cyberattacks. There's also continuous pressure due to new arising threats. I mean, look at what we talk about every week. This stuff is real, you know, like oh my god, you'd better not have Remote Desktop Protocol exposed. And if you do, it's real trouble.

It's funny, as I was thinking about this and looking at and reading over this report, it really struck me that this is like the problem with asymmetric warfare. You know? It's not like the British lining up in a row in very brightly colored uniforms with their muskets and like, okay, now we're going to - when we say "go," both sides are going to charge each other. You know? This is asymmetric. This is bad guys all over the world trying to pry their way in through a nook and cranny.

And I'm glad I don't have responsibility for a large organization, as I've, you know, back when we were talking about the Sony hack, Leo, I said very clearly I don't think it's possible to secure an organization like that. So imagine having the responsibility for the security of a major firm on one's shoulders. I just - I can't imagine it. So anyway, it turns out that through the years CISOs have often pointed out the problems with their jobs and the stress and damage that those jobs inflict upon them and their families. But

there's been no conclusive study up until now to support what were essentially these broad assertions.

Last November Nominet, they're an Internet and DNS security firm that we've talked about before, the name's familiar to me, I forgot exactly what their product is, but N-O-M-I-N-E-T, they independently surveyed 800 CISOs and executives from companies in the U.S. and the U.K. to explore and examine this topic and to determine how much of a role stress plays for CISOs across the industry. The survey's results painted a gloomy picture about one of today's most in-demand jobs. I mean, it's no longer the case that a company can go without somebody whose job is to focus on the security of the company's Internet and networking infrastructure.

So what the report found, I have a link to the entire report in the show notes. I think I do. I don't see it here. Oh, yeah, back at the top of this topic is there. So what the report showed, 88% of CISOs reported being between moderately to tremendously stressed. Eighty-eight percent. Nearly half, 48%, said that work stress has had a detrimental impact on their mental health. Forty percent of CISOs said that their stress levels had affected their relationships with their partners or their children. Thirty-two percent, essentially one in three, said that their job stress levels had repercussions on their marriage or romantic relationships. The same, 32%, said that their stress levels had affected their personal friendships. Twenty-three percent of CISOs said that they had turned to medication or alcohol as a means of dealing with the stress from their job.

Nominet, who prepared the report, said that even when they are not at work, many CISOs feel unable to switch off. As a result, CISOs reported missing family birthdays, holidays, weddings, and even funerals. The report said they are also not taking their annual leave, their sick days, or time for doctors' appointments, which contributes to physical and mental health problems because of course, if you never feel like you have enough time in the day to get the work done that you need to get done, you're going to keep pushing those things off. Nominet said that while investigating the cause of CISO stress, they found that almost all CISOs were working well beyond their contracted hours by an average of 10 hours of extra time per week, for which they were not compensated.

Furthermore, many were under pressure from their boards. Almost a quarter of those interviewed said that boards didn't accept or understand that breaches are inevitable. So what we know of that is, because we've often talked about this, that there's a culture clash. There's those who don't get it, and the CISO who does get it. He's not making excuses. He or she is trying to explain this. So the board said they don't understand that breaches are inevitable, and the CISOs reported that the boards would be holding them personally accountable for any security incidents. So you can imagine how that affects stress levels.

Nominet said that 29% of CISOs who answered the survey said they'd be fired in the event of a breach, while 20% said they'd be fired anyway, even if they were not responsible. So the answers explain why most CISOs don't last in their jobs more than an average of 26 months, and why 90% of those surveyed were willing to take pay cuts if they could reduce stress levels. Nominet said CISOs were willing to give up, on average - and the reason this is a weird number is that it's an average of the responses - on average, $9,642 per year, so almost 10K per year, on average, just to reduce stress levels and improve their work-life balance, which many CISOs said they had problems with.

Nominet's numbers may seem staggering to someone looking in from the outside, but of course they come as no surprise to anyone working in the field who realizes what a mess this is right now. Although the Nominet study only surveyed high-ranking CISO executive jobs, the problem is widespread across the industry. Infosec, or cybersecurity, has a habit of grinding through employees due to the rigors of the job. They said low-level

infosec positions like threat analysts or pen testers, penetration testers, are just as bad in terms of stress, if not worse, primarily for the same reasons - a constant fear of new incoming attacks, long work hours, low pay, and very little job satisfaction.

