Recall's Re-Rollout

Description: We have the full story about the Linux remote code execution flaw. What bad stuff can happen if a domain escapes control even briefly? What social media platform is now in Russia's Roskomnadzor crosshairs? Update VLC to eliminate a potential remote code execution flaw. Tor merges with Tails for greater efficiency. Telegram announces that it will now obey court orders to disclose information. Interesting info from Bobiverse's author, and some early feedback about Peter F. Hamilton's latest novel. How to keep Windows from re-asking to set up an already setup system. And Microsoft is re-rolling out Recall. Have they actually addressed the valid concerns? Or is this just more lipstick on a pig?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-994.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-994-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. The full story about the remote code execution on Linux he talked about last week. We now know what it was. It's not as serious as it seemed, but it could potentially be a problem for a lot of people. What social media platform is now in Roskomnadzor's crosshairs? We'll tell you. You should update VLC. There's a big flaw in it. And Steve takes a closer look at the security in Recall, and the things Microsoft has done to make it safer. Can you put lipstick on a pig? Maybe you can, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 994, recorded Tuesday, October 1st, 2024: Recall's Re-Rollout.

It's time for Security Now!, the show where we cover your security, your privacy, your science fiction reading online with this guy right here, Mr. Steve Gibson of GRC.com.

Steve Gibson: And Leo, we actually do have actually a little bit of sci-fi from John Slanina.

Leo: JammerB.

Steve: Famously known as JammerB.

Leo: JammerB. You know, JammerB of course was our studio manager, has since retired. And I know he's watching right now. I have a little JammerB corner in the

studio. The very first time I met him he brought me that telephone, you know, the one with the "Hello, Central, give me..." you know, the thing you hold to your ear.

And then the last time I saw him he gave me the Macintosh, the original Mac 128K, and he had set it up so it would run. And he texted us and said, "If Leo runs Load Runner in the background, it's got a great active screen." It's actually playing Load Runner right behind you. So John is, even though he's not in the studio, he is memorialized in the hardware behind me. He's also memorialized in one other way. I have him saying "Hey."

CLIP: Hey, hey.

Leo: Because he used to, anytime somebody swore, I don't think it happened on this show very often, but he would get all upset. So he recorded this for me.

CLIP: Hey, hey.

Steve: Your own personal FCC.

Leo: Yeah. Hey.

Steve: Hey.

Leo: What's coming up this week on Security Now!?

Steve: We have the full story about the Linux remote code execution flaw.

Leo: Oh, good.

Steve: Which we previewed with some unknowns and questions and just a little skepticism. But, you know, why was there controversy? We're going to find out. We're going to look at what bad stuff can happen if a domain escapes one's control even briefly. What social media platform is now in Russia's Roskomnadzor crosshairs? The need to update VLC, the very popular VideoLAN media player.

Leo: Oh, I use that.

Steve: To resolve a potential remote code execution flaw there.

Leo: Okay.

Steve: Tor and Tails have some news. Telegram has some news. Also we've got some interesting info from Bobiverse's author; and, as I mentioned, some feedback about Peter Hamilton's latest novel from none other than JammerB. Also a listener provided

some information I didn't know I needed until he offered it, about getting Windows to stop re-asking to set up an already setup system. It's like, what? I already went through this before.

Leo: Yes.

Steve: Anyway, turns out you can turn that off. And Microsoft is re-rolling out Recall. Have they actually addressed the valid concerns, or is this just more lipstick on a pig? Today's episode is Recall's Re-Rollout for October 1st.

Leo: Once a pig, always a pig.

Steve: Always, yeah, that's right.

Leo: Not much you can do to make it less of a pig, but we'll see, we'll see.

Steve: I'm not suggesting anyone that listens to this podcast is going to be excited, but we're going to take a look at it and see how much they should be forgiven for what they first tried to foist off on the industry.

Leo: Yeah.

Steve: And, oh, we've got a great Picture of the Week.

Leo: I only see the title. I haven't seen the picture. It's in front of me. We'll see it together, shall we, in just a moment.

Steve: That sounds good.

Leo: Yeah. Except for those of you who cheat and download the show notes ahead of time, which you can get at GRC.com.

Steve: Actually, the mailing to all of our listeners went out last night. This is the first time in 19-plus years that I had the podcast, like, actually finished on Tuesday.

Leo: Did you have a hot date or something?

Steve: I just started early, and everything kind of came together.

Leo: Okay.

Steve: So, yeah, those people who have chosen to sign up for the Security Now! mailing list got - in fact, one person wrote back and said, hey, this is great, I can read it, so I'll have an idea what you guys are talking about tomorrow.

Leo: Prepare for the show the night before, that's a good idea.

Steve: Do your homework, that's right.

Leo: Well, and we are sitting here in Petaluma, California, rapidly approaching 100 degrees. It's 96. And I have a - I will ring this bell when we get to 100.

Steve: Oh, good.

Leo: Just some old-fashioned radio fun; okay? All right, Steve. I am ready. I am going to scroll up on the Picture of the Week, and we will look at it together. Are you ready? [Fanfare] "Electrician Wanted." I don't get it, but it's funny.

Steve: Keep going. Keep going. Keep going.

Leo: Oh, there's more. "Experience required this time." Okay. Maybe you'd better describe. That is pretty good. The caption makes it, Steve.

Steve: Yeah. So, okay. So what we have is a green wall, and inset is some sort of an electrical, presumably high-tension wiring situation. The doors...

Leo: You can see the wires hanging out there.

Steve: Yeah, the wires are clear, and the door's been left ajar, apparently as a consequence of what recently happened. Now, imagine - it really is good - if somebody was wearing hard-soled shoes, and they exploded. Well, the shoes, the soles of the shoes would keep the ground at its original color where they were. But you'd get this singed look like everywhere around.

Leo: Basically, the guy exploded in a puff of greasy black smoke, and that's all that's left. Holy cow.

Steve: So, yes, they're looking for a new electrician because we can see what happened to the last one.

Leo: Not good.

Steve: And they're saying, you know, make sure you know what you're doing because, you know. And believe me, if you walked up to this panel, looking down and seeing the

remainder of this guy's shoes, the previous electrician, you'd be very careful with which wires you touched.

Leo: Very nice. I like it. Well done, Steve.

Steve: Hey, thanks to our listeners. They're out scouring the Internet, finding these goodies. And in some cases, you know, they're like walking past something, go ooh, this would be a perfect picture for Security Now!.

Leo: Always be thinking.

Steve: And they take the pictures themselves and send them in.

Leo: Yup, always be thinking Picture of the Week.

Steve: Thank you, thank you, thank you. So we have news of that somewhat controversial, unauthenticated, meaning you don't have to log in or do anything, Linux remote code execution vulnerability which we discussed last week. Simone Margaritelli began his widely anticipated and still clearly annoyed expos, which he posted late last week, by writing: "Hello, friends. This is the first of two, possibly three (if and when I have time to finish the Windows research) write-ups. We'll start with targeting GNU/Linux systems with an RCE." And we know that's Remote Code Execution. "As someone who's directly involved in the CUPS [C-U-P-S] project said: 'From a generic security point of view, a whole Linux system as it is nowadays is just an endless and hopeless mess of security holes waiting to be exploited.'"

He ends the quote, and he says: "Well they're not wrong. While this is not the first time I try to more or less responsibly report a vulnerability, it is definitely the weirdest and most frustrating time as some of you might have noticed from my socials, and it is also the last time. More on that later, but first."

Okay, so first, to interrupt him for a minute, that acronym "CUPS" is the abbreviation for the Common Unix Printing System. It's a modular printing subsystem for Unix-like computer systems, including Linux. So the Hacker News reported on what Simone Margaritelli revealed by writing as following. They said: "A new set of security vulnerabilities has been disclosed in the OpenPrinting Common Unix Printing System (CUPS) on Linux systems that could permit remote command execution under certain conditions. Security researcher Simone Margaritelli said: 'A remote unauthenticated attacker can silently replace existing printers' (or install new ones) IPP URLS with a malicious one, resulting in arbitrary command execution (on the computer) when a print job is started (from that computer).'"

So Hacker News said: "CUPS is a standards-based, open-source printing system for Linux and other Unix-like operating systems, including Arch Linux, Debian, Fedora, Red Hat Enterprise Linux, ChromeOS, FreeBSD, NetBSD, OpenBSD, openSUSE, and SUSE Linux."

Leo: I think CUPS is also used on macOS.

Steve: Oh, yes, right.

Leo: Yeah, yeah.

Steve: "Simone identified four vulnerabilities," they wrote, "which have received CVE designations. A net consequence of these shortcomings is that they could be fashioned into an exploit chain that allows an attacker to create a malicious, fake printing device on a network-exposed Linux system running CUPS and trigger remote code execution upon sending a print job.

"Network security company Ontinue said: 'The issue arises due to improper handling of "New Printer Available" announcements in the "CUPS-browsed" component' - which is a service, as we'll see here in a minute - 'combined,' they wrote, 'with poor validation by CUPS of the information provided by a malicious printing resource. The vulnerability stems from inadequate validation of network data, allowing attackers to get the vulnerable system to install a malicious printer driver, and then send a print job to that driver triggering execution of the malicious code. The malicious code is executed with the privileges of the printing user - not the superuser "root."'

"Red Hat Enterprise Linux, in an advisory, said all versions of the operating system are affected by the four flaws, but noted that they're not vulnerable in their default configuration. It tagged the issues as Important in severity, given that the real-world impact is likely to be low. Red Hat writes: 'By chaining this group of vulnerabilities together, an attacker could potentially achieve remote code execution which could then lead to theft of sensitive data and/or damage to critical production systems.'" And I would argue, if you're installing a malicious driver, it can probably do worse than that. But, you know, that's Red Hat wanting to sort of tamp this down a little bit. And there was arguably, you know, it had some need of some tamping.

