A Week of News and Listener Views

Description: What mistake did Microsoft make that allowed Russians to access their top executives' email? What does the breach of U.S. Health and Human Services teach us? What does Firefox's complaint about Apple, Google, and Microsoft mean? Why has the Brave browser just reduced the strength of its anti-fingerprinting measures? Last year CISA started proactively scanning. How'd that go? What new feature of smartphones has become a competitive advantage? And just how incognito is that mode?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-958.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-958-lq.mp3

Then we'll wrap up the week by looking at some of the best feedback from our listeners, including what's the future of fraudulent media creation? How should a high school listener of ours get started with computing? Why did a popular Android app suddenly become sketchy? Does Google's Privacy Sandbox allow websites to customize their presentations to their visitors? How might last week's LG smart washing machine have become infected? Does the Protected Audience API also protect its audience from malvertising? And why do big ISPs just pull the plug on DDoSed sites rather than attempt to protect them?

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. And, man, do we have a jam-packed show. It's my favorite kind of show, lots of listener questions and lots of Steve's answers. We'll also learn what farbling is, and why it turns out too much farbling is too much of a good thing. Or something like that. Why Mozilla is unhappy with the heavy-handed tactics of Big Tech, and I kind of don't blame them. And of course a Picture of the Week that makes absolutely no sense. It's just part of the fun every week, right here on Security Now!, next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 958, recorded Tuesday, January 23rd, 2024: A Week of News and Listener Views.

It's time for Security Now!. I know, I know, you've been waiting all week, and here it is, Tuesday. It just never comes around fast enough. But Steve Gibson is here with another thrilling, gripping, how many pages did you say, 19 pages?

Steve Gibson: Nineteen pages. And Leo, this week people on Apple platforms will be able to see the pictures.

Leo: All around you. You didn't buy a Vision Pro, huh?

Steve: No, no.

Leo: No, me neither.

Steve: I'm astonished by the technology, and I don't think I know anybody except through TWiT who will have any.

Leo: Well, I'm coasting on those guys.

Steve: I'm not a big - long term, I think VR can be astonishing because, you know, our animal natures get hooked by what our senses perceive, I mean, powerfully. And in fact I actually have some comments about that later in today's show. But so I think VR can be very powerful. I just think, you know, I remember when we tried to do the first generation of laptops, and they had to have wheels because, okay, well, you can move it around, but you need to get Bruno to put it up on the desk for you. Finally we got actual laptops. But it took a decade from when we first began trying. I think VR is like that. We're going to get there. And until we do, everyone's going to be like, oh, VR doesn't work, it's nonsense, blah blah blah. It's like, no, it's just too soon, you know. Our ambition is exceeding our technology at the moment.

Leo: Yeah, you heard and agreed with, I think, Jason Snell's take.

Steve: Yes.

Leo: On MacBreak Weekly earlier.

Steve: Yes. I think it absolutely makes sense for Apple to be launching this now to get a whole bunch of developers going. They're going to learn so much, Apple is, from all the feedback and experiences. And this is also first-generation technology. It's incredibly impressive. It's not clear at the moment how it can be like super reduced. But, you know, there was a great movie, remember "Brainstorm"?

Leo: Oh, dimly.

Steve: With Christopher Walken.

Leo: Yeah.

Steve: Christopher Walken. And the very first...

Leo: It was a Michael Crichton book; wasn't it?

Steve: I think it was, yes. The very first cap was like, you know, all this crap and a huge umbilical going down to a cart that they had to push around next to the guy. And through a succession of innovations, they reduced it to just a small little clip that you stuck on your head that still had the same effect. And, yeah, we're going to get there.

Leo: It will get there.

Steve: We're just not there yet. I look at that the most modern, the underside of today's hard drives, and there's a 16TB hard drive. It's got a little itty-bitty circuit board like that runs along the connector. And it's like, what we used to have was crazy compared to the degree of integration that we have today.

Leo: We used to have a card in a slot to run a hard drive; you know?

Steve: Yeah and sometimes a daughter board and lots of cables running around.

Leo: And you didn't have - and now they've got 30TB hard drives which we never thought would happen. And I certainly bought those little ones.

Steve: I don't think they actually exist, Leo, because no one's ever managed to actually fill one. So how would we know?

Leo: We wouldn't know. You've got to run your little program on it and see.

Steve: That's right.

Leo: On 30TB it might take a little while. What do we have? What's on the menu for today?

Steve: We have Episode 958 for this second to the last, that would make it the penultimate episode of January's Security Now!. No single topic jumped out and grabbed me. So I titled this "A Week of News and Listener Views." But that is not to say there's not a lot going on. We're going to find out what mistake Microsoft made that allowed Russians to access their top executives' email. What does the breach of the U.S. Health and Human Services Department teach us? What does Firefox's complaint about Apple, Google, and Microsoft mean? Why has the Brave browser just reduced the strength of its anti-fingerprinting measures? Last year CISA started proactively scanning. How'd that go? What new feature of smartphones has become a competitive advantage, thankfully? And just how incognito is that mode?

Then we'll wrap up the week by looking at some of the best feedback from our listeners, including what's the future of fraudulent media creation? How should a high school listener of ours get started with computing? Why did a popular Android app suddenly become sketchy? Does Google's Privacy Sandbox allow websites to customize their presentations to their visitors? How might last week's LG smart washing machine have become infected? Does the Protected Audience API also protect its audience from malvertising? And why do big ISPs just pull the plug on DDoSes rather than attempt to

protect them? Of course we have a great Picture of the Week for our listeners to view, and I think another great podcast this week.

Leo: So somebody's saying that "Brainstorm" was not a Crichton book. It sounds like one, though.

Steve: Yeah.

Leo: It seems like it would be. I'm going to have to watch that tonight. Maybe I'll watch it today. I love Christopher Walken.

Steve: It's a great - Christopher Walken. Also...

Leo: Natalie Wood, Cliff Robertson, Louise Fletcher? What a cast.

Steve: Fletcher is the one, yes, it's got a great cast.

Leo: Nurse Ratched's in it, yeah.

Steve: And it's also - it's a very cautionary tale about VR. I mean, it is the early VR movie, early VR sci-fi. And I'm tempted to say more. But I don't want to spoil it for any of our listeners because he does something, well, there are two very controversial aspects of it. So anyway, said enough. Great movie, definitely.

Leo: And I will watch it.

Steve: It is a great, it is a good sci-fi movie.

Leo: From 1980, what, '83? Wow.

Steve: And it was Natalie Wood's last movie.

Leo: Oh, that's sad. I will watch it. Loved her. All right. Let's take a little break; shall we? And then we will get into the show, in the depth. You know, as you read your list of topics for today, I realized your show really is more and more kind of about everything going on in computing. I mean, it is as much a, you know, here's what's happening in computing show as TWiT is, frankly, since so much of it revolves around security these days.

Steve: And privacy.

Leo: And privacy technology. So I can't wait. I have some thoughts about some of these topics, too.

Steve: Cool. I just got my renewal notice from [Bitwarden] since it was a year ago.

Leo: What do you pay, 10 bucks a year.

Steve: Ten bucks. I don't need to, but I want to keep them going.

Leo: Right, exactly. I pay the 10 bucks too for the premium account. I don't need to. But I want to support them. I just think they're the greatest, yeah.

Steve: Okay. So I assume you've not yet seen the Picture of the Week.

Leo: No, I always try to keep my eyes clean.

Steve: When you can, that's good. And this will be one of those because this one is - oh.

Leo: All right. I'm scrolling up now. I'm looking at the show notes. You can do it with me, folks. Let's scroll up. "You have to wonder," Steve writes, "how much use that peephole gets." Okay, Steve. You got me. That's hysterical. Do you want to explain?

Steve: Okay. So we're all familiar with the little peephole that people have on like the doors of their residences, where there's some lensing so that, you know, before you open the door to admit someone, you're able to stick your eye up to it and see who's standing on the other side.

Leo: But that's usually on solid doors.

Steve: Yes. Not on a door that is basically four large glass panes. That's like, what? What?

Leo: That's pretty funny.

Steve: And there's also a glass side panel. So even if the door was solid, you'd still have to be careful about how you approached the door. You couldn't approach from the left on the inside or they'd see you walking over to the door.

Leo: That's very funny.

Steve: So anyway, so the point - now, the only thing I can think, Leo, is that the door comes in glass or non-glass panel options.

Leo: Oh, that's what it is, sure. Yeah, yeah.

Steve: So you could have had it where the whole thing was white, with opaque white panels. Then the peephole would have mattered. So the peephole is probably there regardless of whether you get glass or not. But it does make for a funny picture because, you know, who's going to - and actually it would be fun if the people who lived there actually had some fun with it, like if someone's knocking at their door, so they go over to the door and look through the peephole to see who it is.

Leo: Oh, how funny.

Steve: Anyway, thank you, our listeners. Our listeners are providing a constant stream of great photos that they think, okay, saw this and thought of you, Gibson.

Okay. Last Friday the 19th, the rest of the world learned that Microsoft's top executives had fallen victim to a Russian state-sponsored password attack - like, what, password? - which breached their email accounts. Here's what Microsoft shared in their Friday blog posting, which was titled "Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard."

They wrote: "The Microsoft security team detected a nation-state attack on our corporate systems on" - now this, you know, a nation-state attack is how you dramatize the fact that somebody guessed your password, it's like, whoops - "on January 12th, 2024, and [the Microsoft security team] immediately activated our response process..."

Leo: We pulled the chain that said "Emergency Only."

Steve: Right. Break glass and pull all the wires, yeah, "...activated our response to investigate process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access." Yes, we changed our password. "Microsoft has identified the threat actor as Midnight Blizzard..."

Leo: How did they identify it, since any moron could have done this? It wasn't like a hefty, you know, eight-stage attack involving a secret hash table or anything like that.

Steve: Let's try Monkey123. Oh, what do you know, we're in.

Leo: Read the sentence about what they did. I love this.

Steve: Okay, well, we'll get there, "...the Russian state-sponsored actor also known as Nobelium."