So I realize I'm not doing a lot to sell everyone here on the glories of being in charge of Internet security for your organization.

Within the infosec community, signs of the growing problem of stress and burnout leading to mental health issues have been mounting. There are some efforts underway to raise awareness about infosec job stress levels - like this report - burnout, along with the mental health issues arising from ignoring this problem. There has also been a rise of so-called "Mental Health Hackers," an online community that's been attending cybersecurity conferences on a regular basis now in order to help raise awareness of the topic, that it's a real thing.

And I don't see any obvious solution to the dilemma, other than time, frankly. The problem ultimately is one of respect. It's impossible for other C-level executives to respect what they do not understand. Traditionally, as we know, nerds and geeks have enjoyed sort of keeping their dark arts a secret. But being understood is vastly more valuable than being mysterious. So part of the job should be to explain and train other C-level execs so they can better understand what the job is all about. And of course, fortunately, time and additional experience with the realities of cybercrime are going, regardless, to slowly bring about a cultural attitude change.

We know that that's in process now. When you have, like, last year's massive, widespread, in the popular press coverage of ransomware attacks, there's no way that C-level board executives are not perforce becoming more aware that this is something happening. And so, yeah, when it happens to them, they realize it's not an isolated incident. There is an aggressive pressure for this to happen. So unfortunately, as we also know, this sort of change takes time.

So I guess my advice to CISOs would be to as much as possible try not to carry the entire organization's cybersecurity responsibility on your own shoulders. I'm sure that's easier said than done, but try. And also try to retain a sense of perspective as much as possible. In the end, it is just a job, and your life is yours. Try not to give it away. So yikes. I mean, it's nice to see a report like that, that helps to put some numbers to a problem that we sort of say, oh, yeah, boy, being in charge of security is stressful. Well, yeah. It's really stressful.

One thing that's helping to take some stress out is Microsoft's ElectionGuard, which as I mentioned at the top of the show, this being a Tuesday, is being used for the first time today. As the saying goes, if it's Tuesday in the U.S., there's an election somewhere. And in this case that somewhere is the small town of Fulton, Wisconsin. What's making history there today is that the residents of Fulton, Wisconsin will be electing representatives for the Wisconsin Supreme Court using voting machines for the first time powered by Microsoft's ElectionGuard software. These are the first voting machines deployed in any U.S. election that will be running Microsoft's new voting software, which we've been keeping an eye on on the podcast since the summer.

Recall that ElectionGuard is a fully open SDK that Microsoft has made available at no charge on GitHub: github.com/microsoft/electionguard. The project's goal is to create voting software that uses strong encryption, actually massively cool encryption. It's built by some of the world's top cryptographers. And it allows it to be, thanks to being open source, extensively audited for bugs. I was very surprised when I saw this news because it was just in May of last year, 2019, that Microsoft announced the existence of this for the first time. They then first demonstrated their prototype voting machines to a small audience of the Aspen Security Forum last July. Then they released the first

ElectionGuard code to GitHub in September, and opened a bug bounty program the following month, last October.

Today's pilot test is deliberately small, expected to have only a few hundred voters casting ballots. But this will provide voting machine vendors, as well as quite anxious U.S. election officials, with a real-world test of the software to see whether it's worth a shot and ready for wider deployment. Before today's event, Tom Burt, who's Microsoft's VP for Customer Security and Trust, thus in charge of this, said that using ElectionGuard won't be complicated, since Microsoft designed the software from the ground up for ease of use, accessibility, and with a user-friendly interface. He explained that the voting experience is a three-step process.

First, a voter will select candidates on a touchscreen and verify their choices. Then the voter will print and review for accuracy a paper ballot and simultaneously receive a separate tracking code. Finally, the voter deposits their ballot into a ballot box for counting. And presumably this is an electronically scannable paper ballot. But as we've described, there's a lot of wonderful, quite advanced crypto technology happening behind the scenes. After casting their ballot, each voter receives that tracking code. They are able to use that tracking code on an election website to verify that their vote has been counted and that the vote has not been altered. In other words, that tracking code lets them see their votes. The tracking code, however, does not reveal the vote, so it won't allow third parties to see who voted for whom.