"Cybersecurity firm Rapid7 pointed out that affected systems are exploitable, either from the public Internet or across network segments, only if UDP port 631 is accessible, and the vulnerable service is listening. Palo Alto Networks has disclosed that none of its products and cloud services contain the aforementioned CUPS-related software packages, and therefore are not impacted by the flaws. Patches for the vulnerabilities are currently being developed and are expected to be released in the coming days. Until then, it's advisable to disable and remove the CUPS-browsed service if it's not necessary, and block or restrict traffic to UDP port 631.

"Benjamin Harris, CEO of watchTowr, said in a statement shared with the Hacker News: 'It looks like the embargoed Linux unauth RCE vulnerabilities that have been touted as doomsday for Linux systems may only affect a subset of systems. Given this, while the vulnerabilities in terms of technical impact are serious, it is significantly less likely that desktop machines and workstations running CUPS are exposed to the Internet in the same manner or numbers that typical server editions of Linux would be.'

"Satnam Narang, senior staff engineer at Tenable, said these vulnerabilities are not at a level of a Log4Shell or Heartbleed. He said: 'The reality is that across a variety of software, be it open or closed source, there are a countless number of vulnerabilities that have yet to be discovered and disclosed.'"

Leo: Oh, well that's okay, then.

Steve: And that's why we're not ending at 999, folks. Countless. We could count our episodes, but we cannot count the vulnerabilities

Leo: Amazing.

Steve: He said: "Security research is vital to this process, and we can and should demand better of software vendors." Oh, also: "For organizations that are honing in on these latest vulnerabilities, it's important to highlight that the flaws that are most impactful and concerning are the known vulnerabilities that continue to be exploited by advanced persistent threat groups with ties to nation states, as well as ransom affiliates that are pilfering corporations for millions of dollars each year." So, you know, that's Tenable's stance on this.

Okay. So this is sort of what we expected; right? If it was a four-alarm fire emergency, there wouldn't have been that controversy surrounding it that was evident when we talked about this last week. In this instance, yes, there are problems. And, yes, they need fixing. But we've seen plenty of CVSS 9.8s, and this collection doesn't rank up there with those. And for his part, Simone still seems, you know, to be smarting over the backlash from his trying to get everyone's attention when he didn't feel that developers were taking it seriously enough.

At the end of Part 1, which is what I shared the beginning of, of his detailed write up - and I skipped that because it's just detail, and I've got a link to it in the show notes for anyone who wants it. Anyway, he summed up Part 1 by writing: "You will maybe be thinking now, 'Wow, that's a lot of stuff to read, code, RFCs, PDFs of forgotten standards, this research must have been so tiring.'" He said: "But in reality this was a weekend worth of rabbit holes. This was the fun part. The actual work, the heavy, boring stuff started when, on September 5th, after confirming my findings, I decided to open a security advisory on the OpenPrinting CUPS-browsed repository and do what to me was the right thing to do: responsible disclosure.

"I won't go into the details of the initial conversation, or the ones that followed. You're free to read them (if they will ever open any of the threads, and you're willing to read 50-plus pages of conversation) or not, and make your own opinion. While the research only took a couple of days, this part took 22. And this part was not fun. I will only say that to my personal experience, the responsible disclosure process is broken. That a lot is expected and taken for granted from the security researchers by triagers that behave like you have to 'prove to be worth listening to' while in reality they barely care to process and understand what you're saying, only to realize you were right all along three weeks later, if ever.

"Two days for the research, 249 lines of text for the fully working exploit. Twenty-two days of arguments, condescension, several gaslighting attempts," he said, "(the things I've read these days, you have no idea), more or less subtle personal attacks, dozens of emails and messages, more than 100 pages of text in total. Hours and hours and hours and hours and effing hours. Not to mention somehow being judged by a big chunk of the infosec community with a tendency of talking and judging situations they simply don't know. Let that sink in for a moment. What the actual F.

"And we're not talking about time spent on fixes while I was impatient and throwing a tantrum on Twitter. The actual fixes (or part of them) started being pushed much later. The vast majority of the time has been spent arguing whether or not these were issues worth considering. While I was trying to report that there's something bad that should be addressed ASAP, the devs were being dismissive (and pushing other code, also vulnerable, for other functionalities instead of fixing) because I dared to criticize the design of their software. While at the same time I was trying to reach out privately to de-escalate and assure whoever was getting offended that my intent was not adversarial.

"To the people that more or less directly questioned my integrity, accused me of spectacularization and of spreading FUD on my socials: I don't do this for a living. I don't need CVEs to get a job, or to prove how good my kung-fu is. Or any attention other than what my projects and research already provide. I don't play InfoSec Influencer like many. My mission was to interrupt the triagers' focus until they re-prioritized. When I saw what I thought was pretty serious was being dismissed as an annoyance, I used the only platform I had plus a pinch of drama as a tool to have them effing re-prioritize. And it worked wonderfully. More fixes happened after two weeks than with all the arguing and talking before. So don't hate me, hate the system that forced me to do that in order to be taken seriously."

And you know, Leo, he's got a point. You know, I mean, we've talked about the downside of the whole open source environment is that it's all volunteers.

Leo: Right.

Steve: Right? Mostly volunteers. There are, you know, like Red Hat is able to employ people professionally to maintain and manage things. But there are people who are busy. If in fact there's the load of defects that, I mean, Linux apparently has them just as much as Windows does, that need to get fixed, then it is a matter of priority.

Leo: There is triage. There has to be.

Steve: Yes, exactly. And, Leo, you can imagine how many less-qualified individuals are in fact reporting specious things that are actually not problems.

Leo: Right, right, right.

Steve: In fact, that's why last week I went to dig into who this guy was, and we saw that, okay, you know...

Leo: He's legit.

Steve: ...he's got some cred behind him. He's been active for a decade and is responsible for finding lots of problems. So he's not nuts. But they don't know that when they're busy, you know, dealing with a lot of reports that probably are less credible. So, you know, his position I think is understandable.

Our takeaway is that some unlikely to be exploitable yet important flaws were indeed found, and they will be fixed in future editions of Linux and BSD code, in their common CUPS subsystems. So Simone did a good thing, and the open source ecosystem is better today for his willingness to push, even though those who were pushed did not appreciate being pushed. Because I'm sure that other people were reading his social media postings and then saying to the devs, hey, what about this? Is this really so bad? So, you know, he used what influence he had in order to try to make them do what he wanted to.

Leo: He's a little annoying.

Steve: Yes. Nobody appreciates having that done to them.

Leo: And some of that is, you know, yes, nobody appreciates that. Unfortunately, people who are attracted to this business often lack certain social skills, shall we say. And he sounds like exactly the kind of nerd, geek, that we run into all the time who's very literal, really takes it seriously, and doesn't know how to apply social grease. A little social grease would have gone a long way here, perhaps. Is it as bad as he's painting it?

Steve: Okay. So maybe. Reports are that there are more than 100,000 instances of that particular vulnerable surface exposed on the public Internet.

Leo: Yeah, because I have CUPS on all of my machines, including the Macs.

Steve: Yes, but...

Leo: But I don't have the browser installed; right? Is that the key?

Steve: Well, even if you did, and there are - I think it's Linux Mint does have it running by default. So there are Linuxes that have it running by default.

Leo: Oh.

Steve: But you're behind a NAT router. Anybody in a home network behind NAT is going to be safe because it's not going to...

Leo: It's not routable.

Steve: ...that UDP port 631 will not be publically exposed. Okay. So a really nice summary of this was just posted in Risky Business News, which summarized this. And they add a bit of additional interesting details. They wrote: "Threat actors are scanning the Internet for UNIX systems that are exposing their printing ports in an attempt to exploit a set of four vulnerabilities in the CUPS printing component. The vulnerabilities were discovered by Italian security researcher Simone Margaritelli earlier this year and were disclosed at the end of last week. They impact CUPS, the Common UNIX Printing System, an open-source component to allow UNIX systems to function as print servers.

"The four bugs are part of an exploit chain that can allow an attacker to deploy a malicious printer, having the printer indexed by a victim's CUPS server, plant malicious code on the CUPS server inside a PPD file, and have the malicious code from the PPD file executed when a user launches a print job via the attacker's malicious printer. The exploit chain is, in this order: CVE-2024-47176, -47076, -47175, and -47177.

"Besides Margaritelli's write-up explaining how the four bugs work, other analyses on the four are also available, which suggests the credibility of this, via Akamai, Rapid7, Elastic, Tenable, Qualys, Datadog, and AquaSec. The bugs received a lot of attention and were extremely over-hyped over the past week after Margaritelli posted about them on Twitter

before patches were released. Let's just say" - and this is Risky Business News writing. "Let's just say they're not as bad as they were made out to be. They don't impact all Linux distros - only a few, actually. They're only exploitable within very limited scenarios, and the 9.9 CVSS score should have been lower. Yes, they're bad bugs that are easy to exploit, but they're not the Linux world-ending kind, like Heartbleed, for example.

"But regardless of their severity and all the weird conditions needed to exploit the bugs, threat actors don't care. After Margaritelli and others published proof-of-concept code at the end of last week, threat actors began scanning the Internet for UDP port 631, which is the port..."

Leo: And they use Shodan and things like that to do that; right?

Steve: Yes.

Leo: Okay.

