Satellite Insecurity, Part 2

Description: What did Apple recently say to the UK? What's Google's "Web Environment Integrity" and why is it so controversial? Who's the latest to express unhappiness over Google Analytics? What happy news did the UK deliver about IoT security that the U.S. has not done so far? Might you be qualified to join the U.S.'s forthcoming Expeditionary Cyber Force? What's the latest on ransomware attack payouts and also on the massive MOVEit maelstrom? And who's the most recent major player to announce the adoption of Passkeys? Once we all have the answers to those questions, we're going to spend some time with our faithful listeners, then wrap up this Part 2 of our look at the current and quite distressing state of satellite insecurity.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-932.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-932-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Get ready. We're going to talk about a lot of things, a farewell to a hacker we know and love, no longer with us, sad to say. We'll also talk about Apple. They're saying, you keep this up, we're leaving the U.K. And a proposal that Google says might eliminate the need for adblockers. That and Satellite Insecurity, Part 2, all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 932, recorded Tuesday, July 25th, 2023: Satellite Insecurity, Part 2.

It's time for Security Now!, the show where we cover your safety, your security, your privacy, and everything else online with this guy right here, Mr. Steve Gibson. Hi, Steve.

Steve Gibson: And basically show you that you have none of the above.

Leo: Yes.

Steve: Despite all of the efforts.

Leo: Which you probably knew, so...

Steve: Which, yeah. And that makes it much more fun and the reason that we're never going to run out of things to talk about.

Leo: That's true.

Steve: We're going to finish our two-part episode today on the topic of satellite insecurity. In our listener feedback section it turns out we've got - I think, when I was first putting this together yesterday, one of our listeners identified himself as in the satellite security industry. And since then I ran across another. So we've got some listeners who are saying, hey, this is great.

But first we're going to talk about what Apple recently had to say to the U.K.; answer the question of what's Google's Web Enforcement Integrity, I'm sorry, Web Environment Integrity, and why it's become so controversial; who's the latest to express unhappiness over Google Analytics; what happy news did the U.K. deliver to IoT security community; and what has the U.S. along those lines not done so far.

Might you, our listener, be qualified - listeners, we have more than one - be qualified to join the U.S.'s forthcoming Expeditionary Cyber Force? What's the latest on ransomware attack payouts, and also the latest on the massive MOVEit maelstrom? And who's the most recent major player to announce the adoption of Passkeys?

Once we have all the answers to those questions laid out, we're going to spend some time with our faithful listeners, then wrap up, as I said, the second part of our two-part look at the current and unfortunately quite distressing state of satellite insecurity. And it's going to be fun because it follows the model of the development of security that we've been tracking now for the 18-plus years of the podcast. And we do have a great Picture of the Week, thanks to another one of our listeners.

Leo: And I have an update from Allyn Malventano, my SSD guy.

Steve: Great.

Leo: Remember we were talking last week about whether, A, you should turn off the swap file on Windows; and, B, if you do have it on, whether you should ever have it on an SSD. And, you know, for years our recommendation was put it on the fastest drive you've got. In fact, you put it on the inner circle of the fastest drive you've got so you get the best performance on your SSD or your swap file. Allyn says, "Hey, Leo, you're both right. Yes, it does add wear. No, it's not enough to worry about," asterisk, "assuming you have sufficient DRAM to handle most tasks that are not constantly heavily swapping to disk."

Steve: You aren't thrashing; right.

Leo: Yeah. "If you are on a very memory-constrained system, swap can quickly become most of the SSD writes. In extreme cases it could wear a drive faster than its rating." He says: "You want me to come on this show with you two and referee?" Thank you, Al.

Steve: Actually, I did have one of our listeners compliment us on the fact that we had a discussion, we obviously had different positions and had a disagreement, but there was no puffery and no one got upset. We just sort of, you know, you said this is what you think, I said this is what - anyway, he said it was really refreshing.

Leo: You never hear that anymore, do you.

Steve: These days, no. It's all pretty polarized.

Leo: So, you know, personally, can you even still turn off the swap file on Windows? I mean, I'm surprised that they still let you do that.

Steve: None of mine are on. They're all turned off. They work great.

Leo: Yeah, okay, you can do that, okay.

Steve: Yup.

Leo: Now I am going to tell you about our sponsor, and then we're going to get into the meat of the show, especially the most important part, the Picture of the Week.

Steve: The Picture of the Week.

Leo: Absolutely. Now, I think, Steve, you have a Picture of the Week for us.

Steve: So this is a great one. I gave this one the caption "Why Reading the Manual Is Always a Good Idea." But it could also have the caption "There's More Than One Way to Skin the Cat." Imagine that you have a sort of an old-school coffee pot, but sort of reminiscent of a teapot, where it's got the main pot and then sort of a, what, a pouring spout spigot, you know, sort of like up and pointing out. Well, the traditional way of pouring coffee from that pot would be to pick it up by its handle and move it over to the cup and tilt it until the coffee runs out of the spout; right?

Well, this picture demonstrates the alternative means of pouring yourself a cup of coffee, or what happens if you try to figure this out and you haven't read the manual, which is we have a guy blowing, he's got his whole mouth over the open top of the coffee pot. He's blowing really hard down into the coffee, which of course forces the coffee up the spout and through a parabolic arc in the air, landing in the coffee cup. And, you know, in this era, this day and age of photoshopping and fake pictures and things, you wonder did this really happen. The coffee landing in the cup looks kind of real. He does have his eyes focused where they should be.

Leo: He's aiming. He's aiming.

Steve: Yeah. Yeah, he's like having to - because you have to, yes, he's got to meter his blow in order to get the velocity correct, or he's going to overshoot or undershoot. I'm sure this was not the first take of this particular operation. Anyway, if this is real, I salute him. Congratulations. And of course he's going to have a mess because as he stops blowing, then all the coffee that's in flight is going to end up being a mess. But if this was an actual photo, stop-action, caught mid-stream, congratulations. Definitely a great candidate for our Picture of the Week. Well, and actually it made it into the Picture of the Week. And, boy, Leo, I've got some other ones, some good ones coming.

I had to share a bit of sad news with our listeners. You already know. The wider world received the news at the end of last week that the famous and long-since reformed hacker Kevin Mitnick had quietly passed away the previous Sunday, on July 16th, which was just three weeks shy of Kevin's 60th birthday. He had been fighting pancreatic cancer for more than a year, and he left unfortunately behind his wife and unborn baby. So I know that, Leo, you were good friends with Kevin. He was on, back in the TechTV days, The Screen Savers a number of times, often with Wozniak, who was also a friend of Kevin's.

Leo: Yeah, we have - I played, on this Sunday on TWiT, and I guess that's why you know that I know, I played a little clip from The Screen Savers where we had Kevin come on after eight years he'd been banned from using the Internet because of his conviction and his jail time. And his probation had ended, and he came on The Screen Savers to use the Internet for the first time. So we brought in Emmanuel Goldstein from the 2600 Magazine, famed hacker. He was the devil on Kevin's left shoulder, and Steve Wozniak the angel on his right shoulder. And Steve, by the way, brought him a brand new MacBook to use for...

Steve: They had a PowerBook.

Leo: Yeah, very nice of him. And so you can see that. It's on YouTube, if you search for Kevin Mitnick and The Screen Savers.

Steve: And it had a great cartoon. Woz had had one of the artists at Apple draw a neat cartoon where it showed the PowerBook on a table just out of reach from Kevin, who was behind bars, trying to, like, poke at it and reach it with a stick or a cane or something from inside his cell.

Leo: It was pretty funny, yeah. He wasn't allowed to use anything, you know, not just a computer but a smartphone of any kind.

Steve: Well, you know, Leo, he could have taken over the world if he'd had a smartphone, from his cell.

Leo: I don't know if he was joking, but he said he couldn't even use an electronic toilet. I don't know if that was a joke or serious.

Steve: Wow.

Leo: Yeah. Well, you know, it was federal crime. I think, you know, there was some agreement that he was perhaps over punished and over prosecuted for a relatively moderate crime. But anyway, he was freed. And it's sad to see his, you know, finally having a family after all that time, to miss out on that is very tragic. He was a really sweet guy. I really liked Kevin.