ElectionGuard employs a homomorphic encryption scheme which was developed in-house at Microsoft under the watchful eye of senior cryptographer Josh Benaloh. Counterintuitive though it is, this homomorphic - I have a hard time pronouncing that - homomorphic form of encryption allows the counting of individual votes while never decrypting them. They stay encrypted, yet they can still be counted. What? Yeah. The ElectionGuard SDK also supports third-party verifier apps which are able to independently check that the encrypted votes have been counted properly and have not been altered. The verifier apps were created for use by voting officials, the media, or any third party interested in the voting process and in adding their own verification to it. And ElectionGuard machines can also produce, as in today's case, paper ballots as a printed record of their vote, which voters can then place inside traditional voting boxes, just like old-fashioned ballots. And, finally, ElectionGuard supports voting through open accessibility hardware. Apparently Microsoft has some Xbox-based controllers that are able to be used.

Leo: Are you joking, or are you serious?

Steve: No, I'm serious. They're Xbox-based controllers, yeah.

Leo: It's not running on Windows; is it?

Steve: I don't know what it...

Leo: It can't be open source. It can't be.

Steve: Well, it could be open source running on...

Leo: On top of Windows. Yeah.

Steve: Yeah, exactly. I mean, given Microsoft. So the voting machines being deployed today in Fulton were built by VotingWorks at Voting.Works. And Leo, if you go there, you will like what you see. Their home page is exactly what we would want to see. It states: "Democracy is a choice. VotingWorks is a nonpartisan nonprofit, building a secure, affordable, and," they said, "delightful voting system." It's delightful. "Our voting machine creates paper ballots that voters can directly verify. Our risk-limiting audit software" - which of course is based on what Microsoft has done - "ensures votes cast on any paper-based system will be correctly tabulated. Our source code is available on GitHub. You can help by making a tax-deductible donation or joining our team."

And VotingWorks is not alone. Other voting machine vendors including Smartmatic and Clear Ballot have also announced partnerships with Microsoft to build ElectionGuard-based voting machines; and a fourth group, Dominion Voting Systems, is also exploring the use of Microsoft's SDK. I think this is a perfect storm outcome since, once officials see how this works, what it means for the systems to be open and auditable, and all of the new features that this system offers, no one who isn't doing this will continue being viable. This makes the welcome and long-overdue end to proprietary closed voting machines, I think, just a given.

And good riddance to, you know, I want to say Diebold or Diebold, and Diebold is welcome to produce ElectionGuard-based machines of their own. But they are going to have a hard time, I think, in the future selling anything that doesn't use this software. We need this, I mean, this has to be the way it's being done moving forward. So, you know, big, big bravo to Microsoft for doing this, putting it out there, giving it away, making it open. And to all those companies that have jumped on it and said, hey, we see the writing on the wall. We need to support this, or we're not going to be able to sell our stuff in the future. So yay. Isn't that cool?

Leo: Yeah. It uses TypeScript. I'm guessing it might not require Windows, though. Might be able to run it on something else because it looks like it's all web technologies.

Steve: Nice.

Leo: Yeah, [crosstalk] Python.

Steve: If it's secure, nice.

Leo: Yeah.

Steve: Very cool.

Leo: Yeah.

Steve: I did want to note that we've added an implementation for SQRL. To the growing list of SQRL implementations we now add a general purpose pure PHP implementation for, I guess it's Laravel, the PHP framework, L-A-R-A...

Leo: Yeah, Laravel, yeah.

Steve: Laravel. So there is now a pure PHP SQRL implementation for Laravel. It's up on GitHub, and I have in the show notes a link to it, and also a thread over in the GRC forums.

I am at work on SpinRite. I have no, of course, it's going to be a while before I have any deliverables. I've just rebuilt the FreeDOS kernel. Back when I stopped working on SpinRite, I had had to tweak the FreeDOS kernel a little bit because FreeDOS just assumes that when it boots up, all of the drives that it sees, it's going to be able to understand. Well, it doesn't understand the GUI, you know, the GUID partition format. It only understands the older MBR format.

And of course one of SpinRite's next features will be the ability to operate on any drives. What happens then is that FreeDOS tries to essentially log onto all the drives it sees, and it freaks out in a very ungraceful manner. So I had previously implemented a new config.sys option, skip init. You just put skipinit=1 in the config.sys for DOS, and it no longer tries to initialize all the drives. I found out that it was a little tricky to rebuild FreeDOS because one of the things I lost is compatibility with 16 bits when I went to a 64-bit Windows, unlike my old XP machine that was still able to run 16-bit code. I've overcome that hurdle and just actually before the podcast I rebuilt the FreeDOS kernel.