Steve: Well, and their own scanners.

Leo: And they can run a scanner, sure.

Steve: Our guy Marcus Hutchins was the one, he posted that he scanned the 'Net himself and found over 100,000 instances.

Leo: Yeah, you could use Nmap or something like that, too.

Steve: Exactly. Yeah, and there are now high-speed scanners that do parallel scanning en masse.

Leo: Signing that, yeah.

Steve: So they wrote: "If this port is exposed on the Internet, then bad things are going to happen to your CUPS server in the coming days." And they finished: "Even if CUPS ships disabled by default on most distros, according to Shodan, there are currently over," and they quoted, "75,000 systems running CUPS exposed over the Internet, which is quite an attractive piece of pie if you're an attacker. Other scans have these numbers at over 107,000, but they could be even bigger than this. Mitigating the vulnerability should be pretty easy. Just disable, remove, or update CUPS. You should not be running that anyway," they said.

Leo: Okay. Interesting. Yeah, he seemed a little whiny. And publishing a proof of concept so early is also problematic; right?

Steve: Yes. I would argue, yes, that the patches are not out yet. They're still happening. And as a result of him jumping up and down and screaming, it brought a lot of attention

to this. And proof of concepts are immediately deployable by people who are scanning. So unfortunately, the upshot of this is that people will get hurt, given that those are true instances of CUPS which are exposed on port UDP 631. As we know, there's a lot of port reuse on the Internet. So it could be some other type of service that is listening or, you know, who knows what.

But still, likely a bunch of systems are going to be hurt. And that's unfortunate. You know, that is a sad consequence of the way we're doing things now. But it's also foreseeable; right? I mean, you know, some guy, as you said, who is impatient and clearly pissed off about the way he feels he was treated by the devs, not escalating this to the degree he wanted it escalated. Then, you know, let's loose too soon, and the result is not what he would have chosen in the beginning.

Leo: This is a big problem in open source is that we have a lot of people with limited social skills for a variety of reasons. Some of them are neurodivergent; some of them are just jerks. And we all have to work together. And not everybody's good at working together.

Steve: Well, Leo, it's a microcosm of the Internet.

Leo: Yes, we're humans.

Steve: You know, where don't you find that on the Internet?

Leo: Exactly. Good point.

Steve: You know, it's just humanity.

Leo: Yeah. Software requires an unusual amount of collaboration, especially open source software. More than we're maybe all used to.

Steve: And it really does require check your ego at the door.

Leo: Yeah.

Steve: I mean, one of the things that I have found that's worked best for me is like just putting the software out there and asking the people, as has happened over in GRC's newsgroups, find my problems. Find the things I screwed up. Find the things that I didn't get right. You know, I know how to use it, so it works for me. And, you know, sure enough, these guys are wonderful about finding stuff that I didn't get right. And I don't care. I mean, all I want to do is have the result be the best it possibly can be. My ego is way down the list of things that I'm concerned about. I just want to be able to offer the best software I can.

Leo: And as Keira points out in our Discord, it's not just Simone's ego that might have gotten in the way. There might have been some other egos, too.

Steve: Yeah. Well, again, the devs are, you know, it's probably difficult for us to imagine how busy they are and the fact that there are probably many other people saying that they found this or that wrong which just isn't.

Leo: Yeah.

Steve: And in fact, in the early days of working on SpinRite, I would have gone insane if I didn't have GitLab just to hold all the stuff, all the reports coming in. And I'd just take a deep breath and just go to the next one and take a look at it, see if I could recreate it. Often it's like, oh, cool, someone found something, and I would fix it. Sometimes I just couldn't ever make it happen. And so we'd wait to see if anybody else could. So, I mean, it really is a process.

Leo: Yeah. And imagine what it was like before we had Git.

Steve: Oh.

Leo: And there are still open source projects who use email for their pull requests and things like that. And that's hard. That's really not ideal.

Steve: Yeah.

Leo: Do you want to take a break now, or do you want to keep going?

Steve: Let's take a break. It's a perfect time. And then we're going to talk about what happens if an enterprise briefly loses control of its domain.

Leo: Oh, that's not good. I can see it.

Steve: Turns out it's worse than you would think.

Leo: Not good.

Steve: No. So the news last week was that Ether.fi, a so-called DeFi, as we're calling it now, a Decentralized Finance Platform, was the target of a DNS hijack after threat actors took control of its Gandi account. So Gandi is their domain registrar. On September 24th, by abusing Gandi.net's account recovery mechanisms - and there's no clear detail on exactly how that was done - bad guys managed to switch Ether.fi's registered nameservers over to those that they controlled.

Leo: Ooh, that's not good.

Steve: That's not good. Since Ether.fi received account recovery notification, within three hours the changes had been reverted, and Ether.fi's account had been successfully locked to further prevent tampering. Now, what I found interesting was that in this reporting everyone appears to be breathing a sigh of relief. But a lot can be done...

Leo: Three hours. Three hours.

Steve: Yes, immediately upon the takeover of a domain. For example, valid web server domain certificates can be immediately obtained from any registrar, from any certificate authority, rather, since proof of domain control is all that's required. And due to the fact that, as we well know, certificate revocation is a myth, those certificates will remain valid throughout their two-year life or more.

Leo: That's a little longer than three hours.

Steve: Yeah.

Leo: Yeah.

Steve: Exactly. And not only can those certificates be used to host a spoofed website, if a victim's traffic can somehow be rerouted, but those same certificates can be used to sign spoofed email from the victim domain, and it will pass right through all SPF, DKIM, and DMARC validation. So my point is, it's likely that for commercial entities owning valuable domains, security is more important at their domain registrar than any other single other place. I know that many of our listeners of this podcast have their own domains. So if you were only to use multifactor authentication in one place, I would choose authenticating to your domain's registrar and doing anything possible to limit anyone else's ability to perform malicious account recovery.

It's a little bit like freezing your credit preemptively because you don't want bad guys to be able to apply for credit in your name. I'm, you know, I have - I think I have one account over at Gandi. I have nothing left at Network Solutions, but I'm all over at Hover. And I've got second-factor authentication set up in both of those locations, and I smile every time I have to put my six-digit code in because I absolutely want to know that they're going to make sure that it's me because, again, the last thing you want is your domain to get hijacked.

So, and recall how LastPass suffered that first security event and then told us and thought that everything was fine. But then later the bad guys were able to use some of the information they had gleaned from that first attack to launch a deeper and much more destructive event. You know, that sort of thing might well plague these Ether.fi folks in the future. It may not be all over. You know, they think everything's been buttoned up. But, you know, that brief nameserver switcheroo may have provided the bad guys with everything they were actually after.

Leo: So if you're a bad guy, time is of the essence.

Steve: That's right.

Leo: Make sure you get it all done fast.

Steve: And you can imagine that they were probably poised, knowing that they wouldn't have it for long. But the moment they got the nameserver switched, they jumped on it and probably issued certs at a bunch of different CAs. Who knows?

Leo: Wow. Wow.

Steve: Okay. Roskomnadzor.

Leo: We're supposed to say it together. You ready? You ready? Wait a minute. It's hard with Zoom. One, two, three. Roskomnadzor.

Steve: Roskomnadzor.

Leo: How about this? [Voice filter] Roskomnadzor.

Steve: Oh, that's good. We'll just put that over in your - you're in charge of saying that from now on.

Leo: I'll be in charge from now on.

Steve: That's good. That's really a good voice, too. Turns out that the social media platform Discord is on the way to being banned in Russia, our favorite Russian...

Leo: That's bad. That's where all of our Club TWiT members live.

Steve: Yeah. Our favorite Russian Internet watchdog - Leo, what's their name?

Leo: Roskomnadzor.

Steve: That's them. They just added Discord to their registry, which is the first step in formally blocking access to a service within Russia's borders.

Leo: What did they do to get that?

Steve: They're just, you know, they're not toeing the line. They're not sufficiently obedient. They're not under the Kremlin's control.

Leo: That's why we love them, yup.

Steve: So the Kremlin doesn't want them loose.

Leo: Wow.

Steve: Just a note for users of the extremely popular VLC VideoLAN player. The project just released a patch to repair an integer overflow vulnerability via a maliciously crafted MMS stream.

Leo: Ooh.

Steve: I don't use VLC to receive MMS streams. But if you do, you want to fix that. The update notes that this could at least be used to crash VLC at a bare minimum; and that, although no one had ever created a remote code vulnerability execution, we know that the possibility of that being done cannot be ruled out. If you are using VLC media player anywhere from 3.0.21 or later, that problem has been resolved.

Also, we've had lots of fun in years past looking at the Tor Project, actually the technology of it, which is so cool because it implements a unique privacy-preserving so-called "Onion Routing" technology. For those who have joined us more recently, I'll just briefly recap that.

The Tor system wraps an outbound Internet packet in multiple successive layers of encryption where the private key used to decrypt each successive layer is only known to the specific router to which that "onion packet" will be sent. So after wrapping the outbound packet multiple times, the sender sends this multiply wrapped "onion" to the first router, which is only able to remove the outer layer of encryption to reveal the address of the next onion router in the sequence. It cannot determine - that is it, the first router, cannot determine the packet's final destination nor its contents because that's still hidden by multiple additional layers. And although that first router knows the sender's IP, since it just received a packet from that IP, the second router that receives the forwarded packet does not know the sender's IP. It only knows the IP of the first router.

When that onion reaches the second router, it and only it is able to decrypt and remove that layer of the onion, thus revealing the IP for the third router in the sequence. And that second router only knows the IP of the first router and the third router, neither the originating IP nor the destination IP. So every hop along the way we have protection of the sender, and also protection of the destination until you get to the final router.