Steve: Yeah. So last Thursday BBC News carried a story under the headline "Apple slams UK surveillance bill proposals," but the first line of their piece was a showstopper. It read: "Apple says it will remove services such as FaceTime and iMessage from the UK rather than weaken security if new proposals are made law and enacted." So, okay. I mean, we've sort of been waiting to hear from Apple; right? We've heard from Signal, and we've heard from WhatsApp.

So as we know, since we've been tracking this super-engaging struggle between the commercial forces who want to enforce absolute privacy, and those in the governments who are wishing to make privacy conditional, the UK is seeking to update their Investigatory Powers Act (IPA), which was originally created in 2016. So now, you know, seven years later they want to update it. It wants to require messaging services to clear their security features with the UK's Home Office before releasing them to customers. The Act also lets the Home Office demand that security features are disabled, without telling the public. And under this forthcoming update, this would have to be immediate upon the Home Office's demand.

So WhatsApp, Signal, and all the others have previously expressed their strongest possible opposition to this, with Signal making what has been, you know, up to now the strongest public statement, stating that they will simply "walk," as they put it, from the UK. Now, you know, Apple has clearly been in opposition to this, too, but until now it hasn't drawn any such sharp line in the sand. But that's what just happened.

The UK government has just opened an eight-week-long what they called a "consultation" on the proposed amendments to the IPA. The government's claiming that they are "not seeking to create new powers," but only to make the Act more relevant to the current technology. Uh-huh. Apple has submitted its formal nine-page response to this now-open consultation period. Apple formally opposes three things: Having to tell the Home Office of any changes to product security features before they're released; the requirement for non-UK-based companies to comply with changes that would affect their product globally, such as providing a backdoor to end-to-end encryption; and having to take action immediately if a notice to disable or block a feature is received from the Home Office, rather than waiting until after the demand has been reviewed or appealed. Which is the way things are today.

Apple says three things: It would not make changes to security features specifically for one country that would weaken a product for all of its users; second, some changes would require reissuing a software update so could not be made secretly; and, third, the proposals "constitute a serious and direct threat to data security and information privacy" that would affect people outside the UK.

And, you know, remember that what the governments, the various governments here, are asking for is not simply the ability for these various encrypted services to respond to targeted court-ordered surveillance. That's an entirely different ask. What the governments are seeking now is universal surveillance of all communications of all kinds for all of their citizens. And it's hard to argue that that's not new. That's not an update to anything that exists today.

The BBC in their report quoted a cybersecurity expert, Professor Alan Woodward, from Surrey University, who said that technology companies are "unlikely to accept the

proposals." In an understatement. He said: "There is a degree of arrogance and ignorance from the government if they believe some of the larger tech companies will comply with the new requirements without a major fight."

And I think that Signal and Apple have been quite clear that they have no interest in, or need, to fight. In order to avoid breaking any newly enacted legislation, they'll simply pull their services from those regions which enact laws that seek to violate the privacy of their users. Period. You know, fight over. Nothing to fight about. Then we'll see what the voters in those areas think of the fact that their government has essentially denied them these services which they had been having and enjoying with no problem, and now apparently they can't any longer. And we'll also see how the bureaucrats, law enforcement, and intelligence services like not having any secure messaging services available for them in support of their own needs for privacy. You know, what's good for the goose.

So the Home Office told the BBC that the Investigatory Powers Act was designed to "protect the public from criminals, child sex abusers, and terrorists." That's obviously an honorable goal, but the price for doing so is just too high, at least using this technology. So anyway, we've been following this fascinating evolution. And it is interesting that here this professor says, oh, you know, the government's ignorant, they think they can do this. Well, governments create laws; right? And so they can create any law that they want to, but no one's forcing Apple to do something it doesn't want to do. So it'll be interesting to see if, you know, does the UK back down when they realize that these companies are serious? Or is it going to take a period of not having these services available and then, what? Anyway, really, really interesting.

Okay. Four Google engineers have put forth a proposal, unofficially, that immediately generated a huge backlash across the web developer community. Despite the fact, and in some cases perhaps due to the fact, that this proposal was dropped on GitHub as one of the engineer's personal projects, not from Google officially, many Google skeptics see this as Google's sort of backdoored means of sliding this quietly into the stream. But if that's what it was, it didn't work because it quickly hit everyone's radar.

The developers termed this proposal, basically a web standards proposal, Web Environment Integrity. The industry, however, quickly slapped it with the term "Web DRM" and noted that it would instantly provide a means for websites to refuse to offer their content to any browser running an adblocker or to disable adblockers remotely. And given that Google's revenue stream is largely advertising, the fact that this new web standard was proposed sort of "off the books" by four web developers who all just happen to be employed by Google, well, one could be forgiven for questioning or at least wondering about the true motives behind this.

And essentially it does, indeed, amount to Web DRM, a means for enforcing the display of exactly what any website wishes to be displayed by empowering websites to selectively remove all user freedom at their web client end to alter the website's display in any way the website chooses. Now, okay. This is not to say that there could not also be true significant upside user benefits. For example, allowing a banking website to rigorously control what, if any, third-party extensions are enabled when a user visits their site, essentially locking the web browser client in order to enhance the visit's security, well, you could see that could be a good thing. But it's equally obvious that taking this control away from users could be abused by allowing any website to decide, on behalf of their visitors, what browser environments are acceptable.

Okay. The engineer authors start off their description of Web Environment Integrity by explaining. They said: "Users often depend on websites trusting the client environment they run in. This trust may assume that the client environment is honest about certain aspects of itself, keeps user data and intellectual property secure, and is transparent

about whether or not a human is using it. This trust is the backbone of the open Internet, critical for the safety of user data and for the sustainability of" - uh-huh - "the website's business.

"Some examples of scenarios where users depend on client trust include," and they give us four. "Users," they say, "like visiting websites that are expensive to create and maintain, but they often want or need to do it without paying directly. These websites fund themselves with ads, but the advertisers can only afford to pay for humans to see the ads, rather than bots. This creates a need for human users to prove to websites that they're human, sometimes through tasks like challenges or logins."

Okay. Second: "Users want to know they're interacting with real people on social websites, but bad actors often want to promote posts with fake engagement, for example, to promote products, or make a news story seem more important. Websites can only show users what content is popular with real people if websites are able to know the difference between a trusted and untrusted environment."

Third: "Users playing a game on a website want to know whether other players are using software that enforces the game's rules." And finally: "Users sometimes get tricked into installing malicious software that imitates software like their banking apps to steal from those users. The bank's Internet interface could protect those users, if it could establish that the requests it's getting actually come from the bank's or other trustworthy software."

So, yes, there are undoubtedly some valid use cases. But this is a problem, too. Whether or not this proposal ever advances past the controversy created by its appearance, it points to a tension that appears to be developing. Should websites be able to reach across the Internet and exert full control over the experiences of their visitors? When we run a native app on our local computer, we have very limited control over what it does and how it works. We can launch it and terminate it, but that's about it. It's not difficult to imagine that many websites would like to enforce that same level of control.

Anyway, I put a link in the show notes for anyone who might be interested in digging deeper into this specific proposal. Because this thing may just be, you know, immediately shot down like a Chinese weather balloon, it's probably not worth going any further. If it ends up taking hold, we'll certainly be giving it a much deeper look. I mean, I looked at the spec. It uses protocols related to WebAuthn. So it's reusing some of that. It uses public key crypto and this notion of something attesting to the state of the client at the user's end in order to essentially provide Web DRM.

And it was interesting to me that Google said, yeah, you know, websites that have ads are going to - they need the advertisers to know that real people are looking at them. And I'm thinking, uh-huh. And those websites also need visitors not to be able to blind themselves willingly by using an adblocker. So both sides to that argument.

We've noted a number of times that various EU countries have been complaining, and have even now taken to suing organizations within their own borders who are continuing to use Google Analytics, which, they state, potentially transfers private identifiable data outside of their borders. But now this concern has come home to roost with a letter that the Federal Trade Commission, our FTC, and the U.S. Department of Health and Human Services (HHS) have sent to 130 hospital systems and telehealth providers warning them about their obligations to protect their clients' personal health information.

