
# THAT "PASSKEYS" THING

**Description:** This week we look at a patch to Android to thwart an actively exploited vulnerability. We briefly revisit Connecticut's new privacy law, and we take a quick look at the raft of recent ransomware victims. The U.S. State Department has added another ransomware group to its big bounty list, and we look at what's being called the biggest cybersecurity threat facing the U.S. Meanwhile, the White House issues a memorandum about the threat from quantum computing, and we have the discovery of a new and pernicious DNS vulnerability that's unlikely to be fixed in our IoT devices. And after looking at F5 Networks' new and quite serious troubles, we close the loop with some listener feedback, briefly discuss the past week of sci-fi news, then finish by looking at the past week's most tweeted-to-me question: "What's that passkeys thing that Apple, Google, and Microsoft are adopting?"

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-870.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-870-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got a patch for another Android zero-day actively exploited vulnerability. We'll find out why President Biden says, "Yikes, quantum computing." And we'll find out what this new FIDO initiative with Apple, Google, and Microsoft means. Is it more secure? Stay tuned. Security Now! is next.

**Leo Laporte:** This is Security Now! with Steve Gibson, Episode 870, recorded Tuesday, May 10th, 2022: That Passkeys Thing.

It's time for Security Now!, the show where we cover your security, your privacy, your safety, how computers work, anything else Steve wants to talk about including science fiction. Here he is, ladies and gentlemen, Steve Gibson. Hi, Steve.

**Steve Gibson:** And we will have a little sci-fi segue since, if you did see it, as you said you were going to last night...

**Leo:** I did. We can talk about it, yes.

**Steve:** We will talk about that. And today's main topic is a topic close to my heart. I titled it "That Passkeys Thing" after the big announcement of what was World Password Day, it turns out, was not only that but Cinco de Mayo.

**Leo:** Really.

**Steve:** Yes. And this is sort of a non-announcement announcement. I mean, it was okay. And in fact, because as you and I were talking before we began recording, I sort of have a dog in this hunt because I spent seven years of my life designing a solution which FIDO is still working to solve. I thought, well, I didn't want to get myself involved. But it was the most tweeted thing of the past week.

**Leo:** Well, yeah.

**Steve:** So I thought, well, okay. And if I hadn't invested seven years in designing SQRL...

**Leo:** You're an expert.

**Steve:** ...obviously I'd be talking about this.

**Leo:** Right.

**Steve:** So I shouldn't allow that to dissuade me from doing so.

**Leo:** Well, and you're an informed source. I was saying on MacBreak Weekly earlier I really hope Steve fills us in on this.

**Steve:** Yeah. So we're going to look at a patch to Android to thwart an actively exploited vulnerability. We briefly revisit Connecticut's new privacy law. And we take a quick look at the raft of recent ransomware victims - not in depth, I just kind of want to just say look at what's happening. The U.S. State Department has added another ransomware group to its big bounty list. And we look at what's being called the biggest cybersecurity threat facing the United States. Meanwhile, the White House issues a memorandum about the threat from quantum computing, and we had the discovery of a new and pernicious DNS vulnerability that's unlikely to be fixed in our IoT devices.

And after looking at F5 Networks' new and quite serious troubles, we'll close the loop with some listener feedback, briefly discuss, or maybe not so briefly because I think you and I will have some things to talk about, the past week of sci-fi news. Then we're going to finish by looking at the past week's most tweeted-to-me question, what's that passkeys thing that Apple, Google, and Microsoft are adopting?

**Leo:** The new FIDO Alliance thing, yeah.

**Steve:** The new FIDO Alliance thing.

**Leo:** I can't wait.

**Steve:** We do have a wonderful Picture of the Week thanks to somebody who knows that I appreciate what we would call physical humor.

**Leo:** It's quite the head scratcher.

**Steve:** It is.

**Leo:** And now, the Picture of the Week, Steve.

**Steve:** So this is a puzzler. For those who are not "seeing" the podcast or haven't seen the show notes, what we have is a roadway and a large wide sidewalk stretching across sort of a gorge. And on the sidewalk, like to the side, is a bridge which is sort of the bridge to nowhere. It goes up, and then it goes down. But you don't have to take the bridge because it just parallels the walking path. And Leo, while you were telling us about Zentry, I was thinking maybe this is of historical significance. This roadway and pedestrian way, it feels like from what we can see on the left like it's bridging some gorge or a river or something. Maybe once upon a time that little walkway was like down below, going across the river. And they thought, well...

**Leo:** Let's just save it, yeah.

**Steve:** For historical reasons, yeah.

**Leo:** Or maybe for the view. It gives you a better view of the hole. That may be it. I don't know. If that were the case you'd put it closer to the edge, though, wouldn't you.

**Steve:** It's not clear from any of the context of the photo where this is. I can't tell, like, what country it's in. But our listeners have quite a reach. So I'm calling to our listeners. You may know. You may have walked past this bridge and thought to yourself, what?

**Leo:** What the heck? It looks like, on these road signs, looks like there might be Chinese.

**Steve:** Yeah, there are, like, distant road signs in the background. So if anyone knows what this is, where it is, why it is, it would be interesting to find out. And I will certainly share that with our - oh, you can almost read that, yeah.

**Leo:** Almost see it. It's either blurry or Chinese. I can't tell.

**Steve:** Anyway, so I love the caption that came with this. I tweaked it a little bit. So here we have this bridge, right, that just, it doesn't really do anything. You don't have to go up it. You could if you want. But you're just going to get back to where you were. Anyway, so the caption reads, for our audience, I mean, for this topic: "When you don't

know what that code does, but you assume it must be important, so you just leave it alone."

**Leo:** Yeah. Don't take it out, yeah.

**Steve:** You know, like you might be afraid to remove this bridge, Leo, because it serves a mysterious purpose like, as you said, gazing into the hole from a better altitude.

**Leo:** You'll find out, for sure.

**Steve:** Yeah. So better just maybe give it a little bit of leeway and just say, well, okay, fine, we're not going to - you could change your mind. Today I'll take the bridge; tomorrow I won't. Either way, you end up at the same place. Anyway, thank you to our listener who said, "Okay, Gibson, you're going to like this one."

Google updated Android to patch an actively exploited vulnerability, not for the first time. This was just their monthly security patch release. It fixed 37 flaws across various components. One of them is a fix for an actively exploited Linux kernel vulnerability that came to light earlier this year. It was a little odd that it took them as long as it did. That vulnerability is CVE-2021, that's last year's CVE number, 22600. It has a CVSS of 7.8, ranked as "high severity" because it could be exploited by a local user to escalate privileges or deny service.

And as we know, especially in the Android ecosystem, where it's not that difficult for malware to be running on your phone, right, I mean, like people download this crap from the Google Play Store all the time, saying, oh, look, it's going to improve your cell phone service and squeeze your memory down to give you more memory. And when you're not looking, it's going to polish your shoes. And someone says, hey, sounds like a good idea. I want some of that. And so they download it. Well, the app is constrained by Linux's security rings; right? Unless the app knows about this CVSS 7.8 high-severity exploit, which allows it to escalate its privileges to root and root around in your phone.

So the flaw was a double free vulnerability residing in the packet network protocol implementation in a Linux kernel. And, you know, it's kernel-wide, so not really just Android. It could cause memory corruption, potentially leading to at least denial of service or, if you're a clever hacker, execution of arbitrary code. And as I said, it wasn't just Android that was vulnerable. Patches were released by various Linux distros including Debian, Red Hat, SUSE, and Ubuntu, back in late 2021, in December, and also early 2022 in January. And it's unclear why Google didn't patch this one sooner. Maybe they just figured, well, as far as we know it's not being used. So anyway, now it is, and so now they did. They said: "There are indications that CVE-2021-22600 may be under limited targeted exploitation."

So last month the vulnerability was added to CISA's Known Exploited Vulnerabilities Catalog due to evidence of its active exploitation in the wild. Google also patched three other bugs in the kernel, as well as 18 other high-severity and also one critical-severity flaw which was in the MediaTek and Qualcomm components. So, you know, update. Actually a couple stories today we're going to have some fun with this issue of updating because, come on, folks.

Okay. Connecticut's recently passed data privacy bill became law last Wednesday. I talked about it last Tuesday. I was incorrect in stating last week that Connecticut's Governor Ned Lamont would need to sign the recently passed legislation for it to become

law. That's normally the way it works. It turns out that the state, Connecticut, has a rule that bills which have passed in the state assembly become law automatically five days after they're passed when during a legislative session. So that seems like an expeditious thing to have. We ought to all have one of those.