Anyway, we're moving forward, and I will keep our listeners updated. There is a page which the people who are participating over in GRC's newsgroups know about. I'm not ready to make it widely public because it'll just generate too much traffic and too many questions at this point. And I need to keep running everything through GRC's newsgroups and not have Greg and Sue submerged in how do I do this and how do I do that questions anyway. But if anyone is interested in participating, there is an active discussion now underway over at the grc.spinrite.dev newsgroup. And you can figure out how to get there by going to GRC.com/discussions. That's the page that explains about our newsgroups.

I actually revved my favorite newsreader for Windows. It turns out it broke at the beginning of 2020. Gravity was first written in the late 1990s. But it is my absolute favorite newsreader. Back then they added a sanity check for any headers in incoming postings, deciding that if they appeared to be older than 2020, then they must be bogus. So of course, well, sort of a variation on the Y2K problem; right? So starting January 1st, date sorting of threading broke. And so the good news is Gravity was released to the open source community, and I'm now maintaining a fork of Gravity that adds that and a number of other features that I have felt were missing for years. And so there's news of that over at GRC.com/discussions for anyone who's interested. So lots of fun stuff happening.

So it turns out that IoT light bulb vulnerabilities are not such a joke after all. Our listeners know that I often joke about having our internal networks hacked and attacked by something as ridiculous-seeming as a light bulb. I chose light bulbs, I guess, to receive that abuse over the general lack of attention to IoT security because they're pretty much the dumbest, lowest rung of the ladder and the least fancy IoT device we have. Well, it turns out that the extremely popular Philips IoT light bulbs, the Philips Hue IoT light bulbs, or in this case actually the bridge that's part of the Philips Hue system,

rather than the light bulbs themselves, are able to, in combination, expose our internal WiFi networks to bad guys.

The Hacker News had some good coverage of this. They explained, well, they began by saying: "There are over a hundred potential ways hackers could ruin your life by having access to your WiFi network that's also connected to your computers, smartphones, and other smart devices." Right, we don't want bad guys on our WiFi network.

They said: "Whether it's about exploiting operating system and software vulnerabilities or manipulating network traffic, every attack relies on the reachability between an attacker and the targeted devices. In recent years," they wrote, "we've seen how hundreds of widely used, smart-but-insecure devices made it easier for remote attackers to sneak into connected networks without breaking WiFi passwords.

"In the latest research shared with The Hacker News, Check Point revealed a new, high-severity vulnerability affecting Philips Hue Smart Light Bulbs that can be exploited over the air from over 100 meters away to gain entry into a targeted WiFi network. The underlying high-severity vulnerability, which is tracked as CVE-2020-6007, resides in the way Philips implemented the Zigbee communication protocol in its smart light bulb. This leads to a heap-based buffer overflow." Whoops.

So, okay. As we know, Zigbee is the widely used mesh wireless technology that allows each device in a Zigbee group to communicate with any other device on that network. And it's widely used. It's the protocol built into tens of millions of devices worldwide, the Amazon device, the home hub device. I'm reluctant to say the name because I don't want to set them off. Samsung's SmartThings, the Belkin Wemo, and many more. Lots of devices use Zigbee.

The Check Point researchers said: "Through this exploitation, a threat actor can infiltrate a home or office's computer network over the air, spreading ransomware or spyware, by using nothing but a laptop and an antenna from over 100 meters away." They also confirmed that the buffer overflow happens on a component called the "bridge" which is the module that receives remote commands sent to the bulb over the Zigbee protocol from other devices like a mobile app or the Amazon home assistant. Due to its severity, that is, the severity of this problem that Check Point found, they have not revealed any technical details, nor are they providing any proof of concept for the flaw, in order to give users some time to apply patches.

But we have a blog from Check Point. Of course they couldn't resist saying "The Dark Side of Smart Lighting" as the title for this. They wrote: "With the help of the Checkpoint Institute for Information Security (CPIIS) at Tel Aviv University, the researchers were able to take control of a Hue light bulb on a target network and install malicious firmware on it. From that point, they used the light bulb as a platform to take over the bulbs' control bridge, and attacked the target network."