So listen to this. They wrote: "The Office of Civil Rights at the U.S. Department of Health and Human Services and the Federal Trade Commission are writing to draw your attention" - and this was sent to 130 hospital systems - "to draw your attention to serious privacy and security risks related to the use of online tracking technologies that

may be present on your website or mobile application, and impermissibly disclosing consumers' sensitive personal health information to third parties.

"Recent research, news reports, FTC enforcement actions, and an OCR bulletin have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.

"Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to healthcare professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others. Health Insurance Portability and Accountability Act of 1996, reminding us of HIPAA, H-I-P-A-A.

"If you are a covered entity or business associate under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules, with regard to protected health information which is transmitted or maintained in electronic or any other form or medium. The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties, for example, tracking technology vendors, includes PHI, personal health information.

"HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or other violations of the HIPAA Rules. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply. This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies.

"To the extent you are using the tracking technologies described in this letter" - meaning, you know, Meta/Facebook pixel and Google Analytics - "on your website or app, we strongly encourage you to review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information." So, yeah. While this is not the same as the "thou shall not use" commandment that EU countries are issuing to their own local entities, Google has been Analyticizing for the past 17 years now, since 2005, and only now does it appear that people are beginning to say, "Hey, hold on here a second," and just looking at what happens under the hood of these tracking technologies.

Leo, I know that you've covered this. I thought this was interesting, at least the U.S. side of this. The European Union has just approved a draft version of what they are calling their "Cyber Resilience Act." It's a set of new cybersecurity-related rules for IoT devices. The Act passed the EU's Industry, Research, and Energy Committee with 61 votes in favor, one against, and 10 abstentions. Under the new regulations, vendors must - get this. Vendors must ensure their products meet a certain set of criteria before being sold in the Eurozone. Products will have to come with automatic security updates as the default option - yay - must ensure data confidentiality using encryption, and vendors must inform authorities of any attacks. And the new rules are expected to enter into effect by next year.

This is great news for the consumer overall, since any products sold globally, which include the Eurozone, would need to be in compliance. So, for example, U.S. consumers would reap the benefits, as well. And in this case the EU is ahead of the U.S. since all we have managed to get done here so far is to design an attractive shield emblem that will

be placed on any devices that are compliant with a set of standards that don't yet exist. But hey, at least we have a pretty-looking emblem shield.

Leo: Yes. I liken that to shipping the T-shirt before you have the product.

Steve: Yeah, look how pretty this is going to be. We don't know what it means yet. We don't know what you're going to have to do to get one. But don't you want it? Yeah. Leo, let's take a break.

Leo: All right. We did talk about it on TWiG because Stacey, as you know, is an IoT guru.

Steve: Yup.

Leo: And the NIST guidelines, you know, are good. And if they follow those NIST guidelines, I guess, you know, including the thing you and I both care about probably the most, which is over-the-air updates, firmware updates of your IoT devices.

Steve: Yes. In fact, I don't think I talked about it on the podcast, but the Zyxel routers had a problem in April, and they're now all being commandeered into a botnet.

Leo: Yeah.

Steve: Because, sorry about that.

Leo: Can't update them.

Steve: Nope.

Leo: Yeah. So that's a big problem. Not just for you as a user, but for the Internet as a community. Steve, let's go. More to do here.

Steve: So we know you listen to the podcast, so you already have some qualifications. Do you like to travel? See faraway places and wonder what the people there are saying? Enjoy wearing ridiculous camo when sitting in front of a computer? Well, you may be just what the U.S. is looking for!

Leo: Woohoo.

Steve: Lieutenant General Timothy Haugh, the nominee to become the next head of the NSA and CYBERCOM, has pledged to create "expeditionary cyber forces."

Leo: Oh, dear.

Steve: That can be deployed into far off lands to reach important tactical targets in forward locations. So get ready to pack up your laptop and head out.

Leo: Wow. Wow.

Steve: Yup.

Leo: See the world.

Steve: We're not sitting in some bunker in Colorado anymore. No, no, no, no. We're going to update our TSA passport and, that's right, see the world and wonder what they're saying when you get there.

Leo: Wow. That's hysterical.

Steve: Yeah. I mean, it's true. Expeditionary cyber forces. So, fun.

Okay. I have in the show notes a chart showing from the beginning that this started being measured in 2019 to now, the percentage of ransomware payouts that have been made based on the number of attacks. It depicts, happily, a more or less steady drop in the percentage of ransomware attacks which actually result in cash being paid. When Coveware began tracking ransom payment rates at the start of 2019, 85% of ransomware attacks resulted in payments. Today, that number has hit an all-time low of just 34%.

Coveware's report, which was just published on Friday, was titled "Ransomware Monetization Rates Fall to Record Low Despite Jump in Average Ransom Payment." So the news is not all good, but it's great that today only one out of every three attacks results in payment. That sure beats 85% from four years ago. The first three sentences of their report reads: "In the second quarter of 2023, the percentage of ransomware attacks that resulted in the victim paying fell to a record low of 34%. The trend represents the compounding effects that we've noted previously of companies continuing to invest in security, continuity assets" - meaning you're not put out of business completely when your machines are encrypted, continuity assets - "and incident response training. Despite these encouraging statistics, ransomware threat actors and the entire cyber extortion economy continue to evolve their attack and extortion tactics."

Still, good news, down to one out of three. So hopefully that cools things down a little bit because 84% guarantee of payment, that would have been much harder to resist than one third. And there's also, you know, a non-zero chance of the good guys catching the bad guys, which we've seen a number of times.

In an update on the MOVEit mess, Emsisoft reports that the total number of confirmed victims of the Progress Software MOVEit Transfer SQL injection attacks has now passed 380. And Coveware expects that the Russian Cl0p gang behind the attacks will receive somewhere between 75 and $100 million in total. So unfortunately it was a worthwhile attack for those guys to launch. Yeah, and there on the screen is the gradual, you know,

pretty much, it's not a straight line, it's a wavy line, but from 2019 it's been heading downward.

Leo: That's good.

Steve: Basically I think four years ago everybody got caught with their servers down.

Leo: It was 85% payouts.

Steve: Yes.

Leo: In 2019. Wow.

Steve: Almost a guaranteed payout. If your company got zapped with ransomware, it was like, oh, crap. Send them some money, we need our data back.

Leo: Yeah.

Steve: And now down to one out of three. So that's great progress. The latest major player to be adding support for Passkeys, would you believe TikTok?

Leo: All right. Yay.

Steve: They said: "We'll begin rolling out passkeys for iOS in certain regions." And I thought it was interesting that they didn't list the U.S. They said: "Starting with Asia, Africa, Australia, and South America beginning this month." And they said: "And anticipate expanding to other geographies and operating systems over time." And they also noted they'd become a member of the FIDO Alliance. And Leo, I was watching something the other day, some talking head show that was - oh, it was in regards to the strike, the Hollywood actors and screenwriters strikes. TikTok has equal revenue to like the big streaming services. It's massive.

Leo: Oh, yeah. Oh, yeah.

Steve: I had no - this is like, you know, Henry doing his cooking videos.

Leo: Yeah. Yeah.

Steve: It's astonishing.

Leo: Don't knock it. He's got pretty good income himself. I'm happy he's paying his own way. Yeah, he's got, like, two - and I asked him the other day because I saw him, he was making a chicken cordon bleu sandwich.

Steve: As one does.

Leo: As one does. I said, "Where do you get the ideas for these?" He says, "I just make them up." And I asked him, I said, TikTok, you know, he has more than two million, I think it's two point something million, 2.2 million followers on TikTok. He said, "Yeah, but it's not my primary platform anymore. Instagram's kind of taken over." And he really wants YouTube Shorts and YouTube to be his place because the payouts are better. That's the difference. That's the difference.

Steve: Yup.

Leo: But TikTok's money, but they keep it.

Steve: And it's like, what is it, like $800 billion or something? I mean, it was like - and it was in a chart showing Netflix and Hulu and...

Leo: Yeah. But you know what? The content on TikTok is much more compelling, and people spend more time watching it - not you and me, we're old.

Steve: I don't even - yeah.

Leo: Yeah. Younger people spend a lot of time scrolling.