So consequently, Connecticut now joins California, Virginia, Colorado, and Utah to become the fifth state to create its own privacy law in lieu, and because the federal government isn't doing anything about this. And there has been a specific reaffirmation that once that law has ramped up to full strength, that Global Privacy Control signal that we talked about last week, which will now, or soon, be sent by browsers, must be honored, and specifically without exception and without any further "are you sure" style prompting by anyone with whom Connecticut residents interact online. So the point being that no one gets hassled with this like you are now with cookies. If you're sending that GPC signal, the browser cannot by law challenge you about that.

**Leo:** Yay.

**Steve:** It just has to say, okay, darn, and go with it.

**Leo:** By the way, web4849 in our chat room has discovered the location of this bridge to nowhere. It is in Korea, the Dongan Bridge. And in Seongnam City, and apparently is intended to not go anywhere. When walking along the 72-meter-long bridge, passersby can choose to walk straight on or, if they "had a little more strength in their legs or a little more time," they could opt to cross over an overpass to get from one end to the other. You could also observe from it the Pangyo Techno Park park.

**Steve:** Leo, you got it. It's an observation point. And when they call it an "overpass," we should note that it's not passing over anything.

**Leo:** Nothing. It's the sidewalk. Yeah, apparently well known in Korea. And thank you to one of our chatters, web4849.

**Steve:** Fantastic.

**Leo:** Who took seconds, mere seconds.

**Steve:** I love the reach of our listeners. Let me think of other things I don't know, and we could...

**Leo:** Yes, exactly.

**Steve:** We could ask some other questions. Okay. I promise not to dwell at length, ad infinitum, on ransomware attacks. But my concern is that in honoring that promise to the letter, we're downplaying it. So I decided, okay, from time to time I'm just going to kind of give people a sense for it. So, for example, Trinidad's largest supermarket chain was crippled by an attack. The German library service is struggling to recover from a

ransomware attack. A major German wind farm operator confirms a cybersecurity incident, which was ransomware. Austin Peay State University in the U.S. was hit with ransomware. The ADA, that is our American Dental Association, confirmed a cyberattack after a ransomware group claimed credit. Coca-Cola is investigating claims of a hack after a ransomware group was offering their stolen data for sale. Whoops.

Conti ransomware has deeply crippled the systems of the electricity manager in a Costa Rican town, and the newly elected President of Costa Rica has since declared a state of emergency as a consequence. The agricultural equipment maker AGCO has reported a ransomware attack. A cyberattack has taken down the network at the State Bar of Georgia. And classes have resumed at Michigan Community College after a ransomware attack, and classes at Kellogg Community College will be resuming tomorrow after two days of outages caused by a ransomware attack. In Battle Creek, Michigan nearly 7,000 students were told last Monday, May 2nd, that ransomware had crippled its systems the previous Friday, April 29th. The school was forced to shut down its main campus in Battle Creek as well as branches in Coldwater, Albion, and Hastings. So there's your...

**Leo:** Good lord.

**Steve:** ...snippet.

**Leo:** What it tells you is it's so commonplace now that it's not worthy of note; right?

**Steve:** Yes, it's just like, it's bad and doesn't seem to be getting any better. But so I just wanted to sort of like put a little punctuation on this, that because I'm not talking about it, it doesn't mean it isn't happening.

**Leo:** Oh, no.

**Steve:** And that this isn't like a really big problem. And which leads us to our next story, the U.S. State Department offering a $10 million reward for information about Conti members. The U.S. State Department has begun offering $10 million rewards - plural, so it's not just a first-come, first-serve, there'll be a line - for any information leading to the identification or location of people connected to the Conti ransomware gang. And in addition, you can get an additional $5 million reward if any information you provide does lead to the arrest or conviction of a Conti member. So a total of $15 million to anyone who can turn in a member of the Conti gang.

And, you know, this is U.S. dollars, 15 million of them. You've got to think that this would make anybody associated with Conti quite uncomfortable. There must be others outside of the immediate gang who are not themselves criminals so they don't face prosecution, but to whom members of Conti have bragged about, like, just over drinks or - I keep trying to say "pillow talk," but no.

So in a statement on Friday, State Department spokesman Ned Price told us something we already know, that Conti has been behind hundreds of ransomware attacks over the last several years. He said: "The FBI estimates that as of January 2022, there had been over 1,000 victims of attacks associated with Conti ransomware with victim payouts exceeding $150,000,000, making the Conti ransomware variant the costliest strain of ransomware ever documented."

The memo also notes that the group has recently claimed credit for that wide-ranging ransomware attack that targeted the government of Costa Rica as it was transitioning to a new president. The attack crippled the country's customs and taxes platforms alongside several other government agencies. And as I noted before, the attack also brought down one Costa Rican town's energy supplier.

Conti also attacked, as we documented at the time, Ireland's Health Service Executive a year ago, back in May of 2021, which resulted in weeks of disruption at the country's hospitals. Ireland refused to pay the $20 million ransom and now estimates it may end up spending $100 million recovering from the attack. Although as I recall, Leo, I think that was the one where they were like going to get all new computers as a result. So it was like...

**Leo:** Yeah, nice.

**Steve:** Maybe they're milking their insurance company a little harder than they...

**Leo:** Who gets the old computers? That's what I want to know.

**Steve:** The group similarly crippled dozens of hospitals in New Zealand, and the group has made a point of targeting U.S. healthcare and first responder networks - they're not nice, oh, and they're Russian, by the way - including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year, so says the FBI.

The group has suffered a number of internal breaches over the years, the most notable of which occurred a few months ago, in February, after it expressed public support for Russia's, no surprise, invasion of Ukraine. Within a few days of the message, the gang's internal Jabber, you know, XMPP server, which carried their private messaging channel, was hacked, and two years of the group's chat logs appeared on a new Twitter handle called @ContiLeaks. The leaks revealed the group's inner workings and illustrated the way they chose their targets. However, those leaks did nothing to slow the group down. Last Wednesday they added New York-based architecture firm EYP to their list of victims.

So Conti now joins the ranks of those carrying a serious bounty on their heads. Last November, the U.S. State Department offered a $10 million reward for any information that would lead to the identification and/or arrest of members of the DarkSide ransomware group with a similar bounty on the operators behind REvil, also the Sodinokibi malware. So this is an interesting tactic that I have to imagine it would be effective. U.S. dollars are valued globally still, fortunately. And again, if nothing else, you have to imagine that this would weigh on the minds of anyone choosing to participate. If they get in, they've got to be very circumspect within their own social sphere because here's the U.S. dangling $10 million just for turning you in. And that's real money.

**Leo:** So frustrating. One of our chatters just sent me a link to a Bleeping Computer article about a college in Illinois, Lincoln College, one of the historically black colleges in rural Illinois, closing after 157 years. It survived a major fire in 1912, the Spanish flu, the Great Depression, two World Wars, the 2008 global financial crisis. But after two years of pandemic and finally getting hit by ransomware they decided to shut down after 157 years.

**Steve:** Wow.

**Leo:** That is horrific and tragic. Just tragic. A cyberattack in December that thwarted admission activities, hindered access to all institutional data, creating an unclear picture of fall enrollment, this fall enrollment. And so they're shutting down.

**Steve:** Wow. Wow. Well, and we've covered when the ransomware was attacking the healthcare industry, it was clearly damaging the lives of people. People were being hurt by the healthcare providers being offline.

**Leo:** So, so sad. Now they're going after schools.

**Steve:** Yup. Yup. Okay. So what's the worst threat the U.S. faces? It's from the Winnti Group, W-I-N-N-T-I, the Winnti Group, also known as APT 41. APT, of course, is Advanced Persistent Threat.

Just how advanced and persistent are these threat actors? Researchers with Cybereason recently briefed the FBI and the DoJ about Operation "CuckooBees" funny name, not a funny operation. This is an ongoing espionage effort by Chinese state-sponsored hackers with the charter to steal proprietary information from dozens of global defense, energy, biotech, aerospace, and pharmaceutical companies. The specific individual organizations affected were not named in Cybereason's report, but they allegedly include some of the largest companies in North America, Europe, and Asia. And the threat actor behind it all is the prolific Winnti Group, also known as APT 41.

Cybereason's CEO Lior Div said that the most alarming aspect of the investigation into Operation CuckooBees was the evasive and sophisticated measures used to hide inside the networks of dozens of the largest global manufacturing companies in North America, Europe, and Asia, dating as far back as 2019. Lior said: "The group operates like a guided missile; and once it locks onto its target, it attacks and doesn't stop until it steals a company's crown jewels. Winnti pilfered thousands of gigabytes of data and, to add insult to injury, also made off with proprietary information on business units, customer and partner data, employee emails, and other personal information for use in blackmail or extortion schemes at a time of their choosing."