Leo: Right.

Steve: Now renamed Midnight Blizzard.

Leo: They must have [crosstalk].

Steve: Because it sounds much more dramatic and, like, how did you manage to survive the Midnight Blizzard? "As part of our ongoing commitment to responsible transparency" - in other words, we're a publicly traded company, and we have to tell you, "as recently affirmed in our Secure Future Initiative (SFI), we're sharing this update.

"Beginning in late November 2023, the threat actor" - okay, now again, late November, right, so now we have December and up to January 12th. So they've been roaming around, apparently for a while. "Beginning in late November 2023, the threat actor used a password spray attack..."

Leo: Yeah, what's that, Steve? What's a password - oh, and worse, on what, Steve? What did they use that password spray attack on?

Steve: Yeah, "...to compromise a legacy non-production test tenant account and gain a foothold" - and in other words, you know, they guessed the password.

Leo: Guessed the password of some old machine that's probably in a corner somewhere.

Steve: Yeah. They sprayed it, Leo. And, you know, it should have been sprayed with cleanser.

Leo: Password spray account attack. Well, all right. That's why we know it's Nobelium.

Steve: They gained a foothold, "...and then used the account's permissions" - which apparently were too permissive...

Leo: Well, that's the real question; right? Okay. So you got in this old server in a closet somewhere, fine, with a bad password and no two-factor. Fine. But what then happened?

Steve: And then in their attempt to minimize this, they said: "to access a very small percentage" - but apparently it was sufficient.

Leo: It was the right percentage. They weren't interested in Joe in accounting. For some reason they only wanted to see Satya Nadella's email.

Steve: But get this. They have to enumerate, right, "a very small percentage" - this is because Microsoft has so many corporate accounts - "a very small percentage of Microsoft corporate email accounts, including..." that small percentage included...

Leo: Tiny percentage. Yeah, just tiny.

Steve: "...members of our senior leadership team and employees in our cybersecurity, legal, and other functions..."

Leo: Maybe they did get Joe from accounting.

Steve: Yeah, it's not good, "...and exfiltrated some emails..."

Leo: Oh boy.

Steve: Some, right, we don't know how many. They know, they're not telling us, "...and attached documents."

Leo: Oh, gobs.

Steve: "The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself." Like what do they know about us? Why did they change our name? We liked Nobelium. Now we're Midnight Blizzard? What? "We are in the process of notifying employees whose email was accessed." Because apparently that's a big process. So, okay.

Leo: It was only a small fraction, Steve. Let's not blow it out of proportion.

Steve: It's a small fraction of a big number, though, Leo. So it's going to take a while for us to notify all those employees.

Leo: Of course the guys who got in weren't interested in 99% of the email accounts.

Steve: Only the good stuff.

Leo: Just the good ones.

Steve: Right. Yeah, we've got cybersecurity, legal, and other not specified functions.

Leo: And the people who run the freaking company.

Steve: Yeah. The leadership team. You know, those guys.

Leo: The fact that they say...

Steve: But apparently we can't get a hold of them right now. So we're in the process...

Leo: We're going to notify him. We don't know where he is. Oh, lord.

Steve: Now, here we come. "The attack was not the result of a vulnerability" - what a nice, fresh change - "in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems." I thought it's interesting now that we're being specific about whether they got into our AI or not. "We will notify customers if any action is required." Not only that, but they sprayed everything, apparently.

"This attack does highlight the continued risk posed to all organizations" - right, not just Microsoft, you know - "from well-resourced nation-state threat actors like [the newly renamed] Midnight Blizzard. As we said," they wrote, "late last year when we announced Secure Future Initiative, given the reality of threat actors that are resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk." In other words, they've decided they're going to get more security focused. "The traditional sort of calculus is simply no longer sufficient," they say. "For Microsoft, this incident has highlighted the urgent need to move even faster" than they apparently were.

Leo: This is the worst kind of corporate doublespeak.

Steve: It really is.

Leo: They're implying - someone guessed the password of a little used machine that happened to have permissions to access their servers.

Steve: Yup.

Leo: That is the worst possible corporate governance.

Steve: Yup.

Leo: This is embarrassing to them. So they've waved - there's a lot of hand-waving about, oh, no, it was a big nation-state. They guessed their password.

Steve: And everybody else is at risk. Oh, my god, yeah. So they explained...

Leo: So infuriating.

Steve: Yeah. So, "We will act immediately" - because we didn't before, so we're going to do it now - "to apply our current security standards to Microsoft-owned legacy systems and internal business processes, even when these changes might cause disruption to

existing business processes." Oh, this causes disruption. "This will likely cause some level of disruption while we adapt to this new reality." Whoa, wakeup call.

Leo: We've got to lock these things down. Holy cow.

Steve: "But this is a necessary step, and only the first of several we will be taking to embrace this philosophy."

Leo: Oh. You know what I think? It was a PlayStation 2 in Satya Nadella's office. That's what I think.

Steve: They're not telling us.

Leo: No, they won't tell us.

Steve: "We are continuing our investigation and will take additional actions based on the outcomes of this investigation. We'll continue working with law enforcement and appropriate regulators. We are deeply committed to sharing more information" - right, oh, and here we come - "and our learnings." We're going to get some more learnings sharing, Leo.

Leo: Oh.

Steve: "So that the community can benefit from both our experience and observations about the threat actor." We can't see them, of course, because it's midnight, and there's a blizzard.

Leo: We're going to sketch them.

Steve: "We will provide additional details as appropriate. You will never hear from us again." Oh, no, I added that part.

Leo: This is clearly written by, I mean, the fact they used the word "learnings" is the tell off, by corporate PR, not by a technical person. But it's embarrassing.

Steve: Leo, the technical people would spill the beans.

Leo: Yeah.

Steve: We can't have that. We have to have someone who knows nothing write our announcement of what happened so that nothing will be known afterwards.

Leo: Yeah. Wow.

Steve: So it does read as a bit of a wake-up call for Microsoft. And it's interesting because arguably they were telling us, and they're right, there's a lesson here for every large enterprise. You know? As you said, Leo, read between the lines, and actually reading the lines, it sounds as though some older systems still have older levels of security, and they've been allowed to continue purring along undisturbed since, you know, they aren't bothering anyone. But they were still online and obviously accepting incoming logons and so getting sprayed with passwords. And, you know, presumably newer systems are being deployed with stronger password quality minimums, multifactor authentication, brute force detection, you know, spray prevention, and all of the additional layers of security that have become modern standard practice.

The lesson here, which Microsoft has just learned the hard way, and which I wanted to bring up, you know, I wanted to bring to the attention of our IT-managing listeners, is that the law of the lowest hanging fruit applies to legacy machines that are not bothering anyone. You know, they aren't bothering anyone until they become the source of ingress into an enterprise's interior. So, just a note of caution to remember that bad guys won't attack the most secure entry points to an organization, or if they do they won't get in. They will attack successfully the weakest. And that might be some machine that still has a password and policies that have not been considered safe since the turn of the century.

And this is really a thing. We all know the lesson LastPass learned by failing to proactively enforce PBKDF iteration counts which were current at the time that they were introduced, and they never changed them again. Security really is a moving target, and older systems won't improve their older security on their own without it being revisited. You know, we would not expect Microsoft, to your point, Leo, to not to put the best face on this possible. So we can assume that they did. But the news of this breach received some harsh criticism from other quarters.

Here's what one respected security reporting group had to say. They started by speaking about some email content, writing: "Microsoft's disclosure language does not specifically state that this was the only stolen material, but it is worth pointing out that Microsoft is currently hosting the Ukrainian government's entire network on its Azure cloud infrastructure." That's interesting. I hadn't encountered that little tidbit before.

Anyway, they continue, writing: "The breach has drawn quite an avalanche of criticism and ridicule for Microsoft for various and well-deserved reasons. First, Microsoft disclosed the breach late on a Friday night, a well-known scummy tactic," these people write, "to hide the incident from extended media coverage.

"Second, the breach took place weeks after Microsoft announced, with bells and whistles, its new Secure Future Initiative, a new plan to re-focus the company's engineering efforts to improve the security of its own products. The new initiative was meant to mimic a similar pledge made by Bill Gates in 2002, named Trustworthy Computing" - something we all know well, those of us who've been in the industry - "that led to significant changes to Microsoft's security posture and the creation of what we now know as Patch Tuesday.

"Third, the new breach took place four months after Microsoft disclosed another state-sponsored hack, this one by China's Storm-0558, which also had access to its internal network." And that's the one we talked out extensively previously. "And fourth," they wrote, "after promoting its multifactor authentication as the next evolution of online account security, the fact that one of its test accounts got popped via a password spray suggests Microsoft was not high on its own supply.

"The hack is quite bad, but not for most of you reading this. It may not have a material impact on day-to-day Microsoft users, but it has quite a reputational damage on Microsoft's position in the cybersecurity market. Having Russian intelligence services breach your cybersecurity team's email accounts to steal data about themselves four months after the Chinese breached your production systems to steal U.S. government emails is not what this industry calls trustworthy." So indeed. Most of that criticism is covered by the observation that they didn't update their older systems. But I just want to say it is certainly the case that old systems need attention, and they should get it. So a useful reminder about that.

A still unknown threat actor stole $7.5 million from the U.S. Department of Health and Human Services in a security breach that took place between March and mid-November of last year.

Leo: Why, that's almost six months, Steven. It's almost nine months.

Steve: I know. It struck me as interesting that the range is that broad.

Leo: It's kind of large, yes.

Steve: There's quite a lot of time between March and November.

Leo: They need a Thinkst Canary.

Steve: Uh-huh. The unknown attackers are believed to have gained access to an HHS system that processes civilian grant payments using spear-phishing. They then proceeded to hijack payments for five grant recipients before being detected. The investigation to identify the perpetrators is still underway. So our takeaway here is that, once again, the human factor remains Security's number one Achilles heel. Having strong outbound security - such as I was reminded by that provided by the ADAMnetworks guys who so impressed me when I talked about them last year - and also training, training, training, including reinforcing that training on a continuing basis. You've got to teach your people not to click on links.