Steve: Wow.

Leo: And you've got the eyeballs, it's a great place. Plus you can put more ads in. You can't put ads in Netflix. Or you can, but we can't...

Steve: Remember having - remember when we had that much time, Leo?

Leo: Ah, those were the days.

Steve: Okay. So we got some feedback from our listeners. Allan E. said: "I agree that I would never save two-factor authentication seeds in my password manager. But it may be the least bad option for protecting shared business accounts on social media accounts in some cases." And so I just wanted to say I didn't intend to suggest that there was no justifiable use case for having a password manager store time-based token secrets. The question was just a perfect opportunity to highlight and talk about a beautiful example of the inherent tradeoff which exists between user convenience and security.

And to that end, Steven Haver, he said: "Re Bitwarden TOTP." He said: "It's actually a huge increase in security for people who otherwise can't be bothered to turn on two-factor authentication," which you can't argue against that. He says: "It's also extremely useful with shared logins that are shared with multiple people via a Bitwarden Organization mode account." He said: "But for more tech-savvy people, I understand why you would want the greater compartmentalization."

He said: "I run a hybrid approach where my 'less important'" - he has in air quotes - "TOTPs are in Bitwarden, the more important ones are in OTP Auth" - as are all of mine - "and the most important ones are WebAuthn" - meaning Passkeys - "on my security keys." He said: "In a way, TOTP seems like a dying format for those who already use a security key, as FIDO/U2F/WebAuthn become available on more and more sites." And, you know, now soon TikTok. "Whereas," he said, "once there were 40 secrets in my OTP Auth, now I'm down to just a handful." He says: "Thanks for a great podcast, and super excited to take 6.1 out for a spin soon." Signed, Steven.

So thank you, Steven. Of course I agree with everything Steven has just said, and with his hybrid approach, which makes sense. I suspect that, for most people, just using Bitwarden will be the way to go. But, again, my point was to use this more as an example of the nature of always the tradeoff that exists between convenience and security. Super long password, way more secure, way less convenient. So, you know, you need some way to manage that.

Sakis Kasampalis. I'm sorry if I butchered your name. I tried. He wrote: "Hey, Steve. How exactly is Threads blocking Europeans using VPNs?" He said: "I thought that the idea of a VPN was that they cannot tell where you're located. Are they blacklisting IPs of the popular third-party VPNs? What about self-hosted ones?" Okay. So that question has multiple parts. The first part is that there are two ends to every connection, and every end inherently knows the address and therefore the rough location of the other end of a connection. So when someone in the EU connects to Meta directly, Meta gets their IP address and can choose to refuse it.

The clearest way to visualize what a VPN does is to see it as two connections, the user's connection to the VPN service and the VPN service's connection to the destination. So when a customer is connecting through a VPN, Meta doesn't see the customer's IP and their rough location. Meta is being connected to by the VPN, so that's the only IP and location that Meta sees. This bring us to the second part of Sakis's question, which is, "Are they blacklisting IPs of popular third-party VPNs?" And the answer to that is probably yes, that's certainly one way to do what they are doing.

It might also be that in the interest of preserving their users' privacy, VPNs might be deliberately stripping out some user tagging information that a user's web browser would normally provide. So Meta might either and/or be detecting the presence of a middleman in the connection through the means of the metadata in their requests. But either way, Meta can simply decide not to honor "indirect connections" through VPNs specifically because they can be used to mask the user's true location.

And finally, as for self-hosting VPNs, the question would be where the VPN's traffic would emerge onto the Internet. Self-hosting sort of suggests that the endpoint is still located local to the user. But then its IP would be geolocated and blocked. So it would be necessary to self-host a VPN in such a way that the VPN's traffic emerged onto the Internet from a non-blocked region. That might be doable, for example, by spinning up an AWS or Azure cloud instance, but that seems like a lot of trouble to go through just to obtain foreign access to Threads, whose popularity, by the way, appears to have collapsed overnight.

And Leo, on Sunday's TWiT show you and your two guests talked about the collapse of Threads traffic. One of the guests noted how easy Meta had made it for Instagram users to join Threads. Even I joined Threads because I have a stagnant Instagram account, and I wanted to grab my handle just in case Threads might amount to something someday.

Leo: Are you @SGgrc on Threads?

Steve: That's exactly me.

Leo: Okay. All right.

Steve: But, you know, I wanted to note that Threads' apparent overnight success was always entirely illusory, because when it's made that easy to join, joining doesn't actually mean anything.

Leo: Right, that's true, yeah.

Steve: You know, it's reminiscent of the news website paywall model. Remember that originally all sites were free and ad supported. Then some of them thought, "Hey, look at all the traffic we have. Let's charge a little bit of money for people coming." And mostly people said, "Wait, what? You want actual money? I think I'll find the same news elsewhere, thanks very much." So it's going to be very interesting, I think, to see how, over the long term, how Meta's Threads does. And that's really the only metric that matters.

Leo: Well, of course Elon gave it a nice big boost over the weekend by changing the name of Twitter to X.

Steve: Oh. And you know who has the trademark on X?

Leo: Microsoft has one. There are many.

Steve: Yes. And maybe it will be dilution, but Meta also owns a trademark which is very, I mean, it looks exactly like, well, close enough. And you know, as we know, for a trademark the test is whether a user might reasonably be confused by someone's conflicting use of a registered trademark.

Leo: And, by the way, this is why I'm very glad that Twitter is no longer Twitter.

Steve: Yeah, that's a good point.

Leo: And Elon is no longer Chief Twit. We had words. We had a little - we had some words with them, back in the day.

Steve: I remember back in the early days, yeah.

Leo: And I'm very pleased that they're now X, and I will not start a podcast network called X. It's not a great name, if you ask me.

Steve: And he can't have or get X.com, can he?

Leo: He has X.com, yes.

Steve: He does?

Leo: He's had that since day one. So the story is hysterical. He tried to rename - so PayPal, before it was PayPal, was X.com. He's had it since then.

Steve: Ah.

Leo: And the story is Peter Thiel and Sam Levchin, his cofounders, fired Elon because he wanted to use X as the name for PayPal, and they said no, we're going to call it PayPal. And so that was when he left PayPal, and he took his money with him, and of course started a few other things since then.

Steve: And I'll note that PayPal has done just fine since Elon left.

Leo: Oh, yeah, yeah. He was apparently difficult. But one of his kids is named X, you know. X is part of the name. But he likes that letter for unknown - you know why? Because he's nuts.

Steve: Well, I would argue that Twitter does need some competition. I mean, like some real competition.

Leo: There's a lot. There's Threads.

Steve: I can't think of any better...

Leo: There's Bluesky. There's of course Mastodon. There's a lot of good choices.

Steve: Yup.

Leo: The problem is they're fragmenting the overall space.

Steve: Right.

Leo: I have to say, because it's Meta, a lot of brands, a lot of politicians, a lot of newsmakers are all on Threads. So that may be just how they win is just that's where everybody went; right?

Steve: And if Meta could actually deliver on some of the challenges that this kind of platform inherently has, you know, which Twitter was admittedly struggling with, but honestly apparently working to fix or, like, at least mitigate.

Leo: Right.

Steve: Having the same platform, I mean, I've listened to so many people who are disappointed in what Twitter has become because it used to be a place they could quickly go to get news. And it's just not that anymore.

Leo: Yeah, yeah.

Steve: I don't need it for that.

Leo: I think it's good to have something like that in the world, I think.

Steve: Yes. It's a real need. It is an absolute need. Matthew N. Dudek, he said: "Hi, Steve. I'm looking into getting some wireless keyboards for the office, and I was concerned about the security" - I'm glad - "of the connection between the keyboard and the dongle," he says, "not Bluetooth, one like the Logitech K400+." He said: "Have you found any info on this, and if man-in-the-middle attacks are a problem for these kinds of devices? What about the security of Bluetooth keyboards? Are they any better?"

Leo: That's a great question, since I just bought a Bluetooth keyboard. Tell me.

Steve: I'm glad you did. And that's what my wife is using, and I'm going to explain why you are both using those.

Leo: Oh, good. Oh, good.