Once the third router receives the onion, only it is able to remove that final layer to reveal the packet's actual contents and its true destination, and it has no idea whatsoever who originated that packet since that's three hops back. And onion routers are all about preserving anonymity.

So that clever multilayered wrapping encryption is the essence of the Onion Routing system whose entire purpose is to give Internet users something that is completely lacking from the Internet's normal point-to-point routing scheme, which is a high degree of anonymity for the sender. When we've talked about how the Internet works, typical packets have a sending IP and a receiving IP. And so there's nothing anonymous from a standpoint of IP addresses. Those are typically known endpoint to endpoint.

Okay. So the other component here is the privacy-centric OS project Tails. Tails is an operating system which is bootable from a USB thumb drive. The Tails website bills itself

as "Your secure computer anywhere," and it explains the OS's purpose, writing: "To use Tails, shut down your computer and re-start it with your Tails USB stick instead of starting Windows, macOS, or Linux. You can temporarily turn your own computer into a secure machine. You can also stay safe while using the computer of somebody else. Tails is a 1.5GB download and takes about half an hour to install. Tails can be installed on any USB stick with 8GB minimum. Tails works on most computers less than 10 years old. You can start again on the system's original operating system after you've shut down Tails." So, you know, you pull it out and reboot, and the system comes back normally.

They said: "You don't have to worry about the system having viruses because Tails runs independently from the other operating system and never uses the hard disk. But Tails cannot always protect you if you install it from a computer with viruses, or if you use it on a computer with malicious software, like keyloggers." So don't do that.

"Tails always starts from the same clean state" - clean state and slate - "and everything you do disappears automatically when you shut down Tails. Without Tails, almost everything you do can leave traces on the computer: the websites you visited, even in private mode; files that you opened, even if you deleted them; passwords, even if you use a password manager; and all the devices and Wi-Fi networks that you touched. On the contrary," they said, "Tails never writes anything to the hard drive and only runs from the memory of the computer. The memory is entirely deleted when you shut down Tails, erasing all possible traces."

Okay. Why are we talking about this? We're revisiting these two important projects today because last Thursday under the blog headline "Uniting for Internet Freedom: Tor Project and Tails Join Forces," they announced their merger. The two projects realized that there was a great deal of duplicated effort with managing and fundraising and operational overhead.

The Tor blog said this. They wrote: "Today the Tor Project, a global non-profit developing tools for online privacy and anonymity, and Tails, a portable operating system that uses Tor to protect users from digital surveillance, have joined forces and merged operations. Incorporating Tails into the Tor Project's structure allows for easier collaboration, better sustainability, reduced overhead, and expanded training and outreach programs to counter a larger number of digital threats. In short, coming together will strengthen both organizations' ability to protect people worldwide from surveillance and censorship.

"Countering the threat of global mass surveillance and censorship to a free Internet, Tor and Tails provide essential tools to help people around the world stay safe online. By joining forces, these two privacy advocates will pool their resources to focus on what matters most: ensuring that activists, journalists, and other at-risk and everyday users will have access to improved digital security tools.

"In late 2023, Tails approached the Tor Project with the idea of merging operations. Tails had outgrown its existing structure. Rather than expanding Tails' operational capacity on their own and putting more stress on Tails' workers, merging with the Tor Project, with its already larger and established operational framework, offered a solution. By joining forces, the Tails team can now focus on their core mission of maintaining and improving Tails OS, exploring more and complementary use cases while benefiting from the larger organizational structure of the Tor Project."

Leo: This is so great. This is so great.

Steve: Yeah. This is really good, and makes them both stronger. They finish, saying: "This solution is a natural outcome of the Tor Project and Tails' shared history of

collaboration and solidarity. Fifteen years ago, Tails' first release was announced on a Tor mailing list. Tor and Tails developers have been collaborating closely since 2015, and more recently Tails has been a sub-grantee of Tor. For Tails, it felt obvious that, if they were to approach a bigger organization with the possibility of merging, it should be the Tor Project.

"The team lead for Tails OS said: 'Running Tails as an independent project for 15 years has been a huge effort, but not for the reasons you might expect. The toughest part wasn't the tech. It was handling critical tasks like fundraising, finances, and human resources.'"

Leo: And dealing with people.

Steve: Exactly. Those pesky critters. "'After trying to manage those in different ways,' he said, 'I am very relieved that Tails is now under the Tor Project's wing. In a way, it feels like coming home.'"

Leo: Oh, that's such a good thing.

Steve: So, yeah.

Leo: Have you used Tails? Do you, I mean, I've read about it for years, and I've always been interested.

Steve: And we've talked about it in the past. My use case, you know, I just don't have a use.

Leo: You have to be very adamant about not wanting to be tagged.

Steve: Yeah. I once talked about the danger, I mean, I can't even imagine logging into one of those hotel business centers' computers and doing anything that mattered there because it's like, uh, no. Now, of course you and I are always carrying multiple computers around with us, so it's not like we have to use somebody else's. But, you know, in a pinch, if you were to stick a USB drive in and reboot the machine with your own clean OS, that's probably as good as you can do.

Leo: Microsoft used to offer, and they stopped it, a version of Windows that would erase itself on reboot, every time, fresh version. And I know a lot of business centers used it. And of course it's gone.

Steve: And, you know, there were some add-on packages back in the day. I remember...

Leo: I remember. That's right.

Steve: Yeah. Like sometimes libraries would use them.

Leo: Exactly.

Steve: Where somebody would log on, they could use the system, you know, and any changes that they made would be completely reverted. Basically it would reset all of those changes and always have the system back in a given state.

Leo: Thanks, [Name]. That's it. SteadyState was a Microsoft product, yeah.

Steve: SteadyState, yes.

Leo: Yeah. What a great idea. Why did they stop it? God knows. Because it's Microsoft.

Steve: Well, you can't run Recall in a SteadyState machine.

Leo: We'll get to that in a moment, yeah.

Steve: That's right. Also, one last little bit of blurb here. As we noted a few weeks ago, Telegram's founder and owner, Pavel Durov, was first detained, then arrested in France, after authorities decided to hold him directly responsible for the many abuses known to be flourishing within the totally unmoderated and unfiltered protection of Telegram's service.

Well, France's strategy appears to have worked since Telegram recently made some waves by amending its privacy policy and agreeing to comply with court orders requiring it to share its users' phone numbers and IP addresses with law enforcement. So Telegram's cooperation will now extend to various criminal investigations expanding beyond their previous limit of only helping in terror-related offenses. And as you might imagine, the exodus has actually been something to behold. I saw a couple articles saying that the bad guys were jumping ship in large numbers. So good riddance.

Leo: Good, good.

Steve: Yes. That's exactly what we want.

Leo: And I'm glad to hear it because I like Telegram. And I would like to use it without feeling bad about it.

Steve: Yeah. And I would argue that as long as you're, I mean, okay, so we know that we have privacy absolutists, right, who absolutely feel that zero consequence of using the Internet in any way they choose should be their right. Unfortunately, they're using somebody else's platform. I mean, we've talked about it. For example, employees in a corporation. What you do on the company network with the company computer is the

company's property, and the company has some responsibility for it. So, you know, as we've said, it'd be a good thing to have a little sign posted on the top of the computer screen saying, "Remember, what you do on this network should not be considered private." You know, it's not your network. It's your employer's network. Anyway, so, yes, goodbye, really, really bad cretins from Telegram. We will not miss you.

Leo: Yes. We will not. Not at all.

Steve: So I've got some feedback to share, Leo. Why don't we take one more break.

Leo: Yeah.

Steve: We'll get into the feedback before, and then on the other side of that we'll talk about the Re-Rollout of Recall.

Leo: And YZF Donor reminds me that there is still a commercial program called Deep Freeze that does what SteadyState does.

Steve: Ah, right.

Leo: I remember that, yeah. Not free.

Steve: And they're still around. That's good to know.

Leo: Yeah, yeah, I'm glad to hear that. Although, you know, I think Tails - Benito, our producer, said "The reason Windows stopped doing it is because they can't show you ads if you keep erasing everything." Yeah, that might be. That might be. Tails might be the right way to go on that one.

Steve: One of our listeners wrote: "Hello. I'm a long-time listener and a much longer time developer. Currently I write mostly for mobile and have apps on the Android Play Store. From time to time I receive emails from 'companies' that want to buy my app and my," he says, "[not many] users. But yesterday I received something new. This guy wants to 'rent' my account to publish his own junk. As you can see, he doesn't value my reputation much."

And then our listener George enclosed the note. I've redacted some things. So the email that he received to his Gmail account said: "Good day, GreenSpot. This is Bytom Gaming Hub. We are reaching out to partner with Google Play Console Account owners for a lasting collaboration to publish our app."

Leo: Oh, please.

Steve: "Our compensation plan includes $70 for each app upload."

Leo: Oh, now I know it's a scam. Okay.

Steve: "$10 for each app update, and $50 every seven days while the app is on your account. If you're interested in collaborating with us, please contact us via WhatsApp at," and then they gave their WhatsApp number. "Yours Sincerely, Bytom Gaming Hub."

What occurred to me is that two years ago, in 2022, Cory Doctorow brilliantly coined the term "enshittification."

Leo: Yeah.

Steve: His use was intended to be aimed at a single company's decline in product quality over time. As Wikipedia defines the term, Wikipedia says: "Enshittification (alternately, crapification and platform decay) is a pattern in which online products and services decline in quality. Initially, vendors create high-quality offerings to attract users, then they degrade those offerings to better serve business customers, and finally degrade their services to users and business customers to maximize profits for shareholders." Okay. So Cory didn't define the term to be used more broadly. But it's so tempting to also use the term to describe what we're all feeling, overall, about just sort of the general decline in the quality of the Internet's service as a whole.