Leo: Yeah, yeah.

Steve: Like, you know, you just have to. And then what the ADAMnetworks guys do is a great job on neutering the clicking of the link if someone still does.

Leo: Right, right.

Steve: So, you know, it's so easy for a harried worker who has too much going on to click a link that they shouldn't. And, you know, that's what happened here.

Leo: Yeah, but Steve, when they use the devastating password spray attack, all bets are off.

Steve: You met my good friend Bob Basaraba.

Leo: Oh, yeah.

Steve: A Canadian. His brother is actually a Hollywood actor, Gary Basaraba, who I see on, like, he makes little appearances here and there. Gary is nontechnical, but just larger than life, just a big guy. Bob was telling him once about a ping flood and how like a ping flood was like pushing somebody off the 'Net. And Gary, who knows absolutely nothing about computers, said, well, why didn't they just use a reverse ping attack?

Leo: Oh. There you go. Another one to add to my quiver of tools.

Steve: Reverse ping attack. That'll teach them to ping you.

Leo: Ping 'em back.

Steve: Also last Friday, Mozilla posted a complaint to the industry under the heading "Competition." The title of this posting was "Platform Tilt: Documenting the Uneven Playing Field for an Independent Browser Like Firefox." Okay. So here's what Mozilla wrote. They said, correctly: "Browsers are the principal gateway connecting people to the open Internet, acting as their agent and shaping their experience. The central role of browsers has long motivated us to build and improve Firefox in order to offer people an independent choice. However, the centrality of the browser creates a strong incentive for dominant players to control the browser that people use. The right way to win users is to build a better product, but shortcuts can be irresistible. And there's a long history of companies leveraging their control of devices and operating systems to tilt the playing field in favor of their own browser.

"This tilt manifests in a variety of ways, for example, making it harder for a user to download and use a different browser, ignoring or resetting a user's default browser preference, restricting capabilities to the first-party browser, or requiring the use of the first-party browser engine for third-party browsers. For years, Mozilla has engaged in dialogue with platform vendors in an effort to address these issues. With renewed public attention and an evolving regulatory environment, we think it's time to publish these concerns using the same transparent process and tools we use to develop positions on emerging technical standards. So today we're publishing a new issue tracker where we intend to document the ways in which platforms put Firefox at a disadvantage. We wish to engage with the vendors of those platforms to resolve these issues.

"This tracker captures the issues we experience developing Firefox, but we believe in an even playing field for everyone, not just us. We encourage other browser vendors to publish their concerns in a similar fashion, and welcome the engagement and contributions of other non-browser groups interested in these issues. We're particularly appreciative of the efforts of Open Web Advocacy in articulating the case for a level playing field and for documenting self-preferencing. People deserve choice, and choice requires the existence of viable alternatives. Alternatives and competition are good for everyone, but they can only flourish if the playing field is fair. It's not today, but it's also not hard to fix if the platform vendors wish to do so. We call on Apple, Google, and Microsoft to engage with us in this new forum to speedily resolve these issues."

Okay, now, of course, many of us prefer to use Firefox as our browser of choice. I have Chrome and Edge, but URL clicks are always sent to Firefox.

Leo: Me, too. On all our machines, yeah.

Steve: It's my default browser. And I have Firefox installed on all my various Apple iOS devices.

Leo: Oh, see, I haven't gone that far. They really don't make that easy.

Steve: Unh-unh.

Leo: And you're not really using Firefox.

Steve: Exactly. So I dug a bit deeper into this new issue tracking system, and it was quickly apparent that Apple had the most strikes against it. At this moment, Mozilla is complaining about Apple Store forbids third-party browser engines; support for third-party multi-process applications on iOS; JIT [Just in Time] compilation support on iOS; accessibility APIs on iOS; messages integration; importing browser data; setting and checking default browser; origin-based Associated Domains dependent features for third-party browser engines; browser extension support; and beta testing support on iOS.

Now, we know how heavy-handed Apple is. I'm an avid user of Amazon's Kindle readers and also of Amazon's Kindle app on iOS, where I use it on iPads and my iPhone. And it is a constant and ridiculous annoyance that Apple refuses to allow Amazon users to purchase books through the Amazon app.

Leo: Absolutely.

Steve: It is so dumb. It's necessary to use a web browser. Why? Because Apple has iBooks and cannot stand the competition.

Leo: Well, they would let Amazon do it, but they would get 30% for it. And Cory Doctorow was talking about this on Sunday, that margins on the books, the eBooks, is lower than 30%. So Amazon would have to give them all the profit and then some.

Steve: Right.

Leo: So it's just not going to happen.

Steve: It's just dumb. So I'm sure that Apple's reticence to allow Chrome and Firefox and any and all other non-Safari browsers to enjoy the same privileges they have on other platforms is largely about security. I mean, I get it; you know? As we know, browsers have become the number one way for evildoers to crawl inside our computers. So I don't blame Apple for that. But given my experience, you know, elsewhere and with

Apple, I also have no doubt that some of this is just pettiness which, as I said, should be beneath Apple. For what it's worth, though, I'm sure Apple is not singling out Firefox for prejudicial treatment. They treat anything that's not Safari as suspect.

Leo: Yeah, exactly.

Steve: Mozilla is also unhappy with their experience over on Google's Android platform. There, they voice three complaints: importing browser data on Android; some Android features launch Chrome instead of the user's default browser; and lower quality search results in third-party browser engines on Android. I was curious to look into these three a bit further, especially the last one, which we'll get to in a second. What I found was interesting.

In detailing their complaint about importing browser data on Android, Mozilla explained: "Browsing information like history, bookmarked sites, and cookies is not accessible to third-party browsers on Android. This data is kept within a web browser application's data directory, which is not directly accessible to third-party browsers, and there's no API or ContentProvider to enable it to be imported. While this is sensitive data," Mozilla agrees, "similar import functionality is possible on all major desktop platforms, and Android is able to mediate access to other sensitive data with user consent. Not being able to import data creates significant friction to change from Chrome. A user should be allowed to bring their data with them to another browser."

And I think that seems like a legitimate complaint and a slippery way for Google to give Chrome an anti-competitive edge over any other browser its user might wish to switch to. And the second issue raised, "some Android features launch Chrome instead of the user's default browser," that seems even more insidious. Mozilla explains: "Features like Google Search or Discover, in the pre-installed Google application, ignore the user's default browser choice. Links to websites outside of the application are always opened in Chrome, regardless of the default browser. This is a widely used application," they say, Mozilla says, "with additional entry points from built-in features such as the search bar on the home screen and app launcher. Each time it opens a link in Chrome, a user is driven away from their default browser. All built-in applications and affordances that open external links should open them in the user's default browser."

Right. That would really annoy me, and this issue will be quite familiar to anyone who has heard Paul Thurrott ranting about Microsoft and Edge doing the same thing.

Leo: Oh, yeah. Edge launches, you breathe on it, it launches, yeah.

Steve: Yes.

Leo: What? Me? You want me? You want me? Yeah, I'm here, yeah.

Steve: As Mozilla says, every time Chrome is launched when the user has installed Firefox and asked Android to use it, drives the user toward Chrome despite their clearly expressed browser preference. And it was the third item in Mozilla's "Platform Tilt" list of grievances that most caught my eye. They wrote: "Lower quality search result pages in third-party browser engines on Android." That seemed like a real antitrust showstopper.

Here's what Mozilla explained. They said: "The web search experience is tightly integrated with a number of built-in features in Android, and the experience provided to Firefox is inferior compared to the version provided for Chrome. As seen in the screenshots, identical search terms show less information and receive a lower quality design in Firefox on Android." And for anyone who's interested, I have the side-by-side screenshot in the show notes, where is it, on page six of the show notes, where indeed you can see the Chrome as a fancy-looking display, and Firefox not so much. It's kind of got a little textual summary instead of some nicer graphics.

Leo: You know you can't do graphics in Firefox. It doesn't - you can only do it in a proper browser, you know.

Steve: Mozilla said: "While strictly speaking this is an issue with the Google Search website, given the prominence and integration of search on Android this is a meaningful user experience gap that creates an incentive for users to not choose a third-party browser."

Leo: They've got a really good point. I mean, this is the same data coming from the same site, a Google site. But they intentionally poorly render it on anything but Chrome.

Steve: Yes. And you know why? It's the user-agent header. It turns out that Google search results are biased against non-Chrome browsers.

Leo: That's terrible.

Steve: I know. It is so wrong. If the user-agent string is changed, then Google will provide the same improved experience to Firefox users as Chrome users. Now, user-agent dependency is nothing new. And once upon a time Chrome's page results rendering may have necessitated producing different results to differing browsers. But those days, you know, those are long gone. This sort of deliberate bias is showing Google's own extreme pettiness. And speaking of Microsoft and Windows, well, Microsoft's own incestuous ties to its own web browser actually, as we know, have been the subject of antitrust lawsuits in the past, and big ones.

Mozilla lists three complaints about Microsoft's and Windows's treatment of Firefox, and you can imagine where this is going. The three complaints are setting default browser on Windows; default browser is set to Edge by several Windows flows; and some Windows features launch Edge instead of the user's default browser. It is starting to sound like a refrain. Under "Setting default browser on Windows," Mozilla writes: "Allowing a third-party browser to programmatically set itself as the default is an important platform feature. Without this, even after the user has installed the browser of their choice, they must navigate operating system settings and make the choice there, as well. This adds friction and creates inertia to continue using Edge, despite the user's obvious preference.

"A well-established design pattern is to allow the third-party browser to invoke a system prompt which permits the user to easily confirm or reject the request to set the current browser as the default. This is an intuitive user experience that mirrors similar permissions models used in operating systems, browsers, and web applications. Android and macOS offer such a capability.

"Unfortunately, Windows does not support anything like this for third-party browsers. Browsers are forced to 'deep link' into the Windows settings UI. On Windows 10, this requires several clicks and a double confirmation in the settings UI. On Windows 11 there is a 'Set default' button. Neither is sufficient. Windows should instead provide a method for third-party browsers to programmatically request they be set as the default."