Steve: Many years ago we talked about the very early widely available wireless keyboards which claimed to be offering "encryption." But we had some fun at the time because the encryption turned out to amount to nothing more than XORing the byte that the keyboard sent with a static value. You know, literally it was an XOR mask which would always flip the same bits in the byte, regardless of what was being sent. So at best we would call that obfuscation, since passively recording the use of the keyboard and performing a frequency analysis of the characters seen would quickly reveal the exact fixed XOR mask. And once you have that, everything typed could be unscrambled, and anything desired could be injected.

Okay, now, the keyboard in question uses Logitech's own "Unifying Receiver" technology. It's not horrible security inasmuch as it uses AES encryption in counter mode. Unfortunately, they tried to do it on the cheap, and a security review of the technology four years ago resulted in CVE-2019-13053. And that CVE was the result of an incomplete fix for CVE-2016-10761 three years before that. Logitech has publicly stated that they feel it's good enough, and that they will not be changing anything. And of course at this late date changing anything would be quite "disunifying."

Leo: Oh.

Steve: So from a quick look at the current state of Logitech's technology, it appears that allowing an attacker to press a few keys on the keyboard - this is with the Logitech unifying receiver technology as it is today...

Leo: That little thing that ships with a dongle, if you want, you can put in your computer.

Steve: Right, right. And I've got, you know, my mouse has one because I like Logitech mice.

Leo: Yeah, me, too.

Steve: Right, right. So allowing an attacker to press a few keys on the keyboard while sniffing its transmission is all that's needed. Also, the protocol leaks metadata for things like turning the NUM LOCK and CAPS LOCK lights on and off and for other functions. This allows for entirely passive attacks. For AES in counter mode to be used securely, the counter's values can never be reused under the same initialization vector. But enforcing that guarantee is difficult for any bare bones protocol, which is what Logitech created for their mice, keyboards, pointers, and other peripherals.

So the solution is simple: Where true security is important, just use the full Bluetooth protocol, though such a keyboard may be more expensive, and they probably are, than Logitech's K400+. All of my own keyboards are wired. But as I said, my wife uses a Logitech MX Keys keyboard.

Leo: I think those are nice, yeah.

Steve: Oh, it is a lovely, lovely low-profile keyboard that uses a full Bluetooth low-energy link. Once it was paired to her Windows 10 machine, she has never had a problem with it. So I can vouch for that and the protocol.

Leo: I wanted a Bluetooth keyboard that would - I have two computers, one monitor, and I wanted a Bluetooth keyboard that would allow me to switch back and forth. And that was Bluetooth. And I also wanted clicky keys. I know you're a clicky key fan.

Steve: Oh, boy, yeah.

Leo: I really, I'm going to recommend - it's 200 bucks, not cheap. But the Keychron Q1 Pro wireless custom mechanical keyboard, and I happen to like the brown switches, the Keychron Browns.

Steve: Uh-huh.

Leo: This is a really wonderful - first keyboard I've really loved in a long time.

Steve: And do you actively switch it between computers? Or does it just pair?

Leo: Yeah. No, no, in this one, and I like it this way, Function Key 1 is the first computer; Function Key 2 is a second. I think you can do 4.

Steve: Oh, so you can have both machines on and listening.

Leo: Oh, yeah, yeah, yeah. That's right.

Steve: In sort of a KVM style.

Leo: Yeah, except it's a little more manual because my mouse is the same thing. I have a Logitech mouse that has three Bluetooth pairings. So I switch the mouse to two, Function 2 on the keyboard, and then my HDMI port I switch to, you know, Port 2 on the monitor.

Steve: Leo. Leo. You qualify for the Expeditionary Force Cyber Team.

Leo: I do wear my BDUs while I'm playing [crosstalk].

Steve: If you've got jammies that look like camo, you're good to go.

Leo: It is a little bit manual, but I have had such bad experiences with KVM switches over the years that just I thought, you know what...

Steve: No, that's very cool.

Leo: It works. It works perfectly every time. It's really a good way to do it, yeah.

Steve: And you may well want to have the other machine's screen still visible while you're over talking to...

Leo: And I could do that. Yes, I could do that. In fact, one of the computers I do keep on because it's a server, so it's always running. So I don't want to - I want to be able to switch back and forth while they're live. And it works.

Steve: Nice.

Leo: Works great, yeah, nice.

Steve: Glenn Lau asked: "Is it possible to SpinRite a phone, iOS or Android, to speed up the phone?" And unfortunately, I'm pretty certain that would not work. While it would be possible to plug the phone into a PC to view it as a drive, only the user-facing storage portion would be seen, not the underlying hidden protected kernel and apps, which is really what you'd want to be rewriting. So, you know, users don't get any access to that from the outside.

Leo: Yeah.

Steve: And we don't want them to, by the way.

Leo: Right.

Steve: Jorge Moran, he said: "Hi, Steve. I'm a big fan. I've been listening to Security Now! for years. I was wondering. A couple of weeks ago when you talked about your Syncthing setup, you said you don't like containers. Is it just because of the added complexity, or do you have more reasons?"

Leo: Ah, good question.

Steve: Okay, so great question. Only personal preference. I totally get it that there's a place for containers like Docker. I agree that they are a terrific solution for many applications. But just for myself, I have often seen how quickly things can get out of control when the approach which I would characterize as "just throw some more code at it" is taken. So if I need to run Syncthing on Synology, and the only way to do that was to be containerized, then that's what I'd do. But Leo, thanks to you, I don't need to do that.

Leo: Yeah.

Steve: It just feels much better to be running Syncthing as a native Synology build.

Leo: Docker's very lightweight. The idea is you're using the same operating system on multiple containers. They're somewhat isolated from one another, so they're pretty lightweight.

Steve: And it brings all of the dependent libraries and stuff.

Leo: Exactly. Exactly.

Steve: Right.

Leo: But Docker is by default not particularly secure, so that's something that made me nervous about running it on my Synology, which must be secure; right?

Steve: Well, and there's a perfect example of why my KISS approach works for me. And his question reminded me of another aspect of a story I've shared before, of how when I attended that DigiCert customer advisory meeting in Utah nearly six years ago, I casually mentioned, like during some coffee time, the rack of equipment that I had at the Level 3 data center. And all of the guys around the table turned and looked at me like I had two heads. So I said, "What?" And one of them said, and he was clearly speaking for all of them, since the rest of them were like nodding their heads, he said: "Steve, no one does hardware anymore."

And I took that to mean that they'd all moved all of their infrastructure to the cloud and were now paying Amazon or Microsoft or whomever for virtually hosting their entire infrastructures. But I also noted that everyone but I worked for a major corporation, and that none of them but I were paying the bills for their infrastructures.

Leo: Ah, yes, that's true.

Steve: And, you know, and it is true that I do occasionally need to drive over to Level 3 to exchange a dead SSD or a spinning drive which has died in a RAID. You know, it's not an emergency, but it's like, okay, I received email saying we've lost a drive, come give us a little TLC.

But in return for that - and of course I do also enjoy getting to touch actual hardware, which always feels good - my infrastructure costs are fixed and very low. I own all the hardware. So I'm renting space, cooling, bandwidth and power. And these days that doesn't cost very much because Level 3 actively wants to keep me from virtualizing my infrastructure with AWS or Azure. I don't tell them that, but they have nothing to worry about. They're not going to be losing me.

So when Jorge ended his tweet asking: "Is it just because of the added complexity, or do you have more reasons?" actually my first thought was, "Hey, I even avoid compilers wherever possible."

Leo: Wow.

Steve: Uh-huh.

Leo: He hand assembles his code with a pencil and a piece of graph paper.

Steve: That's right, baby. One one zero, one zero one, one zero zero. People wonder, why is SpinRite taking so long? One one zero. Zero zero one. One one zero. Brian Weeden, he said: "Steve, loved the show this week on satellites. I work in the space sector on this issue."

Leo: Wow.

Steve: "As you're prepping next week, I can offer up an open source report that my org puts out which includes an entire chapter on cyberattacks on satellites." I have a link in the show notes. He said: "Looking forward to next week's Part 2."