Cybereason said that throughout its 12-month investigation, it found the intruders took troves of intellectual property and sensitive proprietary data including formulas, source code, R&D documents, and blueprints, as well as diagrams of fighter jets, helicopters, missiles and more. And remember, China. The attackers also gained information that could be leveraged for use in future related cyberattacks, like details about a company's business units, network architecture, user accounts and credentials, employee emails, and customer data. This group gets in your network, you're hosed, basically.

And of greatest concern, according to Cybereason's CEO, was that the companies had no clue they had been breached. In a pair of detailed reports, Cybereason attributes the attacks to Winnti based on an analysis of the digital artifacts the group left behind after its intrusions. Several other cybersecurity companies have also been tracking Winnti since it first emerged 12 years ago in 2010, and researchers have observed that the hackers are clearly operating on behalf of Chinese state interests while specializing in cyberespionage and intellectual property theft.

The group used a previously unknown and undocumented malware strain called DEPLOYLOG, as well as new versions of malware like Spyder Loader, PRIVATELOG, and

WINNKIT. The malware included digitally signed, kernel-level rootkits, as well as an elaborate multistage infection chain that enabled the operation to remain undetected. The group also managed to abuse the Windows Common Log File System (CLFS), which allowed the intruders to conceal their payloads and evade detection by traditional security products. CLFS is a logging framework that was first introduced by Microsoft in Windows Server 2003 R2 and has been included in all subsequent Windows OSes.

Cybereason explained that: "The attackers implemented a delicate 'house of cards' approach" - that was their term - "meaning that each component depends on the others to execute properly, making it very difficult to analyze each component separately." And unsurprisingly, "Operation CuckooBees" generally took advantage of existing weaknesses including unpatched systems.

**Leo:** [Grunting]

**Steve:** I know.

**Leo:** [Grunting]

**Steve:** Yes, thank you. Insufficient network segmentation, unmanaged assets, forgotten accounts, and lack of multifactor authentications. In other words, stupid oversights.

**Leo:** Yeah. Easily remedied. Easily.

**Steve:** Yes, exactly. Cybereason said that the attackers generally obtained their initial foothold in the organizations through vulnerabilities in Enterprise Resource Planning (ERP) platforms. Last month, FBI's director Christopher Wray told "60 Minutes" that the "biggest" threat American law enforcement officials face is from Chinese hackers stealing proprietary information. He said that the FBI opens a new China counterintelligence investigation about every 12 hours.

**Leo:** Oh, my god.

**Steve:** Think about that. Every 12 hours another new Chinese counterintelligence investigation is opened by the FBI. Wray said that: "They are targeting our innovation, our trade secrets, our intellectual property on a scale that's unprecedented in history. They have a bigger hacking program than that of every other major nation combined."

**Leo:** Wow.

**Steve:** "They have stolen more of Americans' personal and corporate data than every other nation combined. It affects everything from agriculture to aviation to high tech to healthcare, pretty much every sector of our economy. Anything that makes an industry tick, they target."

**Leo:** There is a difference, though, between this and the ransomware gangs we were talking about earlier, which are actually trying to steal from companies and bring them to their knees. This sounds like it's intellectual property theft.

**Steve:** Yes.

**Leo:** That the Chinese hackers aren't trying to destroy us or destroy our industry. They're just trying to find out how we make things so they can make them cheaper, things like that. And admittedly there's an economic consequence to that. But that's not nearly as offensive as the Conti Group; right? Or am I wrong?

**Steve:** Well, when you're digging into our military industrial complex.

**Leo:** Well, if they go after the military, you're right, that's different because then that has...

**Steve:** And they're in there.

**Leo:** Yeah.

**Steve:** That's where they're going.

**Leo:** But if the military's getting hacked because they haven't patched and they're not using two-factor, we have other reasons to be upset.

**Steve:** And Leo, we have other reasons to be upset.

**Leo:** Yes. And we're going to get upset about something else in a minute, I'm sure.

**Steve:** We are.

**Leo:** All right. I'm ready to talk about quantum computing. And in fact for a long time I've been wanting to ask you how - see, I look at this, and to me it looks like Google and everybody, it's just a way to get money from the feds. Like they aren't really - are we close?

**Steve:** No, no. Okay. So this one made me shake my head.

**Leo:** Okay.

**Steve:** The headline was "White House wants nation to prepare for cryptography-breaking quantum computers." Okay. To give everyone a sense for this, the reporting on

this which appeared in The Record started out saying: "A memorandum issued Wednesday by President Joe Biden orders federal agencies to ramp up preparations for the day when quantum computers are capable of breaking the public key cryptography currently used to secure digital systems around the world. The document, National Security Memorandum 10" - so of course we have to have initials, right, NSM-10 - "calls for 'a whole-of-government and whole-of-society strategy'"...

**Leo:** Oh, let me get right on that. Whoa.

**Steve:** Yeah, huh? "...for Quantum Information Science (QIS), including 'the security enhancements provided by quantum-resistant cryptography.'" Uh-huh.

**Leo:** Well, that's one reason I switched from RSA to, what is it, ESCD 50,000, whatever it is? The elliptic curve? I don't know what I'm doing. But that's why I changed my SSH keys; right?

**Steve:** Right. Well, so...

**Leo:** Is that more quantum resistant?

**Steve:** I was looking at this, and I was thinking, okay, why don't we just cure cancer? And then I thought, oh, wait. That was what Biden was going to do while he was...

**Leo:** Oh, we already did it. Oh, good.

**Steve:** ...Barack's VP. We going to take that, do that. How'd that work out? But seriously, okay.

**Leo:** I did Ed25519. Right? That's the keys I should use; right?

**Steve:** Yes.

**Leo:** Okay.

**Steve:** So he's ordering the federal government to ramp up preparations for a day when quantum computers are capable of breaking public key cryptography which, by the way, doesn't yet exist. The federal government...

**Leo:** Right. And we don't know when it will exist; right?

**Steve:** No, no.

**Leo:** It's like fusion energy. Someday.

**Steve:** Well, actually that's in the notes, Leo, yes. The federal government is apparently unable to update its own software when being handed patches to do so.

**Leo:** That might be more important.

**Steve:** Someone somewhere says, eh, not today. We haven't yet secured our computers for technology we already have against attackers we already have. So I don't know. How about having the White House use a memorandum ordering the various agencies in the federal government to please just reboot their computers.

**Leo:** Even that would be a step forward.

**Steve:** How would that be? You know? We would actually get more security right now today if we did that. And to your point, yes, sure. Quantum computing technology shows promise. But let's remember that it's been showing promise for quite some time. We've had nascent quantum computing technology since around the late 1970s, so for more than four decades. It's intriguing and interesting. And it's been moving forward gradually. You know, like most really big problems do, and like fusion power, exactly like that. And the federal government should absolutely be funding ongoing research in universities to allow our nation's brightest young minds to continue pushing this frontier forward. There's clearly something tantalizingly possible there. And I agree that we should not forget that we have adversaries. As we know, China is also working hard on this problem. So Leo, if we patch and reboot our computers, we might be able to keep them from stealing it once we figure it out.

**Leo:** Wow. Wow.

**Steve:** But yes. It absolutely is the case that at some point in the future - I think right now the most I saw was four cubits we were able to deal with. I kind of have a hazy sense that I saw something about more. But, I mean, it doesn't scale linearly. Like if you get four, you can't simply say, oh, let's use 128 of those to get 512. No. They can't do that. So we are so far away from, like, this actually being a threat. So I just scratch my head. It's like Joe Biden is issuing a memorandum telling us to scale up our preparedness, when we cannot reboot our servers?

**Leo:** It's not a bad idea by itself, but it's not maybe the first thing we should do. IBM says they've got a 127-cubit device.

**Steve:** Ah, that may be what it was that I remember.

**Leo:** Yeah. IBM's selling these now. $1.60 per runtime second on their 27-cubit Falcon r5 processor. I mean, so maybe, maybe. Maybe it's happening. I don't know. I don't know what you could do with 27 cubits.

**Steve:** No. Basically you can absolutely simultaneously solve a symmetric crypto that uses an 8-bit key, I think, is what it comes down to.

**Leo:** Okay. So we've got to get to more than a thousand cubits before we're in trouble.

**Steve:** Yes. We've got to get way...

**Leo:** Am I right saying that if I did Ed25519 that...

**Steve:** Yes. The technologies which do - so the concern is that the one thing which has been protecting us, the RSA crypto, is that we don't know how to factor big numbers.