So they said, first, the attacker controls the bulb's color or brightness to trick users into thinking the bulb has a glitch. The bulb appears as "Unreachable" in the user's control app, so they try to reset it. The only way to reset the bulb is to delete it from the app, then instruct the control bridge to rediscover the bulb. Apparently it's that action of the rediscovery that allows the bulb to then attack the bridge which has just rediscovered it.

They wrote: "The bridge discovers the compromised bulb, and the user adds it back onto their network. The hacker-controlled bulb with updated firmware then uses the Zigbee protocol to trigger a heap-based buffer overflow on the control bridge by sending a large amount of data to it. This data enables the hacker to install their own malware onto the bridge, which is in turn connected to the target business or home network." Malware then connects back to the hacker and, using a known exploit like EternalBlue or whatever,

they're able to infiltrate the target IP network from the bridge to spread ransomware or spyware.

So this is a classic get in and then pivot attack. So the bad guys take control of the light bulb, install their malign firmware onto it, make the light bulb go crazy so that its owner thinks, what the hell, it's gone nuts. The owner deletes the bulb, re-adds the bulb to the system, and in that repairing process the bulb is able to infiltrate the shared hub, get its malware then onto the hub. And the hub is now in a privileged position, being part of the WiFi network, in order to exploit the internal network from its vantage point. And as I'm reading this, I'm thinking, wow, you know, all this from somebody who wants to have Philips Hue smart light bulbs and control them using wireless technology.

This research was first disclosed to Philips and Signify, who is the owner of the Philips Hue brand, last November, so a few months ago. Signify confirmed the existence of the vulnerability in their product, and after about two months they issued a patched firmware version. So anybody who has Philips Hue bulbs are going to want to take note of this. You want to make sure this is the firmware you're using. It ends in 4040, that's the easy way to - it's Firmware 1935144040.

Leo: And they do over-the-air updates. So the chances are you already do have it. You don't have to do anything.

Steve: Yes, exactly. I was curious about that, so I wanted to make sure that that was done. And there is meethue.com. Check Point said: "In a joint decision with Signify, we decided to postpone the release of the full technical details of our research in order to allow Philips Hue clients to have enough time to safely update their products to the latest version. The full technical details of this research will only be published in our research blog in the upcoming weeks. Stay tuned."

So anyway, I was curious to know, as you said, Leo, if there is auto update, to verify that. There apparently are two bridges. There's a Version 1 bridge, which is a rounded shaped bridge, well, they said round-shaped bridge, and a Version 2 which is a square-shaped bridge. And that's the one that supports the Apple HomeKit. And they wrote on their page, if you don't want to miss any improvements on quality, security, or performance, and you want your Hue system fully compatible with the upcoming new Hue products, please be sure that you enable automatic updates for your Hue system in the Hue app. That's under Settings > Software Update > Automatic Update. And I presume that's the default setting, right, Leo?

Leo: Actually, I should check. That's what we've been saying, but I should check just to make sure.

Steve: Yeah. And on January 13th of 2020, so last month, almost a month ago, they said Firmware 1935144040 for the Version 2 bridge, they said: "We regularly update your Hue bridge to improve the performance and reliability of the system."

Leo: My bridge is up to date, and I didn't do anything. So yes.

Steve: Good. This update includes a patch for a security vulnerability in the Hue Bridge v2.

Leo: Make sure, it says, all your lights are powered on to get them up to date. It can take up to one hour per light or accessory to download, and lights may briefly turn off while updating.

Steve: Wow, well, that's cool.

Leo: What world we live in, huh?

Steve: I know. Can you believe it, Leo? It's like, okay, turn on the lights and wait an hour. And I'm not surprised because it's going to be a slow - it's a low-power, bandwidth-constrained protocol. And they're having to receive a firmware update through Zigbee. So it's going to take a while.

Leo: Yeah.

Steve: But I'm glad to know that the light bulb itself, not just the bridge, can be updated. That's a question I had, and I'm glad you answered it for us.

Leo: And the weird thing is this was a problem earlier. They didn't patch it correctly, apparently, and so it came back.

Steve: Whoopsie.

Leo: Yeah. But, yeah, you should automatically be updated. And if you for some reason turned off auto updates, well, you might want to turn those back on.

Steve: Yeah. And so the big takeaway here, and this perfectly factors into our next topic, our final discussion, the so-called "Sweyntooth vulnerabilities" which have just been disclosed, the utter importance that anything you have that which is IoT has an upgrade path. I mean, I know that I always say this. There's typically some reason to bring it up every single week. But it is crucial that we have that.