And to that I'll just say, yup. This is the traditional way that we've all historically experienced the addition of a third-party browser being installed. The browser notices that it's not currently the system's default URL handler and asks its user whether they would like it to switch them over to using this browser instead. The user says "Yes, please" or "No, thanks," and it's done. But no longer. Microsoft, exhibiting the same pettiness we see from Apple and Google, clearly wishes to hold onto the use of Edge every way possible. As I sit in front of Windows 10, I'm periodically reminded of just how much my life could be improved if only I would allow their Edge browser to service my needs. No, thank you.

And speak of the devil, here's Mozilla's second complaint: "In general, the Windows 10 and 11 operating systems have persistent messaging that Microsoft Edge is the 'recommended' browser for Windows, and offer affordances to change the default browser to Edge. In some cases the wording is misleading, asking a user to adopt 'recommended browser settings,' which does not obviously suggest a default browser change. This messaging is a moving target, with examples added and removed from Windows over time, often on UI surfaces that appear automatically on update or otherwise, making it difficult to enumerate specific examples." Right, so they've become quite slippery.

"In all cases," Mozilla says, "these Windows components are able to change the user's default browser directly, and are not forced to use ms-settings: protocol deep linking that browsers are required to use. Windows should consume the same affordances and APIs that are available to third-party browsers for setting-to-default." Yep. Just another of the many reasons I am perched in front right now of my trusty, and crusty, old Windows 7 system. You know? I'm subjected to none of that extraneous crap.

Okay. And lastly, Mozilla says: "There are at least three prominent Windows features that open URLs in Microsoft Edge and not in the current default browser. The user's default browser choice should be respected when web pages are opened by built-in operating system features. The first is Windows Search, also known as Start Menu Search, and formerly known as Cortana. The UI for this feature is represented by a taskbar search box or search button, depending on the user settings; and a search suggestions/results UI that appears when activated and updates as the user types. The suggestions and results UI also appears if the user starts typing when the start menu is open, and by the WIN+S hotkey. All links from this UI, whether they initiate web searches or link directly to articles or results, open in Microsoft Edge, regardless of the user's default browser.

"The second is the new Windows Copilot, currently only available on Windows 11, which appears as a docked window on the right side of the screen. If Copilot produces links in its responses, or offers other links within its rendering area, these links open in Microsoft Edge, regardless of the user's default browser.

"Third, there are Windows 'widgets' which are called 'news and interests' on Windows 10, and a UI surface which can be activated by a taskbar button. These show information like news, weather, stocks, and sports scores. On Windows 11, new widgets can be added from third parties. Regardless, all links to a web page from widgets will open in Microsoft Edge, regardless of the user's default browser."

So, okay. In summary, what we have from Mozilla is highlighting and detailing pervasive pettiness. And, you know, not playing fair on the parts of Apple, Google, and Microsoft.

It's not like they absolutely refuse to accept a default, you know, to accept a browser change. That would probably get them in some serious hot water; right? Instead, it's like, oh, yeah, you can install a browser. And then they do everything they can not to really let the user use the browser, not the way they obviously could if they wanted to. Clearly not playing fair. So Leo, what do you think is behind this?

Leo: It does seem...

Steve: Is this like gearing up for a little antitrust activity here?

Leo: Yeah.

Steve: Microsoft seeing their market share dwindle?

Leo: It's hard to explain because with Edge they had an opportunity in the early stages, and Paul Thurrott's always saying this, to say, hey, we're a better Chrome than Chrome. We're Chrome without the privacy problems, you know, they've always knocked Google for its privacy plan. I mean, this bugs me about Microsoft all around is that they could actually do very well by saying we're a private platform. We respect our users. We keep it private. We have a better browser that's got less stuff. Instead, they put coupon codes in there and all sorts of crazy...

Steve: Well, and then it's got - I've got shopping fact on - it's like, what the heck?

Leo: Yeah. And so is it, I mean, they don't need the money. Except Apple doesn't need the money by charging 27% instead of 30% if Kindle uses its own Amazon link. These companies are greedy. I think really what's happening, and we're seeing it again and again, we're seeing it in Big Tech, but we're also seeing it in our politics, where people go, I don't care if you don't like it. It doesn't matter.

Steve: Right.

Leo: I'm going to do what I want to do.

Steve: You're right.

Leo: Screw it, you know. And the heck with the FDC and...

Steve: Basically abusing the power that they have.

Leo: We're going to abuse the power.

Steve: They have the power. They're going to abuse the power.

Leo: And they no longer care about governments. They no longer care about users. They care about profit. It's very disappointing.

Steve: Microsoft knows nobody has a choice. They're, like, forcing people up to newer versions of Windows, and those newer versions of Windows are increasingly creating lock-in.

Leo: The thing that's frustrating is they don't need to do this, and they could do so well for themselves if they said, no, no, it's a better Chrome than Chrome. We're privacy focused. We don't need to do all of that. You own the computer. You own the platform. They would, I think, do better by doing that. And so it's baffling.

Steve: And look at Chrome's market share. I mean...

Leo: Oh, they're gone, completely gone.

Steve: My wife has Chrome on Windows 10.

Leo: Of course she does.

Steve: Because she doesn't - and she keeps complaining about this Bing, and like it keeps Binging her. She says, "How do I stop this?"

Leo: It's unfathomable.

Steve: And it's obviously not working.

Leo: But I honestly think that these companies have gotten to the stage where they don't care, and they just don't need to. And this is what Cory Doctorow's always talking about with [crosstalk].

Steve: They're too big to care.

Leo: They're too big to care. It's time for them to squeeze us. Steve, it is your turn once again.

Steve: So, meanwhile, last Thursday, the Brave browser, which is super popular among those who are truly privacy and anti-tracking concerned...

Leo: That's the one Paul Thurrott likes.

Steve: Yup, notified its users that Brave would be reducing the strength of its anti-fingerprinting protections.

Leo: That's weird.

Steve: Under the heading "Brave browser simplifies its fingerprinting protections," the Brave team wrote: "With desktop and Android version 1.64 in a couple of months, and in today's nightly release for testing, Brave will sunset Strict fingerprinting protection mode. This does not affect Brave's industry-leading fingerprinting protection capabilities for users." What? "Instead, it will allow us to focus on improving privacy protections in Standard mode and avoid web compatibility issues."

Okay. Now, they say: "Brave will sunset Strict fingerprinting protection mode," and then immediately follow that with "This does not affect Brave's industry-leading fingerprinting protection capabilities for users."

Leo: What?

Steve: I know; right.

Leo: How does that not - what?

Steve: Yeah.

Leo: You're reducing protection but it doesn't affect your protection?

Steve: That's right. So...

Leo: Huh?

Steve: They said: "Brave currently offers two levels of fingerprinting protections which make it harder for tracking companies to identify you as you browse the web, Standard and Strict mode. Over time, however, we've observed significant disadvantages of Strict mode." Okay. Here they are. "First, in order to block fingerprintable APIs, Strict mode frequently causes certain websites to function incorrectly or not at all."

Leo: Oh, okay.

Steve: Whoops.

Leo: So it breaks functionality. I can understand that, yeah.

Steve: "This website breakage" - yes. "This website breakage means that Strict mode has limited utility for most web users. Next, fewer than half a percent of Brave users are using Strict fingerprinting protection mode, based on our privacy-preserving telemetry data." So, you know, we know that, but don't worry, we're not spying on you. "Third, this tiny cohort of users could be more vulnerable to being fingerprinted because they stand out as a result of using Strict mode." Which, you know, that's an unintended consequence. "Although we've not seen issues around this, it is a valid concern given that users who use Strict fingerprinting protection might have done so because of an elevated concern about tracking." Right. Why else would you do it? And "Fourth, maintaining Strict mode and debugging why some websites are broken on Brave takes our engineers' time away from focusing on default privacy protections that can benefit all of our users."

They said: "These observations have led us to the conclusion that sunsetting Strict mode in Brave will actually be beneficial to our users' privacy." And they explain: "Brave's Standard fingerprinting protection is already very extensive and the strongest of any major browser. Brave's innovative farbling of a number of major fingerprintable Web APIs makes it difficult for fingerprinters to get a reliable unique ID on your browser. Going forward, we will continue to strengthen and expand Brave's Standard fingerprinting protections so that all our users have ever-improving protection against fingerprinters, while maintaining the highest possible level of compatibility with websites."

Okay, first of all, you did hear me use the term "farbling." I have no idea where they came up with that, but okay. I tracked it down, and it's Brave's term for introducing some random jitter noise into the values being returned by the Web APIs that are commonly used for fingerprinting. Those APIs are the Canvas API, WebGL, WebGL v2, the WebGL Extensions, the contents of the browser's user-agent header, web audio, the browser's plugins, hardware concurrency, the enumeration of system devices - both their ordering in the enumeration and their labels and IDs - and the user's dark mode setting.

Since I was curious and knew our listeners would be, too, I tracked down the difference between Brave's soon-to-be-discontinued "Strict" anti-fingerprinting mode and the mode that all Brave browser users will be left with. So here's how Brave describes the two modes. They said: "Brave has two levels of fingerprinting protections. In the default 'standard' configuration, Brave adds subtle noise to APIs commonly used to fingerprinting scripts."

Leo: Ah, fuzzing.

Steve: Without, yes, without breaking websites.

Leo: Interesting.

Steve: "And will provide good protections against web-scale online trackers. Brave also includes a 'strict' option. When set to 'strict' mode, Brave only returns random values from APIs commonly used by fingerprinters. This provides a higher level of protection against highly determined attackers, who may attempt statistical and/or targeted attacks to identify users. This mode will also break websites who depend upon these features to work correctly."

Leo: So it's fuzzing versus farbling, I guess you could say.

Steve: Well, actually, I would say that the milder "standard" mode uses, dare I say, only moderate farbling of API values which do not cause website issues because only some of the least significant bits are being farbled.

Leo: Well, then, there you go.