**Leo:** Right.

**Steve:** So the concern is a quantum computer could theoretically kill the factorization barrier.

**Leo:** Right.

**Steve:** I mean, that was the trapdoor that you could only go through one way. And the worry is that a quantum computer could just go, oh, you want to factor that? Here. I mean, like it doesn't even take any time. Just say here.

**Leo:** Here.

**Steve:** You know? It's like...

**Leo:** Here's the factors.

**Steve:** So we're wanting to get away from a crypto that is based on the multiplication of two primes that you're then unable to factor. Well, elliptic curve crypto is that.

**Leo:** Oh, good. Okay.

**Steve:** So you've got enough bits of elliptic curve crypto, and we're not worrying about factorization any longer.

**Leo:** I think I'm doing 512. No, 500 - it's weird, it's 521 bits for some reason. I don't know what that means. But like I said, I just put in the formula, that's all.

**Steve:** That's good. Okay. And that's what's so easy about this.

**Leo:** Yeah.

**Steve:** And this has been the point I'm making. We have all the tools. All the toolkits are there. All the work has been done. The academic guys have pounded on it, and they've said, "Here you go." And so all it takes now is just plugging these in and using them correctly. And unfortunately, well, and not making any bad mistakes, which continues to dog us.

Okay. As I've often said, I am stunned by the elegance and fundamental simplicity of the Internet's design. It was so beautifully conceived in the beginning. But as we know, it's not without a few blemishes. One of the original sins of the Internet's early design was, and still is, a lack of entropy in some fields which are critically important. This entropy is crucially necessary for robust attack resistance.

And in defense of the Internet's early designers, the last thing they were thinking about while they were trying to get this whole thing to go was about active and aggressive adversaries. They were trying to keep coincidental things from causing a problem, which is very different from preventing an active aggressor from leveraging their design to create mischief. That wasn't on their map at all. So they designed and built beautiful technology which has, against all odds, withstood decades of explosive growth being put to use in applications they could never have and didn't ever imagine.

But we've got a few problems. For example, the endpoints of a TCP connection are identified only by an IP address and a port number. And the progress of the connection's data flow is tracked by a 32-bit sequence number. In the early days of this podcast we examined how the predictability of the sequence numbers being issued by TCP/IP software stacks could be weaponized and used by attackers to splice into existing TCP connections. Since nothing identified the other endpoint other than its source IP address and source port, TCP packets carrying spoofed source IP and source port, and guessing a sequence number that would be expected by the receiving endpoint could and did back then succeed in injecting malicious traffic into established TCP connections.

Another quite famous lack of entropy may, and often does, exist in DNS queries. Being UDP, the spoofing task is much easier. If a DNS client emits a query to a DNS server having a knowable IP address, and if the 16-bit source port of its query and the 16-bit transaction ID are predictable, it's not difficult for an adversary to jam a bogus DNS reply back into that client which looks identical to the reply it's expecting to receive from the authentic DNS server. And as we know, this form of DNS cache poisoning spoofing attack can have devastating consequences. The IP being looked up will be altered, and traffic will be silently redirected.

It was the realization of that which hit Dan Kaminsky back in 2008, when nearly all DNS servers in the world were vulnerable to exactly that attack because their queries had very low effective entropy. That caused the world to secretly prepare and then synchronize a simultaneous global update of all affected DNS servers. It was a great example of global coordination.

But we missed something, something that today afflicts many IoT devices, such as routers by Linksys, Netgear, and those loaded with OpenWRT firmware, as well as Linux distributions like Embedded Gentoo. This exposes many millions of IoT devices, right now today, once again, to this once-solved security threat. What we missed, or at least weren't worrying about 14 years ago, was that it's not only DNS servers and our desktop operating systems which emit DNS queries. They were all fixed. But many other low-end

IoT-ish devices also emit DNS queries, and we forgot about them. Maybe it wasn't a big problem or concern back then. But the crucial fact is, the lesson of the need to deeply randomize source port and transaction query IDs for DNS was not learned well enough.

Nozomi Networks Labs discovered a vulnerability, now being tracked as CVE-2022-30295, which affects the DNS implementation of all versions of uClibc and uClibc-ng which are very popular C standard library replacements used in many IoT products. The C standard library is this big library which is very capable, highly cross-platform. You can compile it just for about anything. But it's huge. And it does way more than a little IoT product with tight memory constraints needs. And for example it supports memory mapping, which embedded IoT, there's a uC Linux that specifically doesn't have memory management because a little embedded product isn't swapping stuff in and out of RAM. So this uClibc and uClibc-ng are what embedded Linuxes use. The flaw, which was found and fixed in all major DNS servers back in 2008, is the predictability of transaction IDs in the DNS requests generated by the library.

In the show notes I have a picture of the code from uClibc where we can see a variable local_id++;. Well, that's a post-increment operation. And since you're doing nothing but that on that particular instruction, it simply increments the value of local_id. The next line reads local_id and then &=, with 0xffff. Okay, so that masks and retains the lower 16 bits of the value local_id.

So essentially what it does is local_id is incremented, and that AND operation, then the logical AND of the lower 16 bits deals with the overflow when it tries to go to a 17th bit. It discards that. So we wrap from 65535 back around to zero because those transaction IDs are 16-bits long. In other words, what this does of course is produce absolutely sequential DNS query transaction IDs. The problem that took the wind and the breath out of the entire network world 14 years ago is present in this library, and apparently has been since its beginning.

While I was doing a bit of background research into this uClibc, I found that the original pre-forked uClibc's last update was May 15th of 2012, so 10 years ago exactly this coming Sunday. Because this library had become unsupported, it was forked to create uClibc-ng. Presumably "ng" stands for next generation. The good news is that one's being actively maintained. But under its home page's History section, talking about the history of uClibc-ng, it explains: "uClibc-ng is a spin-off of uClibc from Erik Andersen," and then from http://www.uclibc.org. "Our main goal is to provide regularly" - which in their write-up was misspelled - "a stable and tested release to make embedded system developers happy.

"The first release 1.0.0, with the code name Leffe Blonde, was made while visiting FOSDEM 2015. It was prepared in a hotel room in Brussels on the first of February, 2015. All releases are prepared while drinking a pair of Belgian beer since then." Because you know, Leo, that's what you want in the replacement for the Standard C library that everyone's embedded IoT devices are using is for it to be maintained by a drunken Belgian. "The idea to fork uClibc started in July 2014," they wrote, "and was discussed on the Buildroot and OpenWRT mailing lists."

Okay. So we've identified a well-understood flaw that has been present in embedded Linux-based IoT devices which use the uClibc library or the uClibc-ng library for the past decade or so. Apparently no one thought to look before now. Now the world knows. I'm pretty sure that the OpenWRT folks will get on this and fix it because that's who they are. The fix, after all, is trivial. The transaction ID sequence simply needs to be unpredictable. And it needs to be unpredictable per instance of that device booting; right? You can't just like make a pseudo, like a fixed pseudorandom sequence because anyone can reverse engineer the firmware, see what the sequence is, and then go back to predictability.

An embedded device without a good source of local entropy, which a really low-end IoT electric plug, for example, might have, or might lack a good local source, could, as it's starting up, use something like high-resolution packet timings to obtain an unpredictable seed. Send out some pings to some known static IPs and time their return at the device's full-resolution clock speed. That will generate a value that's unknowable by any external attackers. I'd then use that value to key a simple symmetric cipher which encrypts a sequential counter. That will produce a per power-up, per boot unpredictable sequence that no one on the outside can know.

What we don't know is everywhere this embedded library has been used in embedded Linux systems. We don't know whether Netgear and Linux, which both use it, will care to update. And most importantly, where and how this flaw will surface in the future. But the bad guys will make it their business to know because that knowledge is valuable to them. And this is the legacy we're building which most worries me, the growing number of well-known problems that are accruing, mostly under the radar, and which are not being diligently fixed. These things don't go away on their own. They accumulate.

What's happening over time and mark my words is that one of the favorite vehicles of fiction writers, which is that anything can be hacked, offensive as I have always found that idea, is gradually becoming true. Anything can be hacked. And this is another perfect example of the way it's going to happen, little by little and bit by bit. A problem like this that just doesn't really rise to the level of an oh, my god, run around, house on fire like we saw with the DNS servers.