So Sweyntooth. The Sweyntooth vulnerabilities are a set of more than 12 newly discovered and disclosed, and notice I said "more than 12," across a wide range of Bluetooth devices. Unfortunately, many of which will never be updated.

Leo: [Sigh]

Steve: I know. More than 480 individual products have been identified that are affected by this. These allow for, among other things, full device compromise. Only 12 of these vulnerabilities have been disclosed so far since some Bluetooth vendors - as you might guess from Sweyntooth, this is about Bluetooth - some Bluetooth vendors have not yet released updated SDKs, so more disclosures will be forthcoming.

But let's back up a bit. First of all, I know everyone is thinking, Sweyntooth? The etymology of Sweyntooth is not as immediately obvious as are many other named

vulnerabilities. In this case, Sweyntooth was formed from the names of Sweyn Forkbeard and his father, King Harald Bluetooth.

Leo: Yeah. King Harald was the Bluetooth, yeah. So it's Bluetooth's son.

Steve: Turns out that King Harald Bluetooth, of course, being the namesake of our widely used Bluetooth technology, he was exiled by his upstart son, Sweyn.

Leo: Don't you know.

Steve: Who revolted against his father, exiled King Harald, and shortly thereafter the king died.

Leo: Oh, no.

Steve: So, yes. Sweyntooth. The discoverers of these vulnerabilities wrote that they "envision that if Sweyntooth-style vulnerabilities are not appropriately handled by BLE vendors, then the technology can become a breeding ground for attackers, which may in turn lead the Bluetooth technology to become obsolete." I doubt that Bluetooth is going to become obsolete, but this is going to be a serious problem. Their paper, "Sweyntooth: Unleashing Mayhem Over Bluetooth..."

Leo: Oh, geez. Oh, no. Mayhem? Oh, man.

Steve: I love that. I love the word. "Mayhem" is one of my favorite words. Mayhem. That's just such a great word. "Unleashing Mayhem Over Bluetooth Low Energy." I've got a link to the disclosures that are posted on GitHub, a link to their 11-page PDF, which is a partial disclosure because they still have not heard from some of the Bluetooth vendors. They start off their paper explaining.

"Sweyntooth captures a family of 12 vulnerabilities - more under nondisclosure - across different BLE software development kits of seven major system-on-a-chip (SoC) vendors. The vulnerabilities expose flaws in specific BLE SoC implementations that allow an attacker within radio range to trigger deadlocks, crashes, and buffer overflows, or completely bypass security, Bluetooth security, depending upon the circumstances. Sweyntooth potentially affects IoT products in appliances such as smart homes, wearables, and environmental tracking or sensing."

They said: "We have also identified several medical and logistics products that could be affected." There was one from Medtronics that I saw. "As of today," they wrote, "Sweyntooth vulnerabilities are found in the BLE SDKs sold by major SoC vendors." So when I was reading this, I was hoping that these were going to be kind of obscure, never really heard about them, don't know who they are so not a big deal. Unh-unh. TI.

Leo: Oh.

Steve: NXP that of course used to be Philips, Cypress, Dialog Semi, Microchip, STMicroelectronics, and Telink Semiconductor, all major suppliers of Bluetooth SoC system-on-a-chip devices. "By no means is this list of SoC vendors exhaustive," they wrote, "in terms of being affected by Sweyntooth. We have followed responsive disclosure during our discovery, which allowed almost all SoC vendors to publicly release their respective patches already. However, a substantial number of IoT products relying on the affected SoCs for BLE connectivity will still need to independently receive patches from their respective vendors, as long as a firmware update mechanism is supported by the vendor.

"Sweyntooth highlights concrete flaws in the Bluetooth Low Energy stack certification process. We envision substantial amendments to the BLE stack certification to avoid Sweyntooth-style security flaws in the future. We also urge SoC vendors and IoT product manufacturers to be aware of such security issues and to initiate focused effort in security testing. A proper classification of the vulnerability set is presented in the next section."

And I'll mention briefly they've got Crash, where vulnerabilities in this category can remotely crash a device by triggering hard faults. They said: "This happens due to some incorrect code behavior or memory corruption, for example, when a buffer overflow or Bluetooth Low Energy reception buffer occurs. When a device crash occurs, they usually restart. However, such a restart capability depends on whether a correct hard fault handling mechanism was implemented in the product that uses the vulnerable BLE SoC."