So I followed the link that Brian provided. And since it's exactly on point for today, I'll share the report's introductory paragraph, which introduces the term "counterspace." It reads: "Space security has become an increasingly salient policy issue. Over the past several years, there has been growing concern from multiple governments over the reliance on vulnerable space capabilities for national security, and the corresponding proliferation of offensive counterspace capabilities that could be used to disrupt, deny, degrade, or destroy space systems. This in turn has led to increased rhetoric from some countries about the need to prepare for future conflicts on Earth to extend into space, and calls for some corners to increase the development of offensive counterspace capabilities and put in place more aggressive policies and postures.

"We feel strongly," writes his org, "that a more open and public debate on these issues is urgently needed. Space is not the sole domain of militaries and intelligence agencies. Our global society and economy is increasingly dependent on space capabilities, and a future conflict in space could have massive long-term negative repercussions that are felt here on Earth. Even testing of these capabilities could have long-lasting negative repercussions for the space environment, and all who operate there. The public should be as aware of the developing threats and risks of different policy options as would be the case for other national security issues in the air, land, and sea domains.

"The 2023 edition of the report assesses the current and near-term future capabilities for each country, along with the potential military utility. The countries covered in this report are divided up into those who have conducted debris-causing anti-satellite tests - the United States, Russia, China, and India." Let me say that again. "Countries covered in this report are divided up into those who have conductive debris-causing anti-satellite tests - the U.S., Russia, China, India - and those who are developing counterspace technologies - Australia, France, Japan, Iran, North Korea [wonderful], South Korea, and the UK. It covers events and activities through February 2023."

And I have to say, when you scroll down and just look at some of the charts, wow. I appreciated the idea that just testing, this report noted that just testing some of these things like debris-causing events, meaning you deliberately blast some out-of-service, no-longer-used satellite to see if you can, and unfortunately it explodes, and a lot more debris now to be tracking. Wow.

And in fact I was watching, TWiT was replaying I guess a recent episode of This Week in Space in the live feed before MacBreak Weekly, and you had a guy, neat guy, on who was talking about exactly this, about like the problems with the number, the individual pieces of crap that now have to all be individually tracked, and it actually is causing a problem when you want to launch something new up there because it's got to - you have to find a clear path. And so you need to time your launch window so that your whatever it is rocket will be moving through a place where it's not going to hit any of this crap on its way up. Oh, my god.

Leo: Not to mention the Kessler effect; right? I mean, at some point...

Steve: Well, that is, that is the Kessler effect is that something hits something else, and then that hits something else, and you end up with this domino explosion of junk. Oh, Leo. We are not so clever.

Leo: Well, here's the good news. It will shield us from the sun. So climate change is no longer an issue.

Steve: It may shield us from departure.

Leo: It may change the climate in the wrong direction, but okay. At least we'll cool off a little. We don't have those hot summers.

Steve: Someday parents will tell their children, you know, eclipses used to be infrequent events. Now, it's like, "Mommy, what are these shadows passing along the ground?" "Well, yes, Earwig, that's now..."

Leo: Really, is that the name of the future, Earwig? Is that what we're going to...

Steve: Yeah. We're going to start, we're going to call our kids - I figured that was safe. That's not a name that anyone's using today.

Leo: It's safe. No one's using Earwig. I can't wait to read your first sci-fi novel, Steve. That'll be fun. Earwig.

Steve: I have no big SpinRite news this week. I am at the start of the work to update SpinRite. Oh, actually I'm well into it. Remember that when I began three years ago I created that new USB drive setup capability since I knew that was going to be needed. So I'm in the process now of amalgamating that, that InitDisk technology, into the Windows SpinRite component. I'll get that done. I'll release it for testing to our group. I'll come back and give the DOS SpinRite another rev because a few pieces of debris have accumulated there in its orbit. And then I will end up merging it all together, and we will have SpinRite 6.1. So on that note, Leo, let's take our final break, and then we're going to look at more about what could go wrong in space.

Leo: Oh, boy. I can't wait. I love it that we have somebody from the Secure World Foundation listening to the show and keeping us honest. That's promoting cooperative solutions for space sustainability. Didn't know such a thing existed. Okay, Steve. Let's talk about Satellite Insecurity, Part Deux.

Steve: So of course last week we began our coverage of this important topic. Now, I'm going to confess that I rolled my eyes when our previous U.S. president, Donald Trump, announced the creation of Space Force, a new branch of the military intended to focus upon what happens above our heads. My eye-rolling was mostly due to a lack of appreciation, which I now have, of what is an obvious need. Satellites are uniquely

vulnerable to many forms of attack. Both physical and cyberattacks are actually happening. Last week we learned that ground-based missiles are capable of destroying satellites from the ground, and that space-borne robot satellites capable of both repairing friendly satellites and deliberately damaging hostile satellites are not science fiction. They exist, too. I was thinking, I don't remember what that James Bond movie was where the opening scene showed some spaceship big maw opened...

Leo: "Moonraker." It was "Moonraker." They took the satellites in. He was stealing the satellites, yes.

Steve: Right, right. Anyway, so that's not - it was fiction then, not so much now.

Leo: Not so much, yeah.

Steve: So it was against this backdrop that all of this was triggered by the recent publication of a research paper which demonstrated that those satellites orbiting above are also disturbingly vulnerable to ground-based cyberattack, which is our focus today.

The short news blurb about this which initially caught my eye said: "Satellite security decades behind." And boy, by the time we're finished with this today, you're going to understand exactly how true that is. "A team of academics from Germany has analyzed the firmware of three Low Earth Orbit satellite models and found satellite security practices lagging by decades compared to modern laptops and mobile devices. Researchers found the firmware to be prone to several types of vulnerabilities, lacking basic protection features such as encryption [wow] and authentication. The researchers claim they devised attacks that could hijack satellite systems, cut satellites off from their ground stations, move satellites to new areas, and even crash them into the ground or into other space objects."

Leo: Oh, no, a message to Q.

Steve: As I mentioned last week, the researchers assembled their research into a paper titled "Space Odyssey: An Experimental Software Security Analysis of Satellites." The research was delivered during the recent 44th IEEE Symposium on Security and Privacy held two months ago in May, and it was awarded a Distinguished Paper Award for the conference.

So here's what the team described of their finding in their paper's Abstract. They said: "Satellites are an essential aspect of our modern society and have contributed significantly to the way we live today, most notable through modern telecommunications, global positioning, and Earth observation. In recent years, and especially in the wake of the New Space Era, the number of satellite deployments has seen explosive growth."

Leo: It was "You Only Live Twice." I got the wrong movie. "Moonraker" would be the obvious one; right?

Steve: Of course.

Leo: "You Only Live Twice." Yeah, yeah, they captured the satellites.

Steve: That's perfect.

Leo: There's James Bond in his spacesuit because 007 is good anywhere. And here they come.

Steve: Uh-oh.

Leo: Uh-oh. Oh, no. Oh, no. Anyway, we can do it.

Steve: Boy, is that a hokey-looking satellite.

Leo: Before CGI, I have to say, we really put up with a lot of crappy-looking stuff, didn't we. We didn't know any better.

Steve: Yeah. Don't watch any old episodes of "Lost in Space," Leo. It really does...

Leo: I know, they don't age well, do they.

Steve: Danger, Will Robinson.

Leo: He was about to fall over every time he waved his arms.

Steve: Wow. So they said: "In this paper we provide a taxonomy of threats against satellite firmware. We then conduct an experimental security analysis of three real-world firmware images. We base our analysis on a set of real-world attacker models and find several security-critical vulnerabilities in all analyzed firmware images." Actually 13 critical problems spread among three actual satellites.

They said: "The results of our experimental security assessment show that modern in-orbit satellites suffer from different software security vulnerabilities and often a lack of proper access protection mechanisms. They also underline the need to overcome prevailing but obsolete assumptions. To substantiate our observations, we also performed a survey of 19 professional satellite developers to obtain a comprehensive picture of the satellite security landscape."

Okay. So in other words, after this team of six researchers had uncovered what they thought they had uncovered, they were like, what? Really? So they did the survey just like as a sanity check, like to confirm that what they thought they saw was like - and the guys were like, uh, yup, that's the way we do it.