But the same problem is in all the other little things that are making DNS queries and that could easily have their query poisoned by somebody who wanted to do that. That would relocate whatever traffic they were looking at to an attacker-controlled IP rather than where it should be going. And lord knows, then, what mischief they can get up to. And you can't even count the hundreds of millions of devices running an embedded Linux that probably use this now known to be defective uClibc library. Well, we're not going to be running out of things to talk about, Leo. That's clear.

F5 Networks Remote RCE. So here's another example of a serious vulnerability that's far more high profile and should get the attention of anyone using F5 Networks' so-called BIG-IP equipment. They've had problems before. We've talked about them before. But both we and the bad guys already know that patching is badly broken, and that there will be F5 BIG-IP equipment online which remains unpatched. Remember that list of ransomware victims from earlier? This is exactly where attacks such as those begin.

Last Wednesday on May 4th, F5, a major cloud security and application delivery network provider, released patches to repair 43 bugs spanning its products. Of the 43 issues they addressed, one is rated critical, this one; 17 are rated high; 24 medium; and one is rated low in severity. But that critical one, oh, baby. It carries a CVSS of 9.8, which arises from a lack of an authentication check which will allow attackers to take control of an affected system. As we're seeing more often now, the flaw took only a few days to reverse engineer, and a working proof of concept has been made public.

So the use of terms such as "might," "may," or "could" in F5's bureaucratically worded disclosure should be replaced with "will," "did," and "have." They wrote: "This vulnerability may allow an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands, create or delete files, or disable services."

Uh-huh. And this security vulnerability appears to be longstanding since it affects all six most recent major version release chains, v11 through v16. It doesn't appear that they'll be patching the oldest two major versions 11 and 12 since patches for the iControl REST authentication bypass flaw have been released for versions 17.0.0, 16.1.2.2, 15.1.5.1,

14.1.4.6, and 13.1.5, leaving the 12 whatever and 11 whatever vulnerable but unpatched.

So we can expect CISA to soon add an alert and a mandatory update commandment for this to their growing catalog of Known Exploited Vulnerabilities. And in fact they just added five more to that catalog, three for which patches were made available in 2014, one in 2019, and another last year. Yet all five are now under active exploitation even eight years, in the case of those three that were patched in 2014, after having been patched. So, wow. We need to patch and reboot.

Okay. A couple pieces of Closing the Loop feedback from our listeners. Someone whose name on Twitter is Lets Burninate, he said - yeah. Let's Burninate. "Hi, Steve. Long-time listener." He said: "I just wanted to share this image when I tried to change my PayPal password and was shocked by this error message for obvious reasons." And it is kind of entertaining. So this is, you know, I'm an avid PayPal user. They're a great solution for the problem that they're there to solve. So this is the Change Your Password dialog. And first they want you to confirm your current password. That's good. And he's done that. Then it says "Enter your new password. Keep your account more secure. Don't use your name."

**Leo:** Good thinking.

**Steve:** Yeah. And then he put in a password which it didn't like. And then it explained why. It turned it red with a red emergency symbol: "Your password can only contain letters, numbers, and these characters." And there's 10 of them. And I thought, what? They looked familiar to me. Sure enough. They are the shifted numeric characters on a U.S. Western whatever you call it, you know...

**Leo:** Yeah.

**Steve:** ...arranged keyboard.

**Leo:** Exclamation mark till left and right parentheses. They leave out tilde for some reason. Interesting.

**Steve:** I don't have tilde in my...

**Leo:** Oh, it's to the left of one. You're right. It's just one through zero. You're right.

**Steve:** Yeah, yeah, yeah. So it's exactly the shifted 1 through 9 and 0 keys on our keyboard.

**Leo:** Oh, that's bad. I see this a lot, I think.

**Steve:** So you can't do colon or semicolon, apostrophe or double quote. You can't use the curly braces or the squares. Apparently you can't use dash, plus, undersign, or equals.

**Leo:** That's weird.

**Steve:** No tilde. No back apostrophe. It's like, no vertical bar or backslash. Why?

**Leo:** Why, why.

**Steve:** No forward slash or question mark. You can't use greater than or less, I mean, they're, like, they've discarded a bunch of really good ones.

**Leo:** Why? Yeah. That's the question, why?

**Steve:** Anyway, Lets Burninate, I agree with you. Lets Burninate.

**Leo:** Let's burn it.

**Steve:** I don't get it.

**Leo:** It's a witch. Burn it.

**Steve:** Weird. Now, and I should note, if we didn't have browser-based hashing, then you'd have to think they were sending this back to central headquarters.

**Leo:** [Crosstalk]

**Steve:** Yeah, who says, no, no, no, I don't know how to pronounce that squiggly one so we're not going to have a tilde. You know, nobody knows what a tilde is, so it's like, okay. Wow. Again, there is no logic whatsoever.

**Leo:** There's no reason, yeah.

**Steve:** To them excluding those. Awk, whose handle is @adrianteri, he said: "Re feedback on 869's Moxie's Knockknock." He said: "One can minimize their exposure of things on the Internet without punching holes on their NAT routers. On 833 you mentioned a couple of more options to 'overlay networks' other than tailscale that might enable one even on a home/residential IP to be able to interconnect their devices across the Internet even with their IPs changing." And Awk, you are absolutely right. I wanted to make sure I mentioned that. I thought that was, you know, thank you for the tweet.

He's of course right. This new class of so-called "overlay networks," you know, Hamachi was the first one that appeared, and now there's a whole bunch that are free and public domain, and great-looking, by all appearances. That is another way to allow a roaming device to participate in an overlay network which is being maintained by a machine on

your network or a router on the border, and not have to do any sorts of hole punching. So again, thank you.

And then Bob Grant asked: "Hi Steve, thank you for your recommendation on McCollum," meaning Michael McCollum. He said: "Can you suggest a good starting point for reading him?" And I think I'd start with his Gibraltar trilogy. I think that was the first one that we all read here on the podcast. You know, Michael McCollum writes old-school hard sci-fi where, for me, the joy...

**Leo:** No otters drifting down rivers, is what you're saying.

**Steve:** We'll talk about that in a minute, yes.

**Leo:** Okay.

**Steve:** The joy is in his plot devices. I love being surprised, and I have always found Michael's work to be full of delightful moments. And to your point, Leo, speaking of sci-fi, I told our listeners that there would be the first episode of a new Star Trek series that I had great hopes for, "Strange New Worlds," premiering last Thursday. It did. I watched it. And I loved it.

**Leo:** It's very much in the old school. Every episode has a beginning, middle, and end. There's a moral at the end. You know, very much like the original series, I thought. There's even apparently a fistfight with aliens.

**Steve:** You've got to have that.

**Leo:** Got to have that. No red shirt guys, but other than that.

**Steve:** Spock gets to do his neck tweak.

**Leo:** Vulcan, yeah, and gets a good line off on it, too.

**Steve:** Yes. So we do have a young Spock and a young Uhura.

**Leo:** Spock is perfect, I have to say.

**Steve:** Yes.

**Leo:** And we have yet to see, but they mention, I don't know if you noticed this, a Lieutenant Kirk onboard.

**Steve:** Oh, no. He did come onboard toward the end.

**Leo:** Oh, did we see him?

**Steve:** I believe that our Kirk, James T. Kirk, had a brother, as I recall.

**Leo:** Oh.

**Steve:** And I think that when they talked about a Lieutenant Kirk, I thought, what?

**Leo:** Yeah.

**Steve:** But it wasn't James.

**Leo:** And a young Nurse Chapel.

**Steve:** Yes, a young Nurse Chapel. Anyway, Lorrie was a bit confused about like the timeline on this. And so I had explained to her that this was a prequel to the original Kirk series.

**Leo:** But only like 15 years before, right, because...

**Steve:** Well, and that Pike was the previous Captain of the Enterprise, to whom Spock had loyalty which superseded his to his own Captain Kirk at the time, and the Federation. Spock stole the Enterprise.

**Leo:** Right.

**Steve:** In that episode.

**Leo:** Right.

**Steve:** And, boy, was Kirk pissed off.

**Leo:** It was the pilot; wasn't it?

**Steve:** It was a pilot that was never aired.

**Leo:** The pilot was never aired. Okay.

**Steve:** Yes. Anyway, I loved it.

**Leo:** Somebody's asking is it the alternate timeline. It is not the new reboot timeline. It is the original series timeline; right?

**Steve:** It is a prequel.

**Leo:** It's a prequel.

**Steve:** Yes.

**Leo:** It is not this new rebooted movie timeline.

**Steve:** Right.

**Leo:** That, no, this is very traditionalist, except for the graphics are updated.

**Steve:** Oh, and Leo...

**Leo:** The bridge looks nice.

**Steve:** Something about me, I don't know, I was getting choked up at various points. It just is so exactly right so far.