So that term comes to mind when we see low-quality apps attempting to pay their way into the accounts of higher-quality apps as a means of riding their reputations. The only reason somebody would pay to have their app offered within someone else's account would be because the value derived from advertising there would be more than the cost of doing so. Of course the overall result is the gradual "enshittification" of the platform as a whole as the valuable reputation of developers is cashed out and watered down to no longer carry the value it once did.

Our listener who shared this was clearly unmoved by the offer. But it is foreseeable that many others would jump at the chance to obtain some additional income from monetizing whatever loyalty their name may have earned. I don't know, Leo.

Leo: That's terrible. That doesn't sound - it seems like there's got to be more to this. I mean, like, there's some - they want to put malware on people's - I mean, 70 bucks?

Steve: Yeah.

Leo: There's something going on here.

Steve: And it would probably be $70 would be all the person would ever see.

Leo: Maybe.

Steve: They would never see $50 per week, you know, ongoing revenue.

Leo: It doesn't seem credible. Yeah, yeah.

Steve: Yeah. Bad. Okay. Another listener, Marv, said: "Hi, Steve. I wanted to give some feedback on the availability of 'Not Till We Are Lost: Bobiverse, Book 5.' After hearing you mention it was published this month, I've been waiting for the Kindle edition on Amazon. And waiting. And waiting. It turns out we Kindle readers will have to wait a few months due to the author Dennis Taylor's agreement with Audible." And so this was signed "Marvin Rhoads, Senior Network Security Engineer." Anyway, so...

Leo: That happens a lot. Yeah.

Steve: And he linked to Dennis's FAQ, where Dennis asks the question and answers it: "Where's the Kindle version?" And Dennis wrote: "Audible likes to have an exclusivity deal with its authors. During negotiations, they'll try for up to a six-month gap before the text versions are produced. The inducements to the author are: Audible pays for the narrator. Audible pays for the cover. Audible does the marketing. Audible offers a much larger advance. Audible is also responsible for about two thirds," he said, "of my total income. So they are by..."

Leo: Yeah, you don't make much on Kindle. That's probably part of it; right.

Steve: Right. He said: "So they are by definition my primary publisher." He said: "Fortunately, my agent, who is a bit of a pit bull, has kept the exclusive period down to four months."

Leo: Oh, good.

Steve: "So the text version for the current contracts, anyway, will always come out four months after the Audible version."

Leo: Oh, good.

Steve: And while I was there on his page I read the rest of Dennis's FAQ; and his irreverent personality, which so many of us have enjoyed in his novels, shows through clearly. Two additional FAQ entries which also provide some additional interesting background are: "Where's the EPUB or other version?" Answer, he said: "Amazon only lists your work in Kindle Unlimited if you go exclusive with Amazon for the electronic version. That means no EPUB or Kobo or Google Play version. Before you ask, KU [Kindle Unlimited] is probably about 25% of my non-Audible revenue."

Leo: Oh, wow.

Steve: And that's, yeah, he says: "And that's still a serious chunk of change. See below for discussion of fiduciary greed."

Leo: So, you know what, I just always assumed that Audible, I mean, Kindle Unlimited was a bad deal for authors, like they would get nothing or a penny or something. So that's actually encouraging. It's a quarter of his revenue.

Steve: And we know from previously looking into this, and I'm sure you'll remember this, how far you read in the book is actually tied to the - they actually get paid per page that you're reading.

Leo: It's pretty hard not to finish a Bobiverse book, I'm just going to say. I don't know about the new one. But, boy, the first four were page turners, they were so good.

Steve: Yeah.

Leo: And I listened to them on Audible. He's got the best reader ever. They were great.

Steve: Right.

Leo: Yeah, you read them on Kindle; right?

Steve: Yeah. I do, because I like actual text. He said: "When I originally self-published Outland, I initially went wide (Kobo, EPUB, Google Play, et cetera). If I made so much as a penny from any of those other channels, I don't remember it."

Leo: Oh, wow. Oh, that's too bad.

Steve: He says: "When I switched to Amazon exclusivity and Kindle Unlimited, my Amazon revenue went up about 20%."

Leo: Well, I think you get some credit for promoting the Bobiverse books. I think maybe he didn't know, but Steve's recommendation was a big part of this.

Steve: We know that it was a huge hit among our listeners.

Leo: Oh, they're such a good book, yeah.

Steve: So that's why I wanted to circle back and mention this. He said: "My Amazon revenue went up about 20%. So there's literally no inducement for me to consider going wide with my novels." And then he says: "Question: So it's all about money?" And he says: "The answer is oh, hell, yes."

Leo: Yeah, good for him.

Steve: He said: "This writing thing isn't a hobby, and I'm not independently wealthy. I have to pay a mortgage, me and my family have grown accustomed to eating regularly, and I'd like the bank to not take my car back." He said: "I literally quit my day job so I could write full-time, which means I can produce books a lot more quickly, but also means I have to be concerned about the financial aspects of my 'job.' So when they wave a wad of bills under my nose, I pay attention. Sorry, that's just the way it is."

Leo: I so understand how he feels about that because people do the same thing to us. They assume that I'm doing this for fun. Which I am. Just because you like something and you're good at it doesn't mean you shouldn't also get paid for it. And it really annoys a lot of people that we have a club, for instance, that charges seven bucks, or that we run ads. This is life. Be a grownup; you know? We've got to get paid. We pay Steve. I mean, I'm sure you love doing this, and you would do it for free.

Steve: I have a wife.

Leo: But I would never ask you to because you deserve to get paid to do this. And so does Dennis Taylor. Good on him for being honest about that.

Steve: Yeah. I liked that, and I thought everyone would get a kick out of his personality showing through.

Leo: Yeah, yeah.

Steve: Listener Ben shared a welcome tip. He said: "Hey, Steve. I recall multiple complaints of Windows 10 asking to be backed up every time there's some sort of update, when many of us already have our own backup solution." And I've heard Paul complain about this, too. He said: "Today I decided to see if there was a way to disable this. Turns out there is."

Leo: Woohoo.

Steve: "Under Settings > System > Notifications and actions, you're able to uncheck the option 'Suggest ways I can finish setting up my device to get the most out of Windows.'" And apparently even after you have finished setting up your device, it leaves it checked on. So Settings > System > Notifications and actions, and then uncheck "Suggest ways I can finish setting up my device to get the most out of Windows." And with any luck, that's never going to happen again.

Leo: No more suggestions. Thank you, Windows. Goodbye.

Steve: Yeah. So Ben, thank you, thank you, thank you. You know, I had never looked, and I had no idea that such an option was available. You know, and I'm also plagued by it incessantly promoting its own solutions and asking do I want to have - would you like a

second keyboard? No. I've got one is all I need. Thank you. I told you that, like, you know, three times already.

Leo: I keep telling you that.

Steve: God. So, you know, it occurred to me that that might be a nice addition to the next release of GRC's InControl freeware. So I made a note of that in the project so, you know, if I ever return to it, I can see about adding that because, you know, how would you like Windows to stop bugging you to, like, set up OneDrive. Yes. Stop bugging me.

Leo: So Settings > System > Notifications.

Steve: Notifications and actions.

Leo: And then...

Steve: Systems > Notifications and actions. Probably one of those little switches down there.

Leo: There's sure a lot of them. Notifications from the app store? No. Print cleanup notification. I don't even know what that is. Notification suggestions. No. Here it is. Setup. No. Security and maintenance. No. Additional settings. You have to really dig because - Show Windows welcome experience. That's it. After updates. Nope, nope, nope.

Steve: There it is.

Leo: And I don't want tips and suggestions, either. So I just turned everything off.

Steve: You know, I got a piece of email, and unfortunately it got lost in the pile, but one of our listeners had a brilliant suggestion. He said: "Steve, why don't you use Windows Server 2022?"

Leo: Right.

Steve: "As your desktop?"

Leo: Because it doesn't have any crapware on it.

Steve: Exactly. And as an MSDN developer...

Leo: You have it.

Steve: I already have it.

Leo: Yeah.

Steve: So it's like, that's just a brilliant suggestion. So yes. Instead of all of this, you know, oh, my god, those flipping tiles and...

Leo: Well, they wouldn't dare do this to...

Steve: ...Solitaire and all that crap.

Leo: ...businesses; right? So they don't turn it on on the business stuff; right?

Steve: No. Amazing. Listener Matt wrote, get a load of this one: "More Experian Woes. Hi, Steve. Because you mentioned some questionable security practice with Experian, I thought I'd mention that I am inadvertently the email-of-record for someone else's Experian account."

Leo: Oh, god.

Steve: He said: "I was an early Gmail adopter and have the Gmail address of my first initial, last name at Gmail dot com. I routinely get messages to others in the world who share my first initial and same last name. Occasionally, someone will sign up for services and enter my email address by mistake, forgetting to add whichever qualifiers distinguish their email from mine." He said: "It's usually harmless, but someone recently signed up for an Experian account with their information and my email address." He said: "Now I receive email messages every time they have a credit alert."

Leo: Oh, my.

Steve: He said: "Conscious organizations have a single-click opt-out for messages, but for me to turn this off I have to log into Experian as that user. This wouldn't be a problem because I could easily reset the account password, as I own the email address behind it. But I don't want to be exposed to any more of their personal details than I already am." He said: "It seems Experian doesn't bother with an email verification loop..."