Second classification, Deadlock. Deadlocks are vulnerabilities that affect the availability of the Bluetooth Low Energy connection without causing a hard fault or memory corruption. Usually they occur due to some improper synchronization between user code and the SDK firmware distributed by the system-on-a-chip vendor, leaving the user code being stuck at some point. Crashes originated from hard faults, if not properly handled, can become a deadlock if the device is not automatically restarted. In most cases when a deadlock occurs, the user is required to manually power off and power on the device to reestablish proper communication. In other words, a deadlock kills the Bluetooth Low Energy device without the user interceding and shutting it down and powering it back up again, which of course still leaves it prone to re-attack.

And, finally, Security Bypass: This vulnerability is the most critical one, they wrote. This is because the vulnerability allows attackers in radio range to bypass the latest secure pairing mode of Bluetooth Low Energy, i.e., the Secure Connections pairing mode. After the bypass is completed, an attacker within radio range has arbitrary read-and-write access to the device's functions, functions which are only intended to be accessed by authorized users. So yes. A complete bypass of BLE Bluetooth security, essentially by forcing a pairing of a malicious device with the Bluetooth device.

This led to a raft of CVEs - yup, all 12 of them are there - affecting different of the devices in different ways. They have in their report a table of vulnerabilities and SDK versions of the affected system-on-a-chip devices. And they're listed, I'm looking at Cypress, at TI, at STMicro, at NXP, at Texas Instruments, Microchip, I mean, they're all there.

So the problem we face here is the nature of the Bluetooth consumer device chain. We're talking about the suppliers of the original silicon way at the start of the chain. They have the silicon. They provide a software development kit where the engineers who are then customizing the system on a chip, integrating it into their solution, are using the Bluetooth software stack that was provided by the system on a chip vendor, the BLE vendor, which ended up being - it gets burned into the firmware of the product. Which is to say that every single Bluetooth device from these companies has these vulnerabilities.

And the sad truth of today's supply chain is most of these will never be updated. By far and away, most Bluetooth-enabled devices are not our mainstream smartphones.

And, for example, Home Hubs or the Philips Hue Hub and bulbs, which I'm glad to find out were updated, they're not - most Bluetooth-enabled devices are not part of an active ecosystem. And notice that you have to have some way of talking to the device. I mean, our smartphones and our home hubs and things like the Bluetooth, well, those are tied into WiFi, which are tied into the Internet, that gives them a means of getting themselves updated. But we've got Bluetooth stuff all over the place which doesn't have a means of getting connected to the Internet. Most of them will never see a firmware update. And even if one was available on some, what, Chinese website vendor or retailer somewhere, how would we the user ever know that it was even there?

So imagine some random Bluetooth Low Energy-based corporate or residential alarm system that was purchased through Amazon from typically these days a Chinese vendor that used a Bluetooth Low Energy chip from Cypress, TI, NXP, Microchip or apparently any of the other still not even named vendors. We know that original manufacturer doesn't care about after-sales support. You bought it. It was cheap. Good luck. No after-sales support is even offered. So that alarm system is now highly unlikely to ever receive a firmware update. It works, yes. But it will also be forever vulnerable - "forever" is the key word - forever vulnerable to wireless proximity attacks that will eventually be made fully public.

And in the specific case of an alarm system, it doesn't need to be vulnerable to the least common of those attacks, which was the full security bypass. It might be sufficient for an attacking burglar's purpose to create a deadlock so that it is unable to sound the alarm. But if a security bypass can be found, even more damage could probably be done. And we've all seen science fiction where, for example, as with Neo at the start of "The Matrix," some lesser skilled individuals are purchasing some advanced hacking technology from him, a more highly skilled hacker. I've always regarded this sort of world as more fanciful than real, that is, the idea that anything, anything can be hacked for a price.

But it's becoming increasingly clear that the way things are going, the fundamentally insecure way that we are now cavalierly and casually purchasing, deploying, using, and relying upon technology can be hacked and, in cases like this, will be forever known to be hackable. This really does suggest that a brave new world where anything could be hacked for a price.