Steve: Well, yeah. Because what you want in your least significant bits is a little bit of farbling.

Leo: Farbling.

Steve: But what strict mode does is to entirely discard the true API values and replace them with fully random values for these API calls that bear no resemblance to reality.

Leo: Of course that's going to break stuff.

Steve: Yes. My reading of this is that the original designers of Brave's anti-fingerprinting technology probably got their farble turned up too high.

Leo: Oh, I hate it when that happens.

Steve: I do not want this. You know, they probably thought, you know...

Leo: Set farble to stun.

Steve: If a little farbling is good, just how great it would be...

Leo: More is better.

Steve: ...if we just farbled the crap out of this. But apparently, after gaining more experience with this, they learned that some websites became quite upset when they were over-farbled. You never want to over-farble, but especially not on a school night.

Leo: Oh, yes.

Steve: Anyway. And actually I can see how the statistical analysis they refer to could theoretically be a problem, since over time the results from a low and safe level of farbling could be averaged out to obtain the true value around which the farbled values are clustered. But on balance I wouldn't worry about that too much. I think Brave is doing the best they can while not causing more trouble than the farbling is worth. So elimination of Brave's "strict mode" sounds like a good thing.

Leo: Actually, they made a really interesting point, which is that so few people use the strict mode, it itself could be a form of fingerprinting.

Steve: Yes.

Leo: I thought that's fascinating. You want to be in the herd. You don't want to be the one on the outlying edges of the herd.

Steve: You don't want to be singled out.

Leo: Yeah, yeah.

Steve: And so if they saw someone's browser that's like producing wildly bizarre values, they'll go, aha.

Leo: We have an over-farbler.

Steve: We weren't sure, but this guy's over-farbling, and there aren't that many of them out there.

Leo: Yeah. That's really - that's actually a fascinating insight into how this stuff has to work. You cannot de-fingerprint people by doing things that only a handful of people do because then they get identified. It's really interesting. Good on Brave. You know, it sounds like they did the right thing.

Steve: Yep, I think so, too. And we have added a word to our lexicon, Leo.

Leo: They mean fuzzing; right? I mean, that's fuzzing.

Steve: I could have named the episode "Never Over-Farble."

Leo: On a school night. You should have.

Steve: That's right, on a school night.

Leo: You should have named it that. It's not too late to change, Steve. We can work it.

Steve: Okay. So coming up on a year ago, in the middle of March 2023, I noted and was quite glad to share that CISA, our already very proactive U.S. Cybersecurity and Infrastructure Security Agency - I never thought I was going to be able to just have that roll off the tongue. But yeah, Cybersecurity and Infrastructure Security Agency...

Leo: Next is Roskomnadzor, and you'll be the king.

Steve: ...was launching an even more proactive initiative. They called it the Ransomware Vulnerability Warning Pilot, and thank god they didn't try to make the abbreviation pronounceable, it's RVWP. So, you know, they're not Google.

Leo: Yeah.

Steve: And they described it this way. They said, this is back in March: "Organizations across all sectors and of all sizes are too frequently impacted by damaging ransomware incidents. Many of these incidents are perpetrated by ransomware threat actors using known vulnerabilities. By urgently fixing these vulnerabilities, organizations can significantly reduce their likelihood of experiencing a ransomware event. In addition, organizations should implement other security controls as described on stopransomware.gov.

"However, most organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network. Through the Ransomware Vulnerability Warning Pilot, which started on January 30th, 2023, so coming up on a year ago, CISA is undertaking a new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors.

"As part of RVWP, CISA leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks. Once CISA identifies these affected systems, our regional cybersecurity personnel notify system owners of their security vulnerabilities, thus enabling timely mitigation before damaging intrusions can occur.

"CISA accomplishes this work by leveraging its existing services, data sources, technologies, and authorities, including CISA's Cyber Hygiene Vulnerability Scanning service and the Administrative Subpoena Authority granted to CISA under Section 2209 of the Homeland Security Act of 2002."

As our listeners know, I'm 100% behind the idea of having the good guys proactively scanning for vulnerabilities. We know that the bad guys are. So to the good guys, my only question would be what took you so long? Anyway, CISA just published their 2023 Year In Review, and it contained some gratifying news of the results from the first year of this pilot program, which I hope they can remove the "pilot" from it.

During this first year, CISA sent out more than 1,200 notifications to U.S. and international organizations, notifying them of early-stage ransomware activity on their networks. CISA also sent 1,700 notifications to organizations that had systems vulnerable to common ransomware entry vectors. In other words, the U.S. is finally proactively scanning the public Internet for vulnerabilities. Together, this totals an average of eight such notifications sent every day of the year last year. And it's difficult to imagine that anyone would blow off a notification from this U.S. agency saying that they've already found evidence of an existing network intrusion or of an existing public-facing vulnerability. So bravo, CISA. Yay.

Leo: I'm looking for farble.com or perhaps farbled.

Steve: Well, Leo, you do not want to look up farble in the Urban Dictionary.

Leo: Oh. Is there actually a word? Oh. No.

Steve: I made that mistake. You will not want to know what it is to farble.

Leo: Okay. I will...

Steve: So says the Urban Dictionary, and I now know that all of our listeners are doing so.

Leo: Oh, boy.

Steve: Sorry for bringing it up.

Leo: Yeah. Oh. You managed to withhold that information until later in the show. Okay.

Steve: So in news of a growing and necessary trend which we've been seeing recently, Samsung's just launched S24 series of smartphones will be receiving seven years of software and security updates.

Leo: Yes. That was good news.

Steve: Yes. That's an increase from the company's previous smartphone coverage, which were five years. So Samsung joins Google to be the only vendors to offer seven years of security updates for their Android devices. And the best news of all is that this suggests that the longevity of security support has finally become a recognized competitive advantage. That's nothing less than a big win for consumers and 100% great news.

Remember that we were recently talking about the lawsuit against Google over the consumers' "misunderstanding" - I'll put that in air quotes - "of the protections provided by Chrome's Incognito Mode. Now, it turned out it wasn't as incognito as we thought. In response to that, Google is changing the text that appears in Chrome's Incognito Mode. The new text much more clearly informs its users that their activity will continue to be tracked, even while they're in the somewhat less than entirely incognito mode. It now reads: "Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks, and reading list items will be saved. Learn more." And then you can click if you want more information. So anyway, they decided, uh, maybe we need to be a little more clear about that.

Oh. I wanted to acknowledge that I received our listeners' many notes that for reasons I think I understand now the images contained within the previous two weeks of show notes were not visible to users of Apple's iOS and macOS devices.

Leo: Oh, that's interesting. I didn't know that.

Steve: Uh-huh. It was also a coincidence that I had captioned last week's Picture of the Week "Please provide an example of irony," and that that picture was missing.

Leo: Ironically.

Steve: Ironically, yes. In any event, it appears that the trouble was that I always run the final show notes PDF, which I download from Google Docs, you know, where each document is authored, through Acrobat's PDF optimizer, from which it very nicely reduces the document size, typically from a couple megabytes down to a few hundred kilobytes. And I don't know what may have changed since it was nothing at this end. On the other hand, since my Acrobat...

Leo: I can see them, though. This is my Macintosh. I can see them fine.

Steve: Last week?

Leo: Yeah.

Steve: That's interesting because I got all - I verified on my - oh, wait, no. I know why. Because I fixed them.

Leo: Oh.

Steve: Yes.

Leo: But this is the attachment in your email. So this would have been the thing that you sent to me.

Steve: That's, you're right, that would have, and that should have been broken. I verified...

Leo: Now, I'm viewing it in the browser, and let me see if I can view it in Apple's Preview. Because as you know I save all of your show notes because god knows I wouldn't want to lose any of them.

Steve: Well, you want to feed them into some AI and have them, you know...

Leo: Yeah, I did do that, by the way, and it was not satisfactory.

Steve: Oh.

Leo: So you're safe. No, yeah, it works. I'm looking on my - this is on my Mac, both in Preview and in - and this is the one you attached to your email, so it's the original.

Steve: Well, my iOS - I have an iOS device, and indeed it did not show the pictures originally.

Leo: Oh, iOS, not Mac.

Steve: Well, I was told Mac, but apparently...

Leo: That's a Mac. Let me look on my iOS. Huh. That's interesting.

Steve: Anyway, my Acrobat, of course, is v9, with a copyright of 2008.

Leo: Which, by the way, should make it more compatible, not less.

Steve: I know, except that - so what I believe, because nothing else happened, nobody else complained, obviously you're able to see it elsewhere, I think I had it set back to version 5 PDF compatibility. I think Apple decided to stop supporting some feature of older PDFs.

Leo: Oh, yeah, here it is on my iPhone. There's a blank where it should be a clear visual example of irony. Okay.

Steve: Yup.

Leo: Okay. All right. Yeah. So on the Mac it's okay, but apparently on iOS they don't.

Steve: And I did find and fix the problem. So all of our listeners, both retroactively for those previous two weeks and also going today and in the future, well past 999, we will have pictures.

Leo: I'm going to open it in some other app on iOS.

Steve: You're really curious about this; aren't you.

Leo: Yeah, because, well, because this is the kind of thing I'm going to get calls about down the road.

Steve: Oh.

Leo: So I just want to - I want to make sure that, like if I have a workaround, that oh, well, if you open it in Google Drive, you'll be able to see it. Then that would be, you know. Let me see. I'm going to upload it to Google Drive and then open it. And no, still it's a blank.

Steve: Yeah. I think it - oh, really.

Leo: Well, wait a minute. Let me...

Steve: Oh, so when displayed on an iOS device.

Leo: Yeah. Maybe that's it. Let's see. Here's the Google Drive, and I just uploaded it. All right. Let's see if I can read this. Oh. Oop. Did you see that?

Steve: I did.

Leo: That was interesting. The thumbnail was there. Hmm. So even in Google Drive I'm not seeing it. Let's do this again. Watch this. Yeah. Did you see it? Briefly it showed up.

Steve: Yeah. Yep.