**Leo:** Spock is perfect, I think, in that. He's just very...

**Steve:** Yes, and I like Pike. I think he's got like the right mixture.

**Leo:** Good hair. He's got good hair.

**Steve:** And he's like, humility and okay, fine. Anyway, I'm very, very, very, very, very hopeful. We're only going to get 10 episodes. So if you wanted to, first of all, you could sign up, if you wanted to pay Paramount, what is it, $5 a month or something for the three months that it'll be airing.

**Leo:** It's pretty cheap, I think, yeah.

**Steve:** Or if you really wanted to be tricky, they offer you five free days. So you could wait for three months, get your five free days, binge it during that time...

**Leo:** Oh, I don't know. That's a lot of Star Trek.

**Steve:** It is.

**Leo:** It's a little, I'm going to say, a little cornball. Because I think really it is so true to the original series that it has that - it's not modern in the sense that it's kind of corny like the original series was.

**Steve:** And like me. Maybe that's why, yeah.

**Leo:** Yeah. I think people who liked the original series will love it because it's much more in that spirit than even TNG or Discovery or any of the other more modern stuff.

**Steve:** So in discussing some of the newer shows, some writer said, "This is not your father's Star Trek." And my point is, this is...

**Leo:** It is.

**Steve:** ...your father's Star Trek.

**Leo:** Absolutely is your father's Star Trek. Or your grandfather's.

**Steve:** And apparently that's what I want because Discovery was like a sped-up videogame. It was just - it was not - well, and I do like that episodic format where you don't have to like, last time...

**Leo:** Each one's standalone, yeah, yeah.

**Steve:** Yes.

**Leo:** No previously, yeah.

**Steve:** Now, it also is the case that the phrase "Picard Season 2" rhymes nicely with "And I hate Q." God, do I hate Q.

**Leo:** I never liked him, either.

**Steve:** I always have, and it turns out I still do.

**Leo:** Yeah.

**Steve:** He is an annoying fly in the ointment. And I suppose that I'm not a huge fan of John de Lancie, the actor. But we're watching the second season. We'll finish it tonight. We have two episodes left. It's better than the first one only because the first one was so horrible. And I heard that the second one was better. It's like, okay. Yeah. But it's got Q. It's like, you know, you just can't have a really annoying omnipotent alien who wants to get in Picard's face all the time. It's just annoying.

So anyway, there were also too many dumb scenes which it very much had the sense that they were trying to draw the episode out to fill the hour. So I don't know. For what it's worth, I'm very capable of disliking something that has Star Trek in its name, even something that has Jean-Luc Picard. "Strange New Worlds" I thought was great.

**Leo:** And Lisa said, "I don't want any more of the ugly old bald Captain Kirk captain. I want the young hot captain." And I think Pike fits this, although she really - I think she really wants Shatner back. Ignore the bald old guy, that's it.

**Steve:** Well, I've got to give Bill Shatner credit for, like, hanging around.

**Leo:** Legend. Legendary, yeah.

**Steve:** He is wonderful. When I was over at IMDB because I wanted to update for the show notes the current ranking of "Strange New Worlds," it is at 8.3.

**Leo:** Oh, that's good.

**Steve:** Out of 10. That's a very good rating. And it's going up. That's what you want to see. You want to see them going up after the actual show has been out for a while. What I stumbled on was the official trailer for the new Avatar movie called "Avatar: The Way of Water." And apparently this is number two. It sure took Cameron a long time to get number two out. But number three is already in post-production, four is filming, and five is in the pipe. So we're going to get a bunch of Avatars.

And, I mean, it looked astonishing. I remember when I was watching the first Avatar I just sat there thinking, how do you make this movie? How do you make this? I mean, it was just an astonishing piece of visualization. But this sort of looks like the first one. And, you know, okay, I guess maybe it's a new story for the kiddies, I'm afraid. I'm not sure that it's going to, you know. But Cameron has never disappointed me. I mean, he gave us "The Terminator," "Aliens" the second one, "The Abyss," "True Lies," "Titanic," "Dark Angel" - that's where we saw Jessica Alba, ooh, baby - and "Avatar." So, yeah.

**Leo:** Mixed bag, I think. Okay, Steve. By the way, I did want to mention, you didn't like Book 4 of the Bobiverse. That's where I was talking about otters floating down the river. I liked it. I liked it quite a bit. So but now I'm waiting for Book 5. Love the Bobiverse.

**Steve:** Good. Good.

**Leo:** Yeah. Now let's talk about this FIDO thing because I'm very - I really want to get your take on it.

**Steve:** So Ars Technica's headline was "Apple, Google, and Microsoft want to kill the password with 'Passkey' standard. Instead of a password, devices would look for your phone over Bluetooth." Bleeping Computer said "Microsoft, Apple, and Google to support FIDO passwordless logins." The Record said "Google, Apple, and Microsoft to expand support for passwordless sign-in standard." And it made the headlines in all of the tech press. And all of these headlines popped up last Thursday, May 5th, which as I said at the top of the show was not only Cinco de Mayo, but also World Password Day. And the news of and questions about this new "Passkeys" was the most tweeted-to-me item of the past week, with many of our listeners wanting to know what it was and what I thought.

Having spent seven years of my life designing, implementing, demonstrating, and proving a complete working solution to this need, I have a good grasp of the problem domain. So I dug into this "Passkeys" news by going to the source, as I always endeavor to. I first read the FIDO Alliance's May 5th press release which was titled: "Apple, Google, and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins." This was the press release that everyone else was quoting in the news. It appeared that whoever wrote it was being paid by the word, since it went on and on to make sure that its reader would come away knowing that all pre-FIDO systems were bad, and FIDO was the cure.

At this point it appears that regardless of whether or not it turns out to be the cure, it will at least be the next thing we try. And I'm in the same boat as all of our listeners. We're all avid users and consumers of the Internet. So we're all hoping that the industry knows what it's doing. But that press release wasn't going to get the job done. Fortunately, it linked to the description of the FIDO Alliance white paper titled "Multi-Device FIDO Credentials."

The description of the paper that links to it said: "The FIDO standards, together with their companion WebAuthn specification, are on the cusp of an important new development. Evolutionary changes to the standards proposed by the FIDO Alliance and the W3C WebAuthn community aim to markedly improve the usability and deployability of FIDO-based authentication mechanisms. As a result, FIDO-based secure authentication technology will, for the first time, be able to replace passwords as the dominant form of authentication on the Internet." What a concept.

"In this paper," they say, "we explain how FIDO and WebAuthn standards previously enabled low-cost deployments of authentication mechanisms with very high assurance levels. While this has proved an attractive alternative to traditional smart card authentication, and even opened the door to high-assurance authentication in the consumer space, we have not attained large-scale adoption of FIDO-based authentication in the consumer space. We explain how the introduction of multi-device FIDO credentials will enable FIDO technology to supplant passwords for many consumer use cases as they make FIDO credentials available to users wherever they need them, even if they replace their device."

Okay. So I have a link in the show notes to the PDF for anyone who wants the raw material. Obviously this descriptive overview still doesn't tell us what we want to know. So I dug into the whitepaper. We get the Executive Summary, followed by "A Brief History of Online Authentication." Then a section titled "FIDO: Starting from the Top," followed by "WebAuthn Level 3: Bringing Up the Bottom." So this brings us to the bottom of page four of the PDF, and we begin to frame the problem as follows. The explanation explains: "FIDO-based solutions can also increase the security of consumer two-factor

authentication by providing phishing resistance, regardless of whether those use cases care about hardware-based sign-in credentials or not."

Now, I should mention that FIDO was always hardware based, which has been the problem that they've been struggling with is that the FIDO authentication standard was you will have a hardware dongle, a token, a something which, because it's hardware, because it's physical, it cannot be spoofed. It cannot be, you know, no one in Russia can get the contents of what you have in your thing you're holding in your hand because you're holding it in...

**Leo:** The YubiKey said there are some that are FIDO2 YubiKeys. That's what you mean.

**Steve:** Yes, yes, yes. And so...

**Leo:** Which is that's good. That's good security. No one would deny that; right?

**Steve:** You could argue it's the best. The gold security.

**Leo:** Yeah.

**Steve:** Yes. The problem is it's physical.

**Leo:** And it makes people buy keys, $50 keys.

**Steve:** Yes. Exactly. The benefit is it's physical. The problem is it's physical. And so if you absolutely - so they said: "FIDO-based solutions can also increase the security of consumer two-factor authentication by providing phishing resistance regardless of whether those use cases care about hardware-based sign-in credentials or not." In other words, they're saying we're giving up. We're going to back down from the position we had taken, I mean, you could still use hardware-based sign-in credentials, but now you're not going to have to. We're not going to make you have to have a hardware dongle. And this has been sort of in the air for a couple of years; right? There's been talk about being able to use your phone as your FIDO authenticator. So this notion isn't completely new. It's been happening.