You know, imagine the phone rings, and the hacker says, "Hey, what's up? Oh. You want to bypass a Chimera 412 home alarm system? Sure. Piece of cake. Those use the old Cypress 2313 BLE chip that its manufacturer never updated. The hack for that's been around forever. But mine has a few extra touches. Transfer one-tenth of a bitcoin to my wallet, and once it's there I'll shoot you a script that you can run on any rooted Android smartphone that'll completely and silently shut down any Chimera 412."

Leo: You don't think that's happening?

Steve: Probably is in some places. Probably already is. You're right.

Leo: I don't think it's that farfetched, really.

Steve: You know?

Leo: There's money out there.

Steve: That's the world we are in, yes. The knowledge is there. Hackers are there. We know that there's an underground world. We now have a means of transferring funds in a way that is essentially untraceable.

Leo: I mean, I think most hackers are honorable, believe it or not. But I think that we've heard that organized crime has started using hackers for hire. I wouldn't be surprised. I mean, all it would take is a small percentage of the total hacking community to be a problem.

Steve: Well, and my point is it's not just big things like RDP servers that we could even, you know, we're able to count those. You can't even count the number of Bluetooth Low Energy devices that are now floating around the world being used, and which are now known to be vulnerable and are never going to be updated.

Leo: That's right.

Steve: Wow. This podcast is going to get more interesting.

Leo: I don't see how it can. We are doing a little party. I can make it more interesting if you're going to be at the RSA Conference in a couple of weeks. Our sponsors, the namers of our beautiful studio, LastPass, are having, as they have in years past, they're having an event at this great place called Bourbon & Branch in San Francisco. It's a speakeasy, and you have to know the password to get in, you know. And it's not "swordfish." And you get in, and there's secret rooms and stuff, and great drinks. And we would love to see you there. I'll be there, Lisa'll be there, a lot of our staff will be at Bourbon & Branch at the speakeasy. It's February 26th, so eight days from today, a week from tomorrow, at 7:00 p.m. I can't tell you what the secret password is. I don't know it. But if you RSVP, it will be sent to you under secret cover.

Steve: Ah.

Leo: Go to twit.to/rsalastpass20. That's the URL shortener we use, twit.to. Twit.to/rsalastpass20. But only if you can be there. You know, some number of people are going to just say, I just want to know what the password is. It's not that interesting, trust me. It's, you know, it's going to be simple. But if you can be at the party, we'd love to have you. Open bar and everything. February 26th, 7:00 p.m., Bourbon & Branch in San Francisco, if you're going to be at RSA. I wonder what's going on in the long run with RSA because, you know, IBM Platinum Sponsor dropped out. I'm just curious. I guess everybody's watching COVID-19 to see, well, is it going to get worse, or is it going to get better?

Steve: Yeah. And you guys were talking about that recently. I think you're right about this really putting a chill on...

Leo: Conferences.

Steve: ...on physical attendance at conferences.

Leo: Shut down Mobile World Congress pretty good.

Steve: And we know that Apple just announced that they've got a profitability problem, said they can't get their stuff out of China now.

Leo: That's right. But so far RSA is still going strong. And if you're going, I would love to see you on the 26th. Steve, thank you so much. Steve's home on the 'Net, GRC.com, the Gibson Research Corporation. That's where you'll find all the stuff that he does, including SpinRite, the world's best hard drive and maintenance utility, now being updated as we speak. You can also find lots of free stuff, including this show, 16Kb audio for the bandwidth-impaired, 64Kb audio for those of you who like the rich stereo experience. We also have, he has carefully written transcripts so you can read along as you listen. That's GRC.com.

Steve's on the Twitter at @SGgrc, if you have a question or a comment. He accepts DMs. And of course you should follow him to see what he's up to. We have copies of the show, audio and video, too, at the website, TWiT.tv/sn. And of course you can get it on demand anytime, just go to that website. We do the show Tuesdays, 1:30 Pacific, 4:30 Eastern, 21:30 UTC. So you can also watch us stream it live for the unexpurgated version, that's at TWiT.tv/live, both audio and video there.

And of course the best thing to do, it would help us a lot if you would subscribe in your favorite podcast application. That just sends them a signal that people like this show. Maybe they'll feature it. It helps us. So subscribe, and that way it'll help you, too. You'll get a copy of it the minute it's available of a Tuesday evening.

Steve, that concludes this thrilling, gripping edition of Security Now!. We'll see you next time.

Steve: Ciao.

Leo: Ciao.