Leo: Yeah. I don't know what that means. Oh, well. I'll leave the detective work to your fine forum members at GRC.com.

Steve: It's fixed.

Leo: All right. Q&A time. This is actually - we used to do this every other show; right, Steve?

Steve: Yeah.

Leo: I love this. I used to love doing this.

Steve: Well, listener feedback we...

Leo: We still do some. We still do some. Close the loop.

Steve: Yeah, Closing the Loop. So our listener said: "Hello. I started my journey in cybersecurity two years ago. I've learned a lot and still have a lot to learn. Recent news

of AI-generated videos got me scared because of the future world my two-year-old son might be growing up in."

Leo: Too late.

Steve: "In your opinion" - sorry?

Leo: Too late.

Steve: Yeah. "In your opinion, what would be the best solution for automatic verification of a video, image, or audio? I'm thinking of some kind of encryption from the camera like a few episodes ago where photos are signed. But if I remember correctly, this is flawed because anyone can buy such a camera, dig the key from the hardware, and sign fake images. I believe this needs to be addressed as soon as possible and not like in 10 years. AI really took off. Who knows what might be next?"

Okay. So through the years we've observed everything that's happening around us. This podcast as a consequence has arrived at a number of "rules of the road," guiding principles which seem to apply. One of those that I've occasionally marched out is quite unsatisfying, though it doesn't render it any less true. And that is "Not all problems have good solutions," an example we were talking about last week being Internet DDoS attacks. Like it or not, the fundamental design of the Internet has made it inherently vulnerable to spoofed bandwidth flooding attacks and other sorts of attacks.

And I believe that we have the same problem here. When I was growing up, I was fascinated by optical illusions. One that pops to mind is that two parallel lines can be drawn on paper. And yep, they look perfectly parallel. But place a series of radial lines exploding outward from a central point, and those still perfectly straight parallel lines look curved. No matter how you try to tell yourself they are not curved, curved is what you see. The trouble is, we're built to believe our senses, and our senses can be fooled.

The corollary rule to "Not all problems have good solutions" is that technology cannot solve all of our problems for us. In fact, it's probably a zero-sum, with technology inadvertently creating just as many problems as it solves. Unfortunately, I am virtually certain that this listener's two-year-old son is simply going to grow up in a very different world than we have. It's going to be a world where the many things we were able to take for granted as being real depictions of events will simply never be the case in a world for someone born recently.

And of course there's been some of that for us. The phrase "Oh, that image was Photoshopped," you know, that's long been a common meme. Until now, it's been the exception. The fact that everyone perceives that what we're about to witness is a wholesale explosion in the volume of fictitious content masquerading as authentic suggests that, if nothing else, it's going to be a self-fulfilling prophecy.

And I don't see this view as pessimistic. I think it's realistic. As they say, being forewarned is to be forearmed. For those of us who have been around for a while, this seems like a big change for the worse. We're accustomed to trusting our senses and believing what we see. But it seems all but certain that this is a comfort future generations will simply not have. But then neither will they miss it, since things will have always been that way for them. We old codgers will eventually die off, grumbling, "When I was a boy..." and so forth.

Leo: I wonder what you think. So Canon announced this a couple of months ago, and they're doing it with a Stanford lab and a USC lab and Thomson Reuters. It's a proof-of-concept, but the idea is using cryptographic methods they're going to embed in the image's metadata information about the image, so Canon will basically verify in the metadata this image was created with a camera. Nikon and Leica have approached the same idea. There is something called the Content Authenticity Initiative. But I'm kind of with you. Anything that these companies can come up with, bad guys will just do an end-around. And in fact it's a false sense of security because you say, well, this has a Canon stamp. This is Canon, so it must be real.

Steve: Yes, that's exactly right. Exactly. I mean, it is exactly analogous to the example we've always drawn of the DVD decryption keys in the DVD player.

Leo: Yeah.

Steve: You know, the DVD player sitting on the consumer's shelf had to have the keys to decrypt the DVD. It didn't take long until everybody had the keys because they were sitting in the DVD player, and they got extracted. You know, it was going to happen. And so Canon's camera digitally signs the photo. And actually it's, I mean, they've done so much technology. There's like this audit trail. You can only use Adobe's tools to make changes, and the Adobe tool creates like a pen's metadata creating an audit trail of all the modifications that were made to the photo.

Leo: It's got a chain of custody for the photo so you know exactly who's had it and who's touched it.

Steve: Yeah, I mean, you know, it's just going to make - it's trying to make money for people, and it's, again, won't be long before it's hacked and cracked, and there'll be photos that are like proven to be authentic of like the sun going supernova.

Leo: Right.

Steve: It's like, wait a minute, I don't think that happened.

Leo: Yeah. You know, this is why I'm glad you're going past 999 because this will, of course, be announced with fanfare, and then it will be hacked, and this is how we're going to learn if it's been hacked or if it's reliable because Steve will let us know. So I'm very grateful because this isn't going to happen in the next year and a half. But, boy, before the next election we're going to see a lot of fake stuff floating around.

Steve: And I do think that to this listener's question the world has changed.

Leo: It has.

Steve: The fact, I mean, the fact that you guys on MacBreak and Andy can create these astonishing images just by asking for them, that is earth-shattering.

Leo: Yeah.

Steve: And it just means that people growing up now will not - they will just always have been in a world that had the Internet, which we didn't have in the beginning.

Leo: Right.

Steve: That was a big change. And they will have always had the Internet, and they will have always had a world where you can't believe the things you see.

Leo: Yeah, yeah.

Steve: They'll just know that.

Leo: And they will just not trust anything they see; right? That's not...

Steve: Right. I was reminded of that wonderful sci-fi movie, which was it, where the aliens believed - they were receiving our TV transmissions from Earth, and they had no concept that they had...

Leo: Didn't understand fiction.

Steve: They had no concept of fiction. And so they thought that they were documentaries of...

Leo: To the moon, Alice. Ricky. Yeah, they thought that was real. They didn't - they thought they were watching documentaries. I don't remember which book that was, either, but that was a great idea for a story.

Steve: It was a movie. Tim...

Leo: Burton?

Steve: No, the comedian. Boy, I'm blanking on everything.

Leo: Oh, oh, I know what movie that is. That was a great movie.

Steve: It was a fun movie.

Leo: Tim Allen. It was a Star Trek movie except it wasn't.

Steve: Yes.

Leo: That was actually a great movie. What was the name of that?

Steve: Sigourney Weaver was there, and a bunch of others.

Leo: Wonderful movie.

Steve: It was fun.

Leo: Yeah, I forgot about that, yeah. Well, we'll keep an eye on this. You know, there's also some real benefits, let's point out. We showed a video yesterday, or Sunday on TWiT, of the President of Argentina speaking at Davos. And of course what Davos saw was simultaneous translation, which kind of took all the life out of what he was saying. And then Alex Lindsay came up with this, a deep fake of it with true translation and his mouth moving in sync with the English language.

Steve: Wow.

Leo: And spoken as if he, you know, in his own way, matching his own intonation and prosody, they call it, and it was really much better. So we're going to see some amazing things, some very valuable things.

Steve: Well, and so much of the content that Netflix has is in multiple languages.

Leo: That's right.

Steve: And if you're not watching the native language of the movie, you know, your subtitles...

Leo: And the dubbing is terrible, yeah.

Steve: Yeah. And so imagine if they could run their content through that and, like, fix it.

Leo: That's just around the corner. I mean, literally this year kind of thing.

Steve: Yeah.

Leo: Yeah. "Galaxy Quest." That was the name of the movie.

Steve: Yeah, "Galaxy Quest." Yes, yes, yes, yes.

Leo: Thank you, chatroom. Thank you, Discord.

Steve: So Matthew Burrell said: "Quick guidance question, please. What three to four computer languages should I learn? That as a kid graduates high school and looks to start a business. That's mostly ground-up, open source, secure, from server side, that can do almost it all, et cetera, backup, database, et cetera..."

Leo: I can't wait to hear your answer.

Steve: "...to web interface, basically website, login, manage clients, database, other, et cetera. Is there a good platform to start from like Synology or something that those languages could be built on top of? Thank you for all your knowledge, guidance, and all that you do."

Well, Matthew, I presume that you're describing yourself here. So you're a young person who is interested in computing technology and want to create intellectual property with computers and eventually support yourself. What you need more than anything is knowledge and experience. I told a story many years ago that had a somewhat surprising moral. The story was about my misadventures surrounding my construction of a sonic beam weapon which, being a high schooler at the time myself, I had named "The Portable Dog Killer." No dogs were killed.

Leo: It did not kill dogs. It just chases them away.

Steve: That was just - that was my name. The moral of the story was that all sorts of interesting and unexpected things transpired, but only because I was actively doing things. I was not sitting on my butt playing videogames. Okay, so we didn't have video games back then. But there were still plenty of similar ways that my peers managed to burn away the seemingly endless hours of their day not learning anything, not pushing themselves, and rarely experiencing anything new. I really didn't have any choice since I loved electronics back then as I love computers and computing today.

So if you truly love computers, being active, not passive, is the key. Turn off the videogame that someone else created and start figuring out how to create your own stuff. And more than anything, don't let having no idea what you're doing in the beginning stop you. That's not where you stop. That's where everyone starts. So pick a language, any language. It really doesn't matter which one. Python is nice, general purpose, easy to get going with, lots of help available online, and it can probably take you anywhere you want to go. Figure out how to get it to print "Hello, world!" and you'll be off and going. Then choose another problem that's not much harder than that, and solve that one. And so on. And before you know it, you'll be programming. The key is start.

Leo: Do it. Get out and do it.

Steve: Do it, exactly.

Leo: Yeah. I'll give you a couple of specific suggestions. I agree with you on Python. Harvard University offers a free online version of its Introduction to Computer Science course, which is excellent, CS-50, five zero. They update it every year. It does, in fact, use Python as its core language. Python's nice because it's kind of like BASIC for us. It's not a language maybe that you would use to write production code in. But because it's interactive and it has a REPL and you can kind of try and see what happens and stuff, it's a great language to start learning with. There is a famous and I think very good book that you can use that's free, it's available, it's out there everywhere, called "How to Think Like a Computer Scientist." And it is more than just Python. It is a Python book, but it kind of teaches you about...