They said: "However, we have observed limited adoption in this latter category, especially in the consumer space, because of the perceived inconvenience of physical security keys - buying, registering, carrying, recovering - and the challenges consumers face with platform authenticators as a second factor, for example, having to re-enroll each new device; no easy ways to recover from lost or stolen devices." They said: "While these drawbacks can make FIDO-based solutions, whether based on physical security keys or platform authenticators" - and I should explain this phrase "platform authenticators." That just means your smartphone or your laptop. They're calling that a "platform authenticator" as opposed to a physical security key. So "...drawbacks can make FIDO-based solutions, whether based on physical security keys or platform authenticators, a tricky proposition for users already accustomed to two-factor authentication, they present an even higher barrier to adoption for users who don't or don't want to use two-factor authentication at all, and are stuck with passwords."

And so finally we get down to it. The white paper explains: "The FIDO Alliance and the W3C WebAuthn working group are proposing to address these gaps in a new version" - which they call "Level 3" - "of the WebAuthn specification." They said: "Two proposed advances in particular bear mentioning." And so here they are, one and two. Number one: "Using your phone as a roaming authenticator." That's the first of these proposed advances.

They said: "A smartphone is something that end-users typically already have. Virtually all consumer-space two-factor authentication mechanisms today already make use of the user's smartphone. The problem is that they do this in a phishable manner. You may inadvertently enter a one-time password on a phisher's site, or you may approve a login prompt on your smartphone not realizing that your browser is pointed at the phishing site and not the intended destination. The proposed additions to the FIDO/WebAuthn specs define a protocol that uses Bluetooth to communicate between the user's phone, which becomes the FIDO authenticator, and the device from which the user is trying to authenticate." You know, your laptop, for example. "Bluetooth," they say, "requires physical proximity, which means that we now have a phishing-resistant way to leverage the user's phone during authentication."

**Leo:** Yeah, the hacker has to be in physical proximity. Which is good. Right? Because Bluetooth is not the most secure - well, go ahead, go ahead.

**Steve:** No. Of course SQRL solved this with a QR code that you let your phone see, as we know.

**Leo:** Right, right.

**Steve:** They said: "With this addition to the FIDO/WebAuthn standards, two-factor deployments that currently use the user's phone as a second factor will be able to upgrade to a higher security level, phishing resistance, without the need for the user to carry a specialized piece of authentication hardware (security keys)." Oh, thank god. So yes, we'll be able to use our phones. Wonderful. That was point one.

Here's point two: "Multi-device FIDO credentials." Okay? They say: "We expect that FIDO authenticator vendors, in particular those of authenticators built into OS platforms" - this is, we've heard the names, right, Apple, Google, Microsoft - "will adapt their authenticator implementations such that a FIDO credential can survive device loss. In other words" - and again, hasn't been done yet, but this is what they expect. "We expect that FIDO authenticator vendors," blah blah blah. "In other words, if the user had set up a number of FIDO credentials for different relying parties" - and "relying parties" is a term of art in this whole identity space - "on their phone." If the user had set up a number of FIDO credentials for different relying parties on their phone.

And notice that in FIDO you need a credential per relying party. That is, a FIDO credential for Amazon, a FIDO credential for PayPal, a FIDO credential for Facebook, a FIDO credential for Google, blah blah blah. One each. So it's a one-for-one mapping in FIDO. "And then," they say, "got a new phone, that user should be able to expect that their FIDO credentials will be available on their new phone. This means that users don't need passwords anymore."

**Leo:** [Gasping]

**Steve:** "As they move from device to device, their FIDO credentials are already there, ready to be used for phishing-resistant authentication." Okay. Now, I'll just pause to note that I solved this problem with one-time password authenticators with my sheaf of printed QR codes; right? We were talking about that last week.

When I'm enrolling on a site that offers me second-factor authentication with a one-time password, and it shows me the QR code which I can then capture with my authenticator on my phone, I also print the page. I print the paper out, and it's securely stored. I have a sheaf of them for all the places I use two-factor authentication. So that, yeah, if I need to set up a new device that doesn't sync in some fashion with the authenticator in my phone, I can do that. It's offline. No one in Russia can get to it. It's very secure. But yeah, it's a little burdensome. I had to do that. Lots of people don't, and then they get stuck if their authenticator won't export or transport and sync.

So they say: "For these multi-device FIDO credentials" - so this is their term. Multi-device FIDO credentials just means cloud sync. That's all that is, multi-device FIDO credentials. "It is the OS platform's responsibility to ensure that the credentials are available where the user needs them." And they said: "Note that some companies are calling FIDO credentials 'Passkeys' in their product implementations, in particular when those FIDO credentials may be multi-device credentials." So in other words, just for the record, passkeys is not a term of art in FIDO. And I imagine that the company that has a trademark on "Passkey" is not very happy. A lot of people noted that the government started to use the term "Shields Up" for one of their things. And it's like, yeah.

**Leo:** What are you going to do.

**Steve:** Okay, fine, I don't care. Exactly. So they say: "Just like password managers do with passwords, the underlying OS platform will sync the cryptographic keys that belong to a FIDO credential from device to device. This means that the security and availability of a user's synced credential depends on the security of the underlying OS platform's (Google's, Apple's, Microsoft's, et cetera) authentication mechanism for their online accounts, and on the security method for reinstating access when all old devices are lost. While this may not always meet the bar for use cases that require physical key level security," they write, "it is a huge improvement in security compared to passwords."

They say: "Each of the referenced platforms apply sophisticated risk analysis and employ implicit or explicit second factors in authentication, thus giving two-factor-like protections to many of their users." So this is FIDO saying, well, it's not as good as physical keys. We're kind of annoyed. But look, it's going to work. Like maybe someone will actually use FIDO because we're going to allow cloud syncing in this Level 3 mode. And the people who are doing the syncing are being responsible enough.

So they said: "The shift from letting every service fend for themselves with their own password-based authentication system to relying on the higher security of the platforms' authentication mechanisms is how we can meaningfully reduce the Internet's over-reliance on passwords at a massive scale." In other words, they're saying that we will rely upon the user authenticating to their own device smartphone or desktop with biometrics or whatever, rather than authenticating to each remote site individually. And yes, that sounds familiar.

Finally, they say: "Syncing FIDO credentials' cryptographic keys between devices may not always be possible, for example, if the user is using a new device from a different vendor which doesn't sync with the user's other existing devices. In such cases, the existence of the above-mentioned standardized Bluetooth protocol enables a convenient and secure alternative: If the FIDO credential isn't readily available on the device from

which the user is trying to authenticate, the user will likely have a device, for example a phone, nearby that does have the credential." So in other words, if you're using Windows, and iOS won't sync to Windows, then you can use Bluetooth on your iOS device to get the credential over into Windows. They said: "The user will then be able to use their existing device to facilitate authentication from their new device."

Okay. So it appears that what this press release and these so-called "Passkeys" - which again as the white paper explains don't actually have anything to do with FIDO, that is, the term doesn't - it's just the introduction of cloud syncing among devices to facilitate the transport of one's collection of FIDO credentials from one device to the next. The other piece, well, and in the case of device loss, when you get a new one, you resync with the cloud and you get all of your FIDO credentials back.

The other piece is that the FIDO Alliance appears to have formally given up on the idea that we're all going to go out and purchase a hardware FIDO token when we all already own a smartphone that can serve the same purpose. The use of a possibly available Bluetooth link allows one's smartphone to be used to authenticate to a website on a desktop that does not contain a FIDO authenticator with one's credentials. And as we said, for clarity, that's what SQRL provides for with a QR code and the smartphone's camera.

And yes, speaking of SQRL, I know that the head of everyone out there who understands SQRL is exploding right now because FIDO still falls very far short of providing the complete solution that SQRL offers. But having moved from simple usernames and passwords to password managers and multifactor authentication and then to OAuth third-party authentication, we're now going to get FIDO, though it will apparently be popularly called "Passkeys." From the samples I've seen online, it appears that it will still be necessary to first identify oneself to the web site being authenticated to. So FIDO with "Passkeys" replaces the password, but unfortunately not the username. So it will continue to be somewhat more cumbersome in that way.