Leo: All they had to do.

Steve: Exactly, "...when setting up accounts, or at least they didn't when this person set theirs up." Unbelievable.

Leo: Oh, my goodness.

Steve: You know? At this point it's not even clear how they could go about untangling that mess; right? You know, we've looked extensively at how, due to the universal presence of the "I forgot my password" links, the security of our email is really what all of our login security comes down to.

Leo: Right.

Steve: Usernames and passwords and even multifactor authentication are really only just logon accelerators since everything ultimately falls back to email. So in this case, what happens when this account owner forgets their password and attempts to use the "I forgot my password" loop, you know, so that confirmation mail lands in Matt's inbox because they always had it wrong on their account.

Leo: And meanwhile, now they're...

Steve: And now they can't get back in, and they can't confirm, like, that they lost their password.

Leo: That's the other side of it. Meanwhile, there's somebody who's going, I never get anything from Experian. How do I get in? But the thing is, Experian makes it easy to create multiple new accounts. Like almost every time you go, if you want to do a credit freeze, you just create a new account with your last four of your social and your email. And so that's all that happened is that person has abandoned that account and opened another one. Meanwhile, it's still active.

Steve: Wow.

Leo: Wow. Terrible. Horrible.

Steve: Edward McDonald said: "Hello, Steve. I recently updated to iOS 18 and saw where Apple now has an app for their password manager. I wondered your thoughts on it versus some of the other password manager software, like 1Password. Thanks, Ed."

Okay. Since I'm personally hanging back with older Apple hardware, iOS 18 is not an option for me at the moment. But when we talked about this back at announcement time, what I recall was that what Apple was doing was mostly just pulling together what they already had for password management, which was kind of buried and scattered around within iOS. They were pulling it all into one place and giving it a more formal UI presence. So, you know, the presence of Passkeys, and the need now to manage them, increased the need for iOS's password management to be somewhat more explicit. So the value of any third-party password manager, whose primary benefit would be much wider cross-platform, you know, cross-ecosystem credential synchronization, is neither changed nor diminished with these recent changes to iOS 18.

Leo: I agree. I agree.

Steve: They just sort of gave you an icon for it.

Leo: Yeah. And honestly, it's a very secure system, really well implemented, I think; right?

Steve: Yup.

Leo: The only drawback is it's not exactly cross-platform. You can use it on Windows, but I don't think there's any way to use it on Android.

Steve: Right.

Leo: But, yeah, if you're all Apple, why not?

Steve: A listener named "E" asked about our mailing solution. He said: "Hi, Steve. We run a self-coded email system for doing weekly mailshots. We would like to shift to third-party code while remaining self-hosted. Recently, when you described your modernization effort on your email system, I seem to recall that you bought/licensed a system and wrote your own code around that. I looked back at Security Now! transcripts, but I seem to have missed it. Could you put me straight on this point?"

Leo: How? How? We've only plugged it five times.

Steve: And we're about to do it again.

Leo: He ought to give you a cut of all sales from now on.

Steve: Well, the problem is he's not charging me enough, or anybody enough.

Leo: Uh-huh, no, it's a one-time purchase.

Steve: It's only $139, and I feel guilty that that's all I've paid for this thing.

Leo: Don't feel guilty, Steve. You've given him tens of thousands of dollars of publicity. You've sold more of this product than anybody.

Steve: Anyway, it is so good. I was so glad to see this question because, you know, and actually I just had a ton of use of it in the last week. The more I use it, the more impressed I become. You know, okay. So the system is nuevoMailer [N-U-E-V-O-M-A-I-L-E-R dot com, neuvoMailer.com. And as with anything new and sophisticated, I have to admit it took me a while to fully grok the way it works. But the more I've used it, the more I've grown to appreciate its power.

It can be used in a simple production capacity, such as sending out a weekly mailing; or I would describe it as an emailing workstation, which is the way I've been using it as I've been shepherding GRC's creaky old email list through today's hyper spam-focused email climate. Anyway, so again, E, neuvoMailer.com. It is just so great. I've gotten to know its author, a Greek author named Panos. His name actually has about 17 more syllables, but Panos is the beginning of it. And it's just - I'm so happy with my choice.

Oh, and DJ wrote: "I just wanted to let you know that I received the SpinRite 6.1 upgrade email earlier today in my AOL/Verizon inbox. It did not end up in my spam folder." He said: "I've been a dedicated listener of Security Now! since Episode 3, 'NAT Routers as Firewalls.' I'm also a proud SpinRite owner and user, and I've successfully recovered priceless files for friends and family. Even as an avid listener, I shouldn't admit this, but I've recovered some of my own files that weren't backed up. Now, after the latest use of SpinRite, my SSD is transferring data like it's new again."

So anyway, naturally, all of that was music to my ears. Over the past couple of weeks, but primarily last week, as I've just mentioned, I've been working to get 20 years of past SpinRite 6 owners notified of the availability of a no-charge upgrade to 6.1. I finished that work on Thursday. Everything went well, but Microsoft appeared to be unhappy with the level of spam complaints or bounces from emailing to these very old, you know, 20 years ago email addresses. I have a test list of 53 people from GRC's newsgroups who've volunteered to receive various test mailings while I've been working to bring all this up and get it working.

On Saturday - so I did the mailing on Thursday. On Saturday a test mailing to that list of 53 bounced back all, actually it was six of those people whose domains were handled by Microsoft, so Outlook.com, Hotmail.com, and Live.ca. All were rejected from GRC. So I found Microsoft's postmaster tools and asked about the block on our sending domain. Their reply the next day on Sunday was they had no record of any block. So I did another test mailing and, sure enough, none of those emails bounced again.

Leo: It's a miracle.

Steve: But they did go to the users' junk folders. So even though Microsoft let them through the front door, they sent them into the back room. So I would not be surprised, I mentioned at the top of the show that we're just shy now of 10,000 subscribers to the Security Now! list. So last afternoon/evening I sent out the mailing for today's podcast to 9,977 or something listeners. If you didn't see it, and you're a Microsoft user, look in your Outlook.com, Hotmail.com, Live.whatever, com or ca. And if you would do me the favor of marking it as not junk, that would be great because at this point I think that's the only way we have of telling Microsoft, okay, we're sorry, we're not going to do that again, but we did manage to get out 20 years of email. And it's been really fun, Leo, to see people's replies.

Leo: Oh, that's so great.

Steve: They're like, SpinRite? You've got to be kidding me.

Leo: That's still around?

Steve: That's still alive?

Leo: I get that all the time. You're still alive? All the time.

Steve: Yeah. Okay.

Leo: By the way, I said I would ring a bell when we hit 100 degrees? [Bell ringing]

Steve: Oh, my. No kidding.

Leo: We are at 101 here in the TWiT attic studio. Man, I want to go back to the Eastside Studio. Please, where's my AC? All right.

Steve: Okay. One last piece about sci-fi. This was from John Slanina, JammerB. He said: "Hi, Steve. I understand not wanting to start it" - oh, and he's referring to Peter Hamilton's book - "to start it until the series is complete. That's what I do with Frontiers Saga. I like to read all 15 books back to back."

Leo: Oh, wow.

Steve: And he said: "(Three more 'episodes')" - meaning three more books - "(and I can devour Part 3)." And he said: "But it's Peter F. Hamilton."

Leo: He loves Peter F. Hamilton, yeah.

Steve: Yeah. He said: "I'm halfway through, looking forward to rereading it before Part 2 comes out. Enjoying it immensely. I will say it's great to have a book that is hard to put down. I have many things I can be doing with all my free time. I can tell you that getting back into this book is always at the top of the list." And then he signed off: "It's a little weird looking in from the outside of TWiT, but I will continue enjoying all the content TWiT produces. Take care, John."

Leo: Aw, JammerB.

Steve: So thank you, Jammer.

Leo: Yeah, you know what, he did the same thing with the last one. He just basically reads it, puts it down. When the new one comes out, rereads the whole thing. He's an inveterate reader. He's, like you, a Kindle guy.

Steve: Yup.

Leo: And he doesn't mind. He likes to pick it up and do it again. So we miss you, JammerB.

Steve: Yup. I think I'm on my, maybe my fourth reread of the earlier books of the Frontiers Saga. It's, I mean, I kind of know what's going to happen, but the characterization...

Leo: You forget after a while.

Steve: ...is so good.

Leo: Yeah, yeah.

Steve: It's just, I mean, you know, people rewatch movies because they see them as art.

Leo: Right.

Steve: Right? I mean, like...

Leo: Exactly.

Steve: Such beautiful productions. And this guy can really write.

Leo: My only problem is I don't read that fast, and so there are so many things I want to read. And I just - I don't want to reread something because I think, well, I'm missing something else. But you know what, John, you convinced me. I'm going to get the new Peter F. Hamilton, and I'll just reread it.

Steve: I think I'm going to do the same thing. I'm going to read the - I'll read it, and then it's like, fine. Well, and we did that with "Pandora's Star"; right? We read the first one.

Leo: Yeah.

Steve: And then it's like, uh. And then when "Judas Unchained" finally came out, it was, okay, read the first one again.

Leo: Exactly.

Steve: And now we slide right into the number two title.

Leo: I will miss him. John worked for us for almost 20 years. I will miss - John's so funny. I would go into the studio, and he'd go, "Oh, I can't, I want to tell you, I can't

tell you, oh." Because he, you know, he'd read this stuff ahead of time. He loves it so much. You know what, I'm going to read it. I'm going to read it. I'm going to read it. And maybe John will do John's book club because he always liked Stacey's Book Club. We could do John's Book Club and do the Peter F. Hamilton. How about that?