Steve: That looks great, Leo.

Leo: ...kind of the concept. It's really kind of a classic now. And I think that's a really good way to start.

Steve: And Python is on all platforms.

Leo: It's everywhere.

Steve: I mean, yeah.

Leo: It's perfect for you, just as said, because you can start right now. In fact, you can get a Raspberry Pi and run Python on it, and you can be doing stuff instantly, almost instantly. So it's a very good choice. I often tell people not to - just like you. Don't focus on the career or the business you want to start. Just start playing with it because ideas will come to you. This is how you kind of get into it. That's how we got into it is we start playing with it. And if you really love this stuff, as soon as you start doing it, you'll go crazy. You'll go, this is amazing. Look what I can do. I can make it say "Hello" a thousand times or whatever. And you will get excited about it.

If you really get serious about learning how to - it's like, if coding is what you want to do, there's another free book that I recommend called "How to Design Programs," HTDP. It was used for years as an introductory course at Rice and at MIT. It uses a student version of a language called Scheme, but the language isn't important. But they strip out all the complicated stuff so that you can just focus on concepts. And by the time you get through that, you will really be a proficient programmer. And then the sky's the limit. So HTDP. There are courses in fact at EDX.org. EDX has CS50 for free. And it has an excellent two-part course on how to design programs by a legendary programmer, Gregor Kiczales. I took that, and it was a really wonderful course. But, you know, make it - you can start simple. Just go online, get Python, read this book. It even works you through how to install Python and everything.

Steve: That's a perfect book to start with.

Leo: Yeah. Yeah. It's really good. I have a lot of opinions on this, as you might imagine.

Steve: Well, yeah. And I know you've been asked through the years on your radio station.

Leo: And I love coding. It's so much fun. Even if you don't do it for a living, it helps you understand how computers work. You'll be much better at troubleshooting and using computers. And it's a wonderful hobby. I don't do anything serious with it anymore. But I love doing those coding challenges and stuff. It's just - it's like doing crossword puzzles. It's fun.

Steve: Yeah. A listener, DBloor, he said: "Hi, Steve. I'm a computer forensics instructor up in Canada and have been listening since Episode 20-ish and love the podcast. Thanks for agreeing to push past 999."

Leo: Yay.

Steve: "I just wanted to see if you think my hypothesis holds up for a $720-plus flashlight app. Did this app potentially get hijacked? I've had this free flashlight app on my Pixel phone for over a year, as it allows me to control the brightness since the stock flashlight doesn't have this option. It's been great and simple. I think it used to show a small banner ad occasionally, but nothing intrusive. Today I tried to use it, and I got a pop-up video ad play for about 20 seconds before I could use the light. I thought, okay, maybe they need some money to keep development going. How much can the paid version be? I really like this app, so why not chip in a bit?

"$15 U.S. per week! You read that right, a subscription for a flashlight like 4x the price of Netflix! $60/month or $720/year for a flashlight. My hypotheses are, one, the app developer got compromised or hijacked, and someone is trying to scam its users of hundreds or thousands of dollars; or the developer had this in mind all along, hoping to get a handful of users subscribe, thinking a flashlight app couldn't possibly be worth more than $15, not realizing it's a subscription. Either way, wow. Is this what our world has come to? Subscription-based flashlights? Anyway, keep up the amazing work. I recommend this podcast on all my courses. The app is called Simple Flashlight, produced by Simple Mobile Tool, and has one million-plus downloads."

Leo: Wow. Who needs a flashlight app? Every phone does flashlights, built-in.

Steve: Yeah. Except that this app allows variable brightness, which he really likes. He didn't want it to be just...

Leo: And it does Apples and, yeah, everything.

Steve: ...set up to blinding.

Leo: You can do that with Apple, too.

Steve: Okay. The fact that this app has over one million downloads and that it played a 20-second ad video, and that the app is just a once-free flashlight app, strongly suggests

that its original developer, who had acquired a large user base, accepted an offer to sell the app to another party. We covered this happening many years ago, also in the Android app store. The developer would be conscientious and well meaning, perhaps tired of keeping an app updated and current for little to no return. Then someone would come along and offer to buy the app from them outright. The developer of the free app, seeing one last chance to cash in and make some money, would take the deal and turn over his developer keys to its new owner.

The new owner, a scam artist, would quickly burden the app with crap designed to make more money than the purchase price they paid to acquire the app, which was likely not very much. The scammer would figure that all of those million-plus users would run it and generate revenue from the ad. And just as our listener suggested, there might be a few, if only a tiny fraction, who might not be paying attention and who would inadvertently subscribe at this inflated rate. Technically, the app's new owner had done nothing wrong, but neither is this a particularly upstanding way to generate income.

And anyway, that would be my guess is that the app changed hands, and its new owner decided, I mean, it changed hands specifically so that the new owner could squeeze its install base and just, you know, basically kill it. And, you know, with a bazillion apps on the Play Store, who cares if there's one, as you said, Leo, one fewer flashlight app because eventually no one uses it anymore because it wants a ridiculous payment and makes you watch an ad.

Leo: Yeah. I mean, the fact that a guy made a flashlight app tells you that he already kind of a scammer to begin with.

Steve: Yeah. Michael Garrison said: "Hey, Steve. I'm listening to Episode 957 about the Protected Audience API, and I have a question I'm hoping you can help me out with. I work with small businesses who have no interest in putting ads on their site, but I'm wondering whether they can still make use of the new ad functionality. Say a company like TWIT wants to be able to customize what shows they feature on their homepage for new visitors. With the proposed (and abandoned) FLoC proposal, the bitmap of interests stored by the browser were available to the site itself. So if they knew which bits represented interest in space, they could alternatively move the This Week in Space banner higher on the page, or move it below other banners.

"With the Topics API, my understanding is that wouldn't have been possible because the same requester, the ad company, would have to have seen the same browser on multiple other sites, obviously leaving first-party site owners in the dark, probably by design. Now, with the new API, I can't find a solid answer yet on whether the site itself would be able to see what categories of interests visitors might have that are visiting it. I assume it won't be available to the site owners; but if you know one way or the other, I'd love confirmation. Thank you for your great work on the show. Can't wait to see what email system you come up with for communicating in the future."

Okay. My reading and understanding of Google's Privacy Sandbox system, which I should say subsumes both the Topics API, which is part of it, and the Protected Audience API, altogether, my reading agrees with Michael's. One of the significant objections - I remember, Leo, you talking about this on some of the podcasts after FLoC was introduced. One of the significant objections raised against the earlier FLoC - that was the Federated Learning of Cohorts system - was that a first time visitor to a site would be disclosing information about themselves to that site without any previous interaction. And many privacy advocates found that to be a big step in the wrong direction.

The Privacy Sandbox is vastly more complex than FLoC, and it employs that complexity to effectively blind all of the parties so that all information flows into the user's browser, and none flows outward. And when ads are shown, their fetch and display frames enforce a new level of inter-frame and page isolation. The objections to FLoC taught us that websites are specifically unable to learn anything about their visitors. That was a big privacy no-no that FLoC had, and the Privacy Sandbox enforces that privacy, even for the sites users are visiting, because that's what they want. They want that privacy.

Guillermo Garca said: "I have a question about the washing machine bot. Is it safe to assume that this malware is configured to infect this specific washing machine? In other words, is someone writing code for this model? How can malware infect various IoT devices? Or is there a unique one for each make and model? Many thanks, and I'm looking forward to being part of 999 and beyond."

Okay. So I'd suggest that the best answer to that question is kind of an all of the above. In the generic case of scanning the Internet for potential victims, we know that there have been turnkey IP stacks sold into the embedded device market which were later found to contain critical remote code execution vulnerabilities, often in their fragmented-packet reassembly implementation, since that's an example of something that's been very easy to specify and turned out to be surprisingly difficult to implement securely. So it would be possible to scan the Internet for any IP presence that could be compromised by such an attack that might be common to a wide variety of different IoT devices, different makes and models of vendors who had all purchased this same embedded IP stack to start with.

And then we definitely have the frequent and common case - and the washing machine might be part of that, too - of a known vulnerability having been discovered in some specific Internet-connected appliance, after which those devices are directly targeted. And then we have the other frequent case of a patch being made to a widely popular device, and that patch being quickly reverse engineered to start an arms race to see how many devices can be compromised before each individual device's administrator has applied the patch to prevent just such remote takeover.

In the case of the LG Smart Washer, I was wondering myself last week how a remote attacker might have gotten into such a machine in the first place, if that's what indeed happened to cause that 3.5GB of upload bandwidth per day. Any such device would be behind a NAT router that would not be admitting unknown traffic. Now, the washing machine might support UPnP, which would allow it to open a port for incoming traffic. But why would a washing machine need to be publicly visible? Another means of compromise might have been entry through some other means, such as a border router vulnerability, for example, if its owner had enabled remote web administration and a problem had been found there. Which, as we know, are not uncommon.

Then, once inside the network, a scan would likely have found everything on the LAN, and at that point a known vulnerability in that specific washing machine might have been exploited to install a bot. Or the machine might be running a small Linux. So a generic exploit against Linux could install a generic Linux bot, and then it would have joined a botnet. So, you know, any or all of the above could have happened.

Roger Stenerson asks: "Hi, Steve. The Protected Audience API sounds interesting and promising. However, the number one reason I use uBlock Origin and ScriptSafe is to block malvertising. Will the Protected Audience API help in that area? To 999-plus and beyond. Thanks for all you do. Best regards."

Thank you, Roger. Okay. So I'm pretty certain that individual ads, once selected by the web browser, will still be able to run their own scripts within their "fenced frame," Fenced Frame being the name of one of the APIs, the Fenced Frames API. So we should not

expect any added protection from malvertising. Roger's question caused me to do a bit of digging into the related Fenced Frames API. The fencing that's created applied the same sort of cookie and other asset stove piping that Firefox implemented quite a while ago, the idea being that, rather than all cookies and other asset storage sharing a single large database which is indexed by the domain performing the access, thus allowing, for example, an advertiser to access information stored under their domain from any website hosting one of their ads because now each first-party website - I got myself confused. Under their domain from any website hosting one of their ads. That's the way things have been.