The way FIDO's crypto works is that it randomly synthesizes a public and private key pair for each and every website the user wishes to authenticate with, and it gives that site the public key to retain while the FIDO authenticator stores the matching private key for each subsequent use for reauthenticating. So it's this collection of individual private authentication keys which are now being called "Passkeys" that Apple, Google, and Microsoft will be obtaining and synchronizing in the cloud for their users. This provides for same-platform cross-device FIDO credential synchronization which is crucial for FIDO since each new website authentication creates another public/private key pair. And it provides for credential recovery in the event of device's loss, and that's certainly needed to create a practical system.

As we know, I went a different way with SQRL. SQRL uses a single master key which can be printed and stored safely. Or it could be loaded in the cloud if you wanted, whatever. From that one key, it deterministically synthesizes unique per-site public and private key pairs based upon the website's domain name; and, like FIDO, it gives each website the public key to use for future authentication. But unlike FIDO, there is no growing collection of randomly synthesized per-site private keys that need to be retained and cloud-synced among devices. So there's no need to back up a large collection of private keys to the cloud or anywhere.

The only thing a SQRL user ever needs for their identity to be secure and fully recoverable for all websites is one piece of paper. And if you have multiple identities on multiple devices, you can log in for the first time on some other device that has your same SQRL identity. And when you log on a different device, the identity works because multiple devices all synthesize the same private key.

So backing off from that, overall, this whole big announcement of Passkeys appears to have mostly been a World Password Day-timed press event without much technology to back it up. We're not getting SQRL. We, all of us, we're getting FIDO. And that means we need cloud-synchronized "Passkeys" to make FIDO's use practical. The good news is we're going to get it. I'll be interested to see how the login flow functions. The other big thing FIDO is missing is it doesn't identify you to the site. You still have to first identify yourself, then FIDO replaces your password. SQRL did both, which was way more convenient. But anyway, we're not getting SQRL. We're getting FIDO. And Passkeys basically makes FIDO feasible because you have to be able, since you are synthesizing completely random keys for every site you visit, you've got to collect them. You've somehow got to cross-device sync them. And Apple, Google, and Microsoft will be taking care of that for us.

**Leo:** So it sounds like it's kind of less secure than if you used a YubiKey, I guess.

**Steve:** Yes. This is absolutely FIDO group, the FIDO Alliance compromising themselves down from their ivory tower because...

**Leo:** Which they needed to do because nobody would use it.

**Steve:** Because nobody wanted FIDO, yes.

**Leo:** Right.

**Steve:** Nobody was going to do it. I mean, yes, high-level, I know that there are Google employees who use their Titan keys to do things. But I don't have one.

**Leo:** It's not going to succeed if everybody - but, see, that's my other issue is not everybody has a smart device.

**Steve:** Correct.

**Leo:** I guess would this work if you didn't have...

**Steve:** It's always possible to still use a username and password.

**Leo:** Oh, okay.

**Steve:** That will never go away.

**Leo:** Okay.

**Steve:** Never, never, never go away.

**Leo:** Which means that's what people are going to do.

**Steve:** Yes. Yes.

**Leo:** So...

**Steve:** You know, my favorite example, Leo, is the person who said, "Oh, I don't need a password manager." And I said, "You can't be using the same password everywhere." And she said, "Oh, no, I don't." And I said...

**Leo:** How do you do that?

**Steve:** And she said, "Well, when I'm creating an account, I just bang on the keyboard a lot." And I said, "Okay." And I said, "So how do you log in again?"

**Leo:** I forgot.

**Steve:** She said, "It always - there's a little line there that says 'I forgot my password.'" She said, "And I never knew it, so I did forget it."

**Leo:** Yeah.

**Steve:** And she said, "Then they send me a link, and I log in with that."

**Leo:** That's actually - that's fairly secure; right? I mean, honestly, yeah?

**Steve:** Well, you know, it uses an email confirmation in order to reassert that you have...

**Leo:** As long as you don't lose control of your email, you're okay.

**Steve:** Correct. And that is the segue to next week's Picture of the Week, which is already in the document and waiting to be displayed.

**Leo:** You don't have anything else, but that's there.

**Steve:** That's right.

**Leo:** I love it. Obviously SQRL would be much more secure. But SQRL has a similar problem which is it is not trivially easy to use. And for that reason I think people are

going to fall back to a password for almost anything. Single sign-on's good. You know, I use Microsoft now for login to Windows. As you know, sends to your phone an authenticator, sends it a digit, a two-digit number, and you say, yeah, I know that number, and you're in. That seems like - is that the same thing as this FIDO thing? It's similar.

**Steve:** Well, so it's specific to Microsoft.

**Leo:** That's right, that's right, yeah.

**Steve:** Yeah. And so we're looking for a broad-based solution which solves the phishing and the "I forgot my password" problem.

**Leo:** Right.

**Steve:** Which is easy to use. The fact is we'll have to see what the flow looks like. It is certainly easy to do login with Facebook, login with Google. We know that that's horrific from a tracking and privacy standpoint, right, because you're bouncing through them.

**Leo:** Yeah. Oh, I don't do that, yeah. I've stopped doing that entirely, yes.

**Steve:** Oh, my god. And in fact I did hear you on TWiT last Sunday talking about how you were finally thinking maybe you should be taking privacy a little more seriously.

**Leo:** Yes, yes. I admitted I was wrong. And that because these data brokers selling information about who visited Planned Parenthood over the past week for 160 bucks. And what that does is it puts you - if you live in Texas, and there are now other states, and soon it might even be...

**Steve:** Criminalizing.

**Leo:** ...23 other states...

**Steve:** Criminalizing interstate travel for the purpose of terminating a pregnancy.

**Leo:** So for 160 bucks anybody, the way this Texas law works, anybody can go after you. So there's now probably a brisk business, people buying that information and then suing you, or law enforcement in Tennessee, for instance, going after you. Or I guess it's Louisiana. In any event, it suddenly became obvious that the government is now starting to go after people for things that they shouldn't be, and it is now dangerous to leave this stuff on, unfortunately.

**Steve:** And that's really, I think that is, you're right, that's the takeaway is that, given a certain set of existing laws, you could argue that with those laws there's a reduced risk from lack of privacy.

**Leo:** Yeah.

**Steve:** But if the laws change...

**Leo:** Well, that's the problem. Exactly.

**Steve:** And suddenly the previous assumptions no longer hold under the new regime.

**Leo:** Exactly.

**Steve:** And that's the danger.

**Leo:** Yeah. If you trust the government, no problem. I no longer trust the government, so problem.

**Steve:** Yeah.

**Leo:** And that's too bad.

**Steve:** Yeah.

**Leo:** But now we have to pay more attention. So you've been right all along. I was a wide-eyed optimist. I am no longer. Steve, thank you, as always. It's always eye-opening and always fascinating.

If you do not tune in every Tuesday to Security Now!, you really ought to. If you're listening today, I think you know now. Several ways you can do this. You can watch live. If you happen to be around 1:30 p.m. Pacific, 4:30 Eastern, 20:30 UTC on a Tuesday, you could just go to live.twit.tv. There's a live audio and video stream there. You could watch that. If you're watching live, chat live at irc.twit.tv. After the fact, you can online go to TWiT.tv/sn. That's our website.

Steve also has the show at his website, GRC.com. In fact, he has two unique formats. He has good hand-contrived transcripts by Elaine Farris, who listens to this show, she's listening even now, and writes it down and then puts it in a transcript. That's really handy for searching. You can also get a 16Kb version for the bandwidth-impaired. Then of course the full 64Kb audio, also available at GRC.com.

If you're over there, you know, it might be a good idea to pick up a copy of SpinRite, current version 6.0. If you buy today, you'll get a copy of 6.1 when it comes out, but you'll also participate in the final stages of that creation. And everybody who has mass storage really needs SpinRite, the world's best mass storage maintenance and

recovery utility. There's lots of other great stuff: GRC.com. You can also leave him feedback there: GRC.com/feedback. Maybe the better way to do it is through Twitter. He has his DMs open, as the kids say. You can slide into them, @SGgrc on the Twitter: @SGgrc.

We have copies of the show at the website, as I mentioned. You know, the easiest thing might be just to subscribe. Both Steve and I have links to the RSS feed. You put that into your podcast client, and you'll get the show the minute it's available, each and every Tuesday so you can listen at your own leisure, at your own pace. I know some people who like to listen at 1.5. In which case when you watch live, I've just got to warn you, we will sound drunk talking at normal speed.