So they begin by explaining a bit of the history of the industry, which I want to share since it will be so entirely believable and even understandable, though also so obviously wrong, to our podcast audience. So these guys explain, they said: "Satellites are sophisticated technical devices that are placed in outer space for research purposes or to

provide terrestrial applications with services that leverage the coverage of the Earth's surface from a distance. While the first satellite, Sputnik, dates back to 1957, we're in the midst of a renaissance of spaceflight referred to as the New Space Era.

Especially in recent years, we have observed an enormous growth in the number of earth-orbiting satellites. According to the United Nations Office for Outer Space Affairs (UNOOSA), the number of satellites has nearly doubled from 4,867 in 2019 to 9,350 last year in 2022. The majority of these satellites form mega-constellations like Starlink, which plans to launch more than 40,000 satellites in coming years." So to put that in perspective, we don't quite yet have 10,000. We have 9,350 last year. Starlink wants to put up an additional 40,000.

They said: "Small satellites are at the heart of this New Space Era as their size and the widespread use of commercial off-the-shelf (COTS), commercial off-the-shelf components makes them affordable even for small institutions. Furthermore, they cover a broad spectrum of use cases ranging from commercial applications like Earth observation, machine-to-machine communication, and Internet services, to research applications such as technology testing, weather and earthquake forecasting, and even interplanetary missions.

"Although their applications vary widely, small satellites commonly consist of radio equipment and microcontroller boards. Hence in the broadest sense they are computer systems connected to a ground station on Earth, and sometimes even to other satellites. Because they rely on wireless connections for command and control, and use microcontrollers, they are potentially as vulnerable to attacks as any other connected IT platform on Earth." Can you say IoT? Except not "I," you know. So it's not Internet of Things, it's Space of Things.

"This issue," they say, "has not been very relevant in the past since access to ground stations was expensive and limited to large satellite operators. However, the situation changed fundamentally in recent years." Get a load of this. I didn't know this. "Nowadays, ground stations are even affordable for private individuals. And with the emergence of..."

Leo: Wait, what?

Steve: "...Ground Station as a Service..."

Leo: What?

Steve: "...(GSaaS) models, such as those offered by Amazon Web Services and Microsoft Azure, the entry barrier becomes even lower." They said: "We've seen in the mobile network security domain how the providers' assumption that the radio equipment required for attacks would be too costly and out of reach for attackers was ultimately disproved by technological advances." Right, like the Pineapple and, Leo, that thing you have in your pocket.

Leo: Oh, the Flipper Zero, yes.

Steve: That's right. So affordable ground stations create a new novel attack surface where adversaries can communicate with satellites and take advantage of software

vulnerabilities. If they successfully compromise the satellite's firmware, they can access the satellite and potentially take over complete control of the system. And in fact these guys did that. They said: "Despite warnings being made early, little has been done to address this problem for several reasons." Once again, our favorite anti-security thing, inertia.

Leo: Yeah.

Steve: Well, and some lack of understanding. They said: "While the lack of security standards for satellites and the complex supply chain complicate the situation, the main reason is the inaccessibility of satellite firmware." Right? It's like, it's up there. You can't get it.

So they said: "Historically, satellite developers have relied on [oh, yes] security by obscurity. The developers of the Iridium network even mentioned that their system would be too complex for attackers." Yeah, how did that work out? "Attackers have nevertheless successfully decrypted the communication of the network. The inaccessibility of satellites in orbit makes dumping of the firmware by researchers very challenging, if not impossible, impeding progress in this area. Hence, the developers of satellite firmware act as gatekeepers and do not provide researchers with research subjects."

And just I'll pause here for a second and think about almost every instance that we talk about here of a security researcher finding serious problems in some widget wasn't supported in any way by the widget's widget maker. It was them taking the widget apart and sticking some probes into its brains and sucking its firmware out through a JTAG interface, and then...

Leo: Sounds painful.

Steve: Oh, the widget is never the same, Leo.

Leo: Oh, yes. No, that's pretty bad news, yeah.

Steve: It's not good for the widgets, no. But some have to be sacrificed for the greater good. So here's the problem. When your widgets are flying around, you know, miles above you, you can't get them.

So they said: "Previous commentators have acknowledged that the topic is still understudied and conclude that collaboration between satellite development and the security field is required. Additionally, well-known topics like the security of satellite communication, the security of satellite-based Internet services, and threat scenarios for satellites have recently gained increasing attention." Thank god, and it's about time. "However, discussions around individual satellites typically lack technical details of satellite and real-world foundations due to the inaccessibility of satellite software."

Okay. So we have a situation where the physical isolation that's inherent in anything launched into orbit has supported a laxity of security rigor. And it also really sounds as though the developers of these systems have not been following along with the startling advances being made in the capabilities of the underground hacking community here on the ground. As we've seen time and time again, if money can be made through some

hack or attack, it's going to happen, and those attacks are only going to be improving over time. It is a very good thing that Bitcoin was not a satellite-based cryptocurrency, or there wouldn't be any satellites left in orbit today.

But in all seriousness, the U.S., China, and Russia don't care about the price of Bitcoin. What they want is the ability to instantly cripple each other's above-Earth command-and-control infrastructure if the you-know-what suddenly hits the fan.

These researchers felt that they were able to significantly contribute to an understanding of satellite-based insecurity in three ways. They said: "First, we present a taxonomy of threats against onboard satellite firmware. Such a systematic review of the attack surfaces allows us to better represent the complex nature of satellites and categorize security-relevant findings throughout the paper.

"Second, we conduct an experimental and comprehensive security analysis of three real-world, in-orbit satellites to better understand the attack surface and the current state of software security in this particular domain. We focus on Low Earth Orbit (LEO) satellites, as this orbit is the main focus of the New Space Era." Meaning these are the ones that are going to be going up a lot, and we need to get them secured. And we've become dependent on these little puppies; and, boy, are they little. Get a load of this. They said...

Leo: They should call them "Little LEOs," then.

Steve: Little LEOs, that's right.

Leo: Awww.

Steve: "The most prevalent satellite class is the nanosatellite" - Nano LEOs - "more specifically, the CubeSat, which is a standard form factor of 10-centimeter cubes called 'Units' or 'U's.'" Okay, that's four inches on a side.

Leo: Wow.

Steve: I know. These satellites, you know, I wonder if they're going to start calling them "cluster satellites." That would be bad. Anyway, "These satellites typically weigh less than 1.33 kilograms per U and are used in many different projects. After a long period of persuasion, trust building, discussions, and contracts" - you know, they had to sign - "we obtained access to several [three] satellite firmware images that we were able to analyze." In other words, they couldn't get them from the air. So they said, look, we're Germans. You can trust us. We're going to sign contracts. We'll tell you what we find. You haven't ever bothered to look at your own code. Please let us look at it. We're going to help you.

Leo: We're Germans. We know how to find this stuff.

Steve: That's right.

Leo: Yes.

Steve: "All vulnerabilities," they said, "have been responsibly disclosed to the vendors." They said: "Note that the entry barrier to identify these vulnerabilities was complex, given the sensitive nature of these systems. To the best of our knowledge, our work is the first to demonstrate exploitation of satellite firmware vulnerabilities allowing attackers to gain persistent control over the satellite."

Third, and this is where they said we conducted the survey of 19 professionals to ask are you serious about this. And there were 17 satellites that they had technical information about, and those participants had worked on an aggregate of 132 different satellites. So this was the right group of people to ask.

So thankfully, satellite communications is not entirely a standards-free, roll-your-own environment, although it is nothing like the Internet. There is a standards body known as the CCSDS for Consultative Committee for Space Data Systems (CCSDS). It's a consortium of numerous space agencies that agree together on the standards that'll be used for a satellite's communications. So the CCSDS provides the protocol standards for communicating with all components and parties involved in spacecraft operations. These standards cover all the layers of the OSI networking model, usually offering a couple of options per layer.

Two protocols stand out and were examined by these researchers. There's the higher level protocol which is like our TCP on the Internet called the SDLS, which is the Space Data Link Security protocol. And as I said, it's the data link layer like TLS. And then there's the lower level protocol, which we would call IP in the Internet, and that's called the SPP, the Space Packet Protocol.