What's happening now moving forward, and Google is introducing this with this Fenced Frames API, is that, as with Firefox, each first-party website has its own private database containing anything that any third party might set while at that site. But if you go to a different site, that same third party is now setting its data in a completely separate site for that website. So there's no longer any chance for advertisement scripts to share data across sites.

So that's what we're getting with Protected Audience API. But I'm virtually 100% sure no explicit malware protection. That still isn't something, I mean, Google is protecting their users against any malicious scripting, whether from ads or not. So we have that. But, you know, malware that presents a link that says "click here" for a special discount on your next, you know, on your car insurance renewal, well, you take a risk when you click the ad.

Defensive Computing's Michael Horowitz, who runs a number of sites, one is Defensive Computing, he also has one that's really great about router security, he says: "Steve, regarding the hacked washing machine, if the router supports outbound firewall rules, the hacked device can be blocked from making any outbound network connections; or, depending on the router, perhaps blocked from contacting certain IP addresses or certain domains. Surely, he says, pfSense can do this."

Okay, now, of course pfSense will do this. And since firewall rules can be tied to the machine's fixed Ethernet MAC address in case its IP should ever change, you could even make a firewall rule that would track the machine's IP changing to block it. But I'm not the one with the LG Smart Washer on the 'Net, so I'm not the one with the problem. I was more referring to the typical LG Smart Washer owner who would typically have no idea what was going on with their own network. I'm certain that our Security Now! podcast listeners could readily block this activity. So really that's not an issue.

But Michael added something else that I thought was interesting. He said: "I live in an apartment building with a laundry room in the basement. Both the washing machines and the dryers report their status to the Internet - running, not running, or X minutes until finished." He says: "This was helpful in the pandemic to avoid personal contact." And I thought that was interesting.

Leo: With your washing machine?

Steve: Yeah. Well, because it's an apartment building. We don't know how large.

Leo: Oh, I see, yeah, yeah, yeah, okay.

Steve: But it's a common tool of shared...

Leo: So if you're washing, you go upstairs, and then it lets you know when it's done. Yeah, yeah, that makes sense.

Steve: Exactly. So anyway, I had said last week that I could not imagine why anyone would have their machines online. This is a pretty good example.

Leo: Yeah.

Steve: So if you're on like the ninth floor, and you want to know if the machines are in use before you take the elevator down to the basement and find out that, whoops, they're all busy. So that's kind of cool. I can certainly see a use case for that.

And finally, SKYNET tweeted: "Hi, Steve. Is there really no way for ISPs like Cogent to differentiate between good and bad traffic so that when a DDoS occurs they can null route only the bad traffic? Can you explain why an ISP is not able to do this?" Okay. Could they? Perhaps. The best way to describe it is that doing so, and I'm not kidding you, is beneath them.

Leo: It's not the kind of thing we as an ISP would do.

Steve: That's exactly right. They simply cannot be bothered.

Leo: It's just not worth it.

Steve: I've had about 30 years of experience with ISPs of all sizes, and I've seen that the smaller the ISP, and the closer they are to their subscriber, the more individualized service it's possible to have.

Leo: Right. That's why we love SonicNet. That's exactly right.

Steve: Yep. But the top-tier Internet backbone carriers like Cogent don't need to be bothered with those details, so they aren't.

Leo: In the words of Lily Tomlin, "We don't care. We don't have to."

Steve: Exactly. If some traffic is causing their downstream equipment any trouble whatsoever, they'll simply drop that traffic as far upstream as it's possible to do so.

Now, the other change we've seen since the first early attacks is in their blockability or lack thereof. The days of the simple ICMP, the TCP/SYN packet, or UDP reflection floods have waned a bit. Back when spoofing source IP addresses was important to hide the traffic source, they were used. They still exist, but they've largely been replaced by non-spoofable HTTPS query floods. And those require highly specialized services such as those we often talk about offered by Cloudflare and others, to block. So these attacks can no longer be selectively blocked by simple firewall rules. So, yeah. Some ISPs like Cloudflare can. Lots behind, you know, who are just, you know, if you're just getting

generic traffic from the Internet, you're going to get flooded, and your ISP's going to say, oh, sorry, and pull the plug on you until the flood stops. That's the way of the world these days.

Leo: But you could get something like Cloudflare or Amazon CloudFront in front of your IP address and protect yourself from that.

Steve: Yes. Yeah. Now, you're paying a price for the protection.

Leo: Right.

Steve: So you're getting connectivity, and you're getting protection both.

Leo: Yeah. I think Cloudflare has a free tier. I don't know if it would work for what you want it to.

Steve: They actually do have a free tier. You're right. And I'm not sure...

Leo: It's very good, I think, yeah.

Steve: ...how much - yeah, yeah. Okay. And lastly, a note about SpinRite since we appear to be for the moment on the cusp of SpinRite's imminent release. So I thought I'd update everyone very briefly. As I planned, after last week's podcast, as I said I would, I finished the work on identifying and patching the known-buggy AMI BIOS which handled USB-connected drives. And after some verification and testing, later in the week I posted the next incremental release of SpinRite.

Leo: Oh, boy.

Steve: The overall reaction within SpinRite's testing community was jubilation since, I mean, it was - I got so much, you know, yay, since SpinRite had now lifted what I had been feeling, and I expressed last week, as my previously heavy-handed 137GB clamp on any and all USB access. But it wasn't long before reports of new SpinRite crashing began to be seen. People were running SpinRite on their larger drives plugged into a USB port, and SpinRite's own attempt to execute an illegal opcode capture screen began popping up. In other words, something somewhere, a bug in the BIOS was causing the BIOS to execute an illegal opcode; and SpinRite, which traps those things, popped up a notification saying, whoops. Something is not right here. And it brought everything to a halt.

Well, it turned out that HP and Lenovo and other BIOSes on older machines were also being found, unfortunately by SpinRite's testers at this point, to be buggy; and they were altering main memory and causing application crashes. SpinRite's ability to patch the flaw that we found in those AMI BIOSes to allow them to then safely work past 137GB was a fluke which just happened to work. I couldn't believe it when Paul Farrer put some NoOps in the BIOS and suddenly it worked past 137GB. Again, now I know why because I completely reverse-engineered that aspect of the AMI BIOS. I see what it was doing. I

understood why it was a solid fix, as it turned out. And I added that code to SpinRite. SpinRite now patches the AMI BIOS, and then it works.

But in general, altering something as significant as an access size limitation would not be expected to be simple. And it turns out that HP BIOSes are in ROM, so they're not even patchable. Anyway, I have a new plan which I will be starting on tomorrow. I think it's going to work. So I'll have news of that next week. I think I know how to solve this problem, even though it has really turned out to be a sticky wicket. But so many people are so excited to have this ban lifted, I mean, I could just simply put the clamp back on as it has been up until last week, and we'd be safe. But some of our listeners would be unhappy. So I think I've figured out how to slice this thing just right, and everybody will have a win.

Leo: And this is why, when I code, I don't write it for any general purpose computing of any kind. There's too many things out there that can go wrong. I just don't want to deal with that.

Steve: When Peter Norton had me up for lunch to Santa Monica and told me he wanted to buy SpinRite, he said: "You know, Steve, it's the most requested feature for the users of the Norton Utilities. They all want it. So now I want to buy it from you." Obviously I told him no, which was the best business decision I ever made. He said, and we were very high in a tower in Santa Monica, and so he looked to the south, because that's where I was located, and he said: "When I first heard about SpinRite," he says, "I thought I was going to look out there and see a big mushroom cloud because you can't do safely what you were doing." He said: "It can't work." But he said: "Somehow you did it. You pulled it off." So, yeah, that was 35 years ago, and I'm still pulling that off.

Leo: Still pulling it off. And it ain't easy, let me tell you. But, you know, I think you probably appreciate being able to do it all by yourself, rather than have a team of people and having to kind of get that code to work with this code and all of that. There's just too many problems.

Steve: Actually, I have the best of all worlds. It's me in my little hovel, my little cave, and hundreds of testers. We have 800 people, I think it was 487 people downloaded the most recent release.

Leo: Nice.

Steve: And then ran it. And oh, my god, is that important. So it's just perfect. And we've got great communication. It's just, it's ideal. And, boy, I can't wait to get this done and started on SpinRite 7.

Leo: Nice.

Steve: Because it won't have any of these problems because it won't have any BIOS. Thank god we're getting rid of the BIOS.

Leo: Although that was the thing; right? You were able to do Interrupt 18 and let the BIOS do all the hard work; right?

Steve: It's why SpinRite was compatible for so long.

Leo: With everything; right.

Steve: Was that it was hiding behind the BIOS, and the BIOS would deal with all of these problems.

Leo: Right, right, right. Now you've got to do it. Now you've got to do it. Which is better in the long run, of course.

Steve: Oh, Leo, it's so fast. It turns out that my half a terabyte per hour estimate was low. SpinRite is doing better than that.

Leo: Nice. That's fantastic.

Steve: It's suddenly really practical.

Leo: Can't wait. So here's how you get it, folks. Go to GRC.com. Now, admittedly, you're getting 6, not 6.1. But this way you're in, you're part of that team of people who are helping Steve make this the best product ever. And you will get a free copy of 6.1 when it comes out.

Steve: And if you get it right now, you can use it to crash your machine, if you have a buggy BIOS and plug in a big drive.

Leo: We call it the Buggy BIOS Tester. See, I'm thinking. You have ValiDrive and you have Buggy BIOS Tester. It's great. It's perfect. Actually, ValiDrive's another reason to go there and make sure the thumb drive you're buying actually has what it says it has for storage. And so many other things. And those are all free. ShieldsUP!, I mean, he does so much great work at GRC.com.