All right. We're going to talk about Recall. And Microsoft's made yet more changes, but is it enough? Steve will have the inside story.

Steve: Lipstick on a pig?

Leo: All right. Speaking of right and wrong, it's time to talk about Microsoft's Recall. Still a pig?

Steve: So our listener Mike wrote: "Leo and Steve. While I can see some value in having a personal AI running from a user-created and selected database, I see far, far, more danger in this both currently and in the future. I believe that it would require a redesigned PC and OS. It could involve partitions or multiple memory devices. It could also involve multiple data incompatible OSes and CPUs, perhaps running in some kind of sandbox. It must be air-gapped from the Internet, and it certainly cannot be connected to a MS account. Authentication would be local only, perhaps with a YubiKey, when querying the AI. It would be independent of any Windows, lacking security functions. An application running alongside but not actually in Windows. Most likely different application for storing and retrieving data, as well. Just doodling some ideas. Signed, Mike."

Okay. So that sort of sets things up here. Way back when the Internet happened, Microsoft had ramped up to compete with AOL, CompuServe, The Source, and other dial-up services at the time. Microsoft had what they were calling MSN, their Microsoft Network. The sudden surging interest in the Internet appeared to take Bill Gates and company by surprise. Windows at the time had local area networking with Microsoft's own LAN Manager and with third parties such as Novell. But there was really no sort of WAN networking.

So they found a TCP/IP stack somewhere, hung it onto the Windows that they had, and put Windows onto the Internet. The only trouble was, the phrase "Windows Network Security" at the time was an oxymoron. And that was the motivation for my own initial entry into the world of online security, with the creation of ShieldsUP! to show people that, if they had previously shared their "C" drive on the private LAN, then now the entire world could see and browse around inside their machine's "C" drive.

The sudden appearance of the Internet represented a discontinuity in the use of Windows. Microsoft was caught off guard without a good solution, so they shipped what they had, despite the fact that it was a total security disaster. In the beginning, when ShieldsUP! was born, my web server was showing its visitors the contents of their hard drives in a browsable tree. It was all accessible publicly, which it's hard to imagine today, but that was Windows on the Internet in the beginning.

So I was reminded of this, by analogy, because Recall represents a similar discontinuity in the use of Windows. This is due to the fact that having an agent locally storing its user's entire computer usage history in machine-accessible form is not something that has ever been done before, and it represents a massive change in the system's security profile. It's not sufficient to say "Oh, we'll just encrypt it," or "Don't worry, it's protected by Windows Hello." Anyone trained in security knows that none of that is anything but feel-good nonsense. It's salve for the masses.

Just as once upon a time Windows had never needed to have any kind of network security that was required to safely attach it to the Internet, Windows has never needed to have the kind of local desktop security that's required to allow it to safely accumulate and protect all of its users' past activity over time. The good news is these fundamental truths were self-evident to anyone and everyone trained in security, and pretty much all of them started screaming and posting when Microsoft blithely dropped a functioning Recall beta into Windows Copilot+ PCs without any sort of protection - exactly as, back in Windows 95, they hooked Windows to the Internet without any preparation.

What's different between now and then is that we've lost our innocence. Today, the world has 30 years of experience with security, and with Windows. And even if Microsoft tends to forget that major new features really do need some peer review, the rest of the world is here to remind them. And thanks to the Internet, the rest of the world has a microphone.

So last Friday David Weston, Microsoft's Vice President for Enterprise and OS Security, posted a comprehensive update on the state of Recall under the title: "Update on Recall security and privacy architecture." My first reaction to what they have done is to judge this as extremely impressive. Microsoft clearly has some big guns who could not have been involved in Recall's initial design. There was no sign of them then. But they are now, and any reading of Recall's new protection system design would have to be prefixed with the statement to the rest of the security industry: "Message received."

Leo: Wow, that's great. That's impressive. Wow.

Steve: Yes. Now, don't read this as, you know, me assuming that I will now be running Recall on my machines.

Leo: Yeah, you'll never use it, yeah.

Steve: No.

Leo: Don't be confused.

Steve: In the first place, only Windows 11 apparently will offer that option, and I'm only now beginning to feel really good about Windows 10.

Leo: Yeah.

Steve: So, you know, I'll be Recall-free for the foreseeable future. Actually I'll probably be running Windows Server 2022, so I'll be stuck there happily. But I know that many of our listeners, their friends, their families, and others whose security they care about will be running Recall. So it's definitely worth updating ourselves on what Microsoft has wrought.

Okay. First off, on the "all or nothing" front, it appears that the option to remove Recall entirely - which our listeners will recall we talked about a few weeks ago - someone at Microsoft said was a bug, not a feature. David is not saying the same. He says, in fact, removing Recall entirely is a deliberate feature.

Leo: Nice. That's huge.

Steve: So, yes. Under that Windows Features and Options, there will be a checkbox. You can uncheck it and say "Update Windows," and Recall, all trace of it, will be gone. So David's posting says, under "The user is always in control," he wrote: "Recall is an opt-in experience. During the set-up experience for Copilot+ PCs, users are given a clear option whether to opt-in to saving snapshots using Recall. If a user does not proactively choose to turn it on, it will be off, and snapshots will not be taken or saved. Users can also remove Recall entirely by using the Optional Features settings in Windows.

Okay. Now, that said, Microsoft clearly wants everyone to turn this on. David's posting shows a screenshot of the Recall offer, at least as it stands today. And of course it's all glowing happiness. The screen that comes up has the catchy offer: "Unlock your photographic memory with Recall." And it reads: "If you allow Recall to save snapshots, an image of your screen will be saved every few seconds. This will create a photographic memory for you of the apps, websites, documents, and images you've seen on your PC."

Then we have three benefits articulated here. "First, easily find what you need. Scroll through a timeline of your snapshots or describe what you're looking for, even text or images within a snapshot. Two, pick up where you left off. From a snapshot, you can seamlessly return to documents, images, emails, and web pages as you left them. And three, you're always in control. You choose if and when snapshots are saved, and only you can access them. In Settings, you can choose which apps and websites to filter out of snapshots, delete snapshots, or change Recall settings anytime." The page concludes with the question: "Start saving snapshots of your screen on Recall?" with the options to "Learn more," or "Yes, save," or "No, don't save."

Okay. That all sounds great, and we didn't expect Microsoft to laden their invitation with any concern over the security of the system's stored snapshots. Right? I mean, after all, it says under the third benefit that "only you can access them." So, okay, then. But here's where we get into the part that impressed me and which made it clear that what is now being presented came from some other place entirely than the initial entirely lame first Recall beta preview. Here's what Microsoft has engineered after clearly awakening to the fact that there really is an awesome responsibility associated with gathering and locally storing all of this potentially very personal and private data.

They highlight three features. First, sensitive data in Recall is always encrypted, and keys are protected. Okay, that's an easy claim, but then they elaborate. "Snapshots and any associated information in the vector database are always encrypted. The encrypted keys are protected via the Trusted Platform Module, tied to a user's Windows Hello enhanced sign-in security identity, and can only be used by operations within a secure environment called a Virtualization-Based Security Enclave." That's VBS Enclave. And I wish it wasn't VBS because that sounds like Visual Basic Script, which is anything but rigorous.

Leo: Microsoft's a master of overloading, I tell you. They constantly do that.

Steve: Yeah. So Virtualization-Based Security Enclave. So they finish this point saying: "This means that other users cannot access these keys and thus cannot decrypt this information." Second, "Recall services that operate on snapshots and associated data are isolated. Within Recall, the services that operate on screenshots and associated data or perform decryption operations reside within a secure VBS [again, Virtualization-Based Security] Enclave. The only information that leaves the Enclave is what is requested by the user when actively using Recall.

"And third, users are present and intentional about the use of Recall. Recall leverages Windows Hello Enhanced Sign-in Security to authorize Recall-related operations. This includes actions like changing Recall settings and run-time authorization of access to the Recall user interface. Recall also protects against malware through rate-limiting and anti-hammering measures. Recall currently supports PIN as a fallback method only after Recall is configured, and this is to avoid data loss if a secure sensor is damaged." That is, the use of a PIN. So you have that as a fallback if the Windows Enhanced Sign-in Security cannot be satisfied because of a sensor failure.

Okay. So all of that means that Microsoft is using its hypervisor-based machine virtualization to create a fully isolated, you know, as isolated a container for this information as is possible without requiring an entirely new hardware design. Microsoft explains what this means under their "Recall security model." And the fact that they actually have a Recall security model, that's new, too.

So they wrote: "Recall snapshots and associated data are protected by secure Virtualization-Based Secure Enclaves. VBS Enclaves use the same hypervisor as Azure to segment the computer's memory into a special protected area where information can be processed. Using Zero Trust principles, code in these enclaves can use cryptographic attestation protocols to safeguard that the environment is secure before performing sensitive operations, such as snapshot processing. This area acts like a locked box that can only be accessed after permission is granted by the user through Windows Hello. VBS Enclaves offer an isolation boundary from both kernel and admin users. So no level of normal privilege escalation gets you across that barrier.

"Recall snapshots are available only after you authenticate using Windows Hello credentials. Specifically, Windows Hello Enhanced Sign-in Security biometric credentials protect your privacy and actively authenticate you to query your semantic indices and view associated snapshots. Biometric credentials must be enrolled to search Recall content. Using VBS Enclaves with Windows Hello Enhanced Sign-in Security allows data to be briefly decrypted while you use the Recall feature to search. Authorization will time out and require the user to re-authenticate access for future sessions. This restricts attempts by latent malware trying to 'ride along' with a user authentication to steal data."