So their paper then delves into the detailed intercommunications among the various satellite components. The attacker's goals are no different in the sky than they are on the ground. They would love to take over the entire package if they could. But failing that, being able to tap into the communications flow might be all that's available. And if so, they'll take that. But if even that is out of reach, then denying the services provided by the satellite to its rightful users is the final fallback. That should all sound familiar because it's exactly what we have down here on the ground.

The researchers explain that the information containment that has historically existed until recently has been crumbling with the many recent changes taking place within the satellite industry. You know, and that makes sense; right? If there's only, like, three companies making and launching satellites, then it's easy to keep your secrets secret. But as we know, the more people who know a secret, the less secret it is.

They said: "For decades, the satellite community and developers have acted as gatekeepers for the topic of satellite security. By keeping the software and components of satellites under lock, they created a barrier of obscurity that prevented any meaningful research on this subject. Hence, external communities had no way to study satellite internals and potential security issues.

"In recent years this changed, as the developments in the space domain have moved towards the use of common off-the-shelf components" - in other words, not some bizarro one-off processor, but a cortex or a standard chip that IDA Pro or Ghidra would be able to reverse the code for. Also we have open satellite designs, and open-source libraries.

They said: "These factors have been multiplied by the explosive growth in the number of satellites and the inherent increase in the size of the community. Hence, the number of people holding knowledge about satellites has been steadily increasing. Overall, we argue

that a transformation is slowly happening concerning the effectiveness of security by obscurity in space-borne assets." In other words, it's not going to hold any longer, folks. And so you can't be relying on that the way you have in the past.

And they conclude with this: "As a result, we must assume that attackers have detailed knowledge of the target satellite, including detailed documentation and access to firmware images. Further, several open-source satellites already enable attackers to study satellites. We therefore assume attackers have detailed knowledge of satellites, including their firmware, except for their cryptographic secrets."

So in other words, this is the modern security model which is being brought to an industry that never had it before, at least from the standpoint of these researchers. The satellite industry may not have caught up yet, but the only way for researchers to test current satellite security is with an honest set of assumptions of the threat model. As we know, it's always necessary to assume that one's adversary knows everything about the design of their target because too often that's exactly the case.

Another area that they needed to address they termed the "Myth of Inaccessibility." They wrote: "Until recently, it was generally assumed that satellites always communicate with prohibitively expensive" - they use the abbreviation "GSes," meaning Ground Stations. "As a result, only a few actors could attack a satellite, similar to the assumption for mobile cell phone networks many years ago. Unfortunately, this assumption had a major impact on the adaptation of security features for satellites, meaning the lack of them.

However, ground station prices have dropped significantly in the past few years. Today it's possible to create a fully functional ground station" - of your own, in your backyard - "for less than $10,000, and there are open-source communities around developing ground stations. In addition, GSaaS" - as we said, Ground Station as a Service - "providers such as Amazon Web Services or Microsoft Azure rent a ground station to the user, or allow ground station owners to monetize unused ground station capacity by temporarily renting it to end users." Right. What could possibly go wrong?

"As a result, one does not even need to own ground station equipment to interact with satellites. Additionally, transceivers for specific satellite services have become so compact and cheap" that Leo even has one in his pocket. No.

Leo: I do, I do, yes.

Steve: So cheap that - just stand outside and point to the heavens, Leo. "Furthermore, there are now many LEO satellite constellations in space with satellite-to-satellite communication capability." So they're able to talk to each other. "At the same time, there is an increasing number of smaller research LEO satellites. There are already a number of satellites with significant communication capabilities in space that are even intended to be used by third parties. Therefore, we believe that there is a paradigm shift in the assumption that satellites are inaccessible, which is particularly pronounced for Low Earth Orbit satellites."

Okay. So the researchers examined a trio of satellites with widely varying architectures. Actually, that was one thing that sort of impeded their research. There was one that was based on a LEON - or no, it was the AVR32 that was just announced very recently, and its instruction set was not yet well-supported by the various disassemblers. But so there are three satellites. One used an ARM Cortex-M3; another used, as I said, that much more recent AVR32 instruction set; and the third used a LEON3 - I wonder if LEON is like for LEO, you know.

Leo: With an N. Leo Nano.

Steve: Yeah, a LEON3 SPARC V8 processor. In all three cases, upon reverse engineering the satellite's current firmware using IDA Pro and Ghidra, both which we've covered in the past, in each case they uncovered multiple remotely exploitable vulnerabilities that led to remote code execution. Meaning these things are vulnerable.

In return for receiving access to the firmware images, they responsibly disclosed their discoveries of a total of 13 of these "all of them were bad" vulnerabilities across the three satellites they examined. The good news is that sky-bound firmware can be uploaded. The bad news is that, for example, in the case of that ARM Cortex-M3 processor contained in a satellite which was launched in 2013, the firmware update process they were told takes anywhere from several days to a week, depending upon the ground station and link quality. This is due to the low-bandwidth UHF/VHF components which run at - wait for it - 9600 baud, and the sharing of bandwidth.

So to share a sense for the sorts of things they found in these 13 items, they wrote: "Insecure-by-design TeleCommands." TCs is an abbreviation for TeleCommands, which is the process of, obviously, sending a command up to something in orbit. So they said: "Even with no access protection, a satellite should be designed so that TeleCommands do not compromise the satellite's stability without further validation. Two deliberately present TeleCommands" - this is in one particular satellite - "allow arbitrary reading and writing of memory. On the technical level," they said, "the attacker controls all parameters passed to memcpy through command arguments, such that these" - I know, Leo, I hear you in the background. Yes, I know. It's unbelievable.

Leo: I didn't even have my mic on and you heard me.

Steve: "Such that these two TeleCommands are dangerous TCs. Anyone with a custom ground station could utilize them to gain remote code execution and seize control of the satellite." They said: "Noteworthy, the ability to execute arbitrary code, which these provide, would allow an attacker to write firmware updates to the flash memory persistently, making the takeover irreversible.

"Modern operating systems such as Linux or Windows deploy defenses to prevent trivial exploitation of such vulnerabilities, but the RTOS in this ARM Cortex-M3 based satellite does not feature any such protections. In particular, neither ASLR" - of course we know that's Address Space Layout Randomization - "nor stack cookies" - which prevents trivial buffer overruns - "are used. To prove the impact of this vulnerability, we built an exploit, sent our payload over the COM interface to our rebuilt satellite in the lab, and executed arbitrary code. In our case, we play sound over the connected speaker."

Okay. So just to be clear, this satellite that they're referring to actually had deliberate commands which were received over its communications link which allowed any of the machine's memory to be read back, written to, or moved around. I mean, again, this is like Microsoft that built that command into the early Windows Metafile; right? Where if the Metafile interpreter didn't do what you want, you could just put some native code in the Metafile and tell the machine to execute it. What could possibly go wrong with running your own native code from a media file that the machine could be sent? Anyway, what could possibly go wrong with allowing firmware to be rewritten in an in-orbit satellite using some commands that are not authenticated?

Anyway, so of course coming from a security-aware state, the security-aware state that we have all been living in for many years now, it's almost difficult to appreciate what

they mean when they say that the security of many of these satellites relies upon a lack of access to satellite communicating ground stations. In other words, they were not kidding at all. Some of these satellites, as I said, will actually obey by deliberate design remote commands to read, write, and move memory around with no concept of protection, just because they thought, well, you know, who can talk to these things? Very few people. And we're not going to give them our firmware, so they're never going to know what's up there anyway.

Here's another example. They call this one "Trusted ICP Size Field. Upon receiving an ICP packet, the packet is passed through a FreeRTOS data queue to the command scheduler, which executes the associated command using the included arguments. We observed that a function parsing the command structure does not validate the 'length of arguments' field against the total length of the ICP packet." I mean, this is Security 101; right? "Or its payload. Thus, any external attacker can specify a malicious field length, which indicates that the arguments would be longer than they actually are. This causes a command handler function to use more bytes from the memory heap than intended, leading to a buffer overread. Hence, an attacker can include other data in the attacker-TC (TeleCommand) which leads to a control data leak.

"Again, we verify that this works on the real satellite by testing it on our recreated hardware and manage to successfully exploit the vulnerability. The leak itself is reliable and is not impacted by environmental conditions, but extracting specific secrets