Okay. So I'll just interrupt to note that none of this was present before. What they released earlier wasn't - you couldn't even call it "half baked." It wasn't even warm. They then repeat the various UI features as privacy controls, you know, snapshot saving can be stopped and resumed, snapshots can be deleted, private browsing will never be recorded, et cetera. But what really makes the difference here is Recall's security architecture. And this is properly where most of their effort has been invested.

The core components of the Recall architecture - again, they actually have a Recall security architecture - are the following. So there's Secure Settings. They explain: "A protected data store used within the Virtualization-Based Security Enclave, which stores security configuration data for Recall. To make any changes to security-sensitive settings, a user must authorize the actions taken within the enclave to prevent malicious tampering. In addition, the settings are secure by default, meaning if tampering is detected, they will revert to secure defaults." So it's like, if the system is not sure about anything, it snaps to full security by default. Again, that's proper security design.

Also, there's the Semantic Index. They explain: "The semantic index converts images and text into vectors for later search. These vectors may reference private information extracted from snapshots, so these vectors are encrypted by keys protected within the Virtualization-Based Secure Enclave. All query operations are performed within this VBS Enclave."

Then we have the Snapshot Store. That "contains the saved snapshots and associated metadata, including any launch URIs provided by apps integrating with Recall User Activity API." Now, I'll get to that in a minute because my eyes went, what? Recall User Activity API. This is the first we've heard of an API. They said: "As well as data like the time of the snapshot, title bar string, app dwell times, et cetera. Each snapshot is encrypted by individual keys, and those keys are protected within the VBS Enclave." Again, each snapshot is encrypted by individual keys, and those keys are protected within the Virtualization-Based Secure Enclave.

Then there's the User Experience, "the UI experience that users leverage to find things they've done on their PC, including timeline, search, and viewing specific snapshots." And finally the Snapshot Service. It is a "background process that provides the run time for saving new snapshots, as well as querying and processing data returned by the VBS Enclave. Recall's storage services reside in a Virtualization-Based Secure Enclave to protect data, keys, and tampering from malware or attackers operating on the machine. Recall components such as the Recall UI operate outside the VBS Enclaves and are untrusted in this architecture." Again, somebody really thought this through, and they did this right.

"Because the Snapshot Service," they wrote, "must release information requested by a user by design, a key tenet of the design is to reduce the potential for exfiltration of data outside the normal use of the Recall system. Processes outside the Virtualization-Based Secure Enclaves never directly receive access to snapshots or encryption keys, and they only receive data returned from the enclave after authorization. The authorization period has a timeout and anti-hammering protections that limit the impact of malicious queries.

"The Snapshot Service is a protected process further limiting malicious access to memory containing the data returned from the query outside the Virtualization-Based Secure Enclave. Protected processes are the same technology used to protect anti-malware and the Windows LSA host from attacks. Lastly, the Recall Virtualization-Based Secure Enclave leverages concurrency protection and monotonic counters to prevent malicious users from overloading the system by making too many requests."

Okay. So it should be completely clear that what we have today is no longer a set of SQL database files containing the user's history snapshots that were found lying around in a user's private directory in that initial public preview release. This is an entirely new ballgame. One thing there that caught my eye was the mention of a Recall User Activity API. Huh? What's that?

Some poking around discovered that this is the means by which it's possible to have Recall return to some past situation and allow the user to pick up from there. As a developer, I was extremely skeptical about Windows' ability to do that, since it would have required snapshotting, not just the system's screen, but its entire running context, and that's just not possible or practical in any way. It turns out that this "Recall User Activity API" is the means by which apps which have been modified to be "Recall Ready" can cooperate with Recall to make that sort of rewind-to-a-past-state possible.

For developers, under the heading "Use Recall in your Windows app," Microsoft explains. They said: "For those who opt-in by enabling 'Recall and snapshots' in Settings, Windows will regularly save snapshots of the customer's screen and store them locally. Using screen segmentation and image recognition, Windows provides the power to gain insight into what is visible on the screen. As a Windows application developer, you will now be able to offer your users the ability to semantically search these saved screenshots and find content related to your app. Each snapshot has a UserActivity associated that enables the user to relaunch the content.

"A UserActivity refers to something specific the user was working on within your app. For example, when a user is writing a document, a UserActivity could refer to the specific place in the document where the user left off writing. When listening to a music app, the UserActivity could be the playlist that the user last listened to. When drawing on a canvas, the UserActivity could be where the user last made a mark. In summary, a UserActivity represents a destination within your Windows app that a user can return to so that they can resume what they were doing. To engage with a UserActivity your Windows app would call UserActivity.CreateSession. The Windows operating system responds by creating a history record indicating the start and end time for that UserActivity. Reengaging with that same UserActivity over time will result in multiple history records being stored for it."

Okay. So that explains a lot about how this can possibly work. In short, it doesn't, until and unless the apps the user is running explicitly add support for it. I'm sure users will be able to turn back the clock to look at what they were doing and to read saved screens. But jumping back into an app at that point in time will require explicit support from the app. I'm sure that Edge and Office and Microsoft's Windows apps will all offer this. And it might, you know, become a competitive feature that other apps will need to remain at feature parity with the things that Microsoft is doing. We'll see how that goes.

There's a bit more that I don't want to skip over in the interest of presenting the whole story. Under "Additional architectural properties that are key to security for Recall," Microsoft adds, under "Bound and verified Virtualization-Based Secure Enclaves," they said, "Encryption keys used by Recall are cryptographically bound to the identity of the end user, sealed by a key derived from the TPM of the hardware platform and are performed entirely within the trusted boundary of Virtual Trust Level 1 (VTL1)."

Under "Virtualization-Based Security (VBS)," they said, "The hypervisor provides the secure enclave environment, which loads integrity-verified code into a confidential and isolated TEE (Trusted Execution Environment).

"Recall only operates on Copilot+ PCs that meet the secured-core standard and include the following capabilities by default, which are verified by Recall: BitLocker (on Windows 11 Pro) and Device Encryption (on Windows 11 Home). Trusted Platform Module (TPM) 2.0: The TPM provides the root of trust for the secure platform, management of keys used by the Secure Enclave, and additional platform hardening primitives, such as unforgeable monotonic counters." The point being they know that the Recall data gets stored on the user's hard drive. It will be strongly encrypted at rest.

"Also virtualization-based security and hypervisor-enforced code integrity. Also Measured Boot and System Guard Secure Launch. If a machine is not booted securely, it cannot attest to the system's security state and release keys, which can unseal content previously protected, thus mitigating early boot attacks." And finally, "Kernel DMA Protection against peripheral attacks must be present and will be verified before Recall will unlock."

And finally and significantly, under "Recall security reviews," they said: "In addition to designing and architecting Recall with security, privacy, and responsible AI in mind, we have also conducted a set of thorough security assessments of the feature. This includes the following efforts to ensure a thoughtful and secure approach." They have three points: "First, the Microsoft Offensive Research and Security Engineering team (MORSE) has conducted months of design reviews and penetration testing on Recall. Second, a third-party security vendor was engaged to perform an independent security design review and penetration test."

Leo: Good, good.

Steve: Yes. "And third, a Responsible AI Impact Assessment was completed which covered risks, harms, and mitigations analysis across our six RAI" - that's Responsible AI Impact - "RAI principles: fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability." They said: "A cohesive RAI Learn and Support document was developed for increasing awareness internally, and external-facing RAI content was published to drive trust and transparency with our customers."

Okay. This is so much more than that original collection of SQL files, as I said, stored in a user's private directory, that it should be abundantly clear that today's Recall implementation bears no resemblance whatsoever to the disaster waiting to happen that Microsoft originally proposed.

This is why I felt it necessary to give Recall's Re-Rollout an entire podcast topic of its own. It would not be fair to Microsoft for our opinion of Recall to remain colored by that first impression. The difference between then and now is so stark that I have no explanation for what that first thing was, where it came from, or who did it. You know, it feels like it was nothing more than an innocent first-pass proof-of-concept that some idiot in marketing insisted upon shipping immediately because it was so amazing. You know, yes, it's amazing. But it could also never have been safe, and never could be safe, unless it was also implemented correctly.

Fortunately, the entire security industry rose up and collectively said "What the Actual F" and got Microsoft's attention. What we have now, what is protecting Recall's aggregated user data, is a seriously well-thought-out state-of-the-art security architecture. And they're even, you know, they've even had it reviewed by outsiders.

Now, even given all that, the number one lesson we have learned about security is that there are no exceptions to this rule; that only time will tell whether this will be enough. But at least it looks like it now stands a chance.

Leo: Yay.

Steve: So bravo to Microsoft.

Leo: Yeah.

Steve: They know they have a potential, I mean, earth-changing feature for Windows.

Leo: Yeah.

Steve: And I can't explain what that first thing was. But we really need to forgive them because they got it right this time.

Leo: Did it right this time around. That's really, you know, that's great. It's good news. Very nice. And I'm glad that you were able to come on and give it a once-over and say, "good." Not that you will ever run it.

Steve: I will never run it.

Leo: And [crosstalk] it's really insecure.

Steve: Never say never. I mean, okay, first of all, you know, maybe Windows 12 because, you know, Windows 11 is just one of those like Vista. It's one that you - or 8 - that you just - it's one of those skip-over versions, yeah.

Leo: All right. All right. Steve Gibson. You've done it again, as always, brought together a two-hour and 10-minute extravaganza of security news, and we're so glad that you did it, and we're so glad that you all joined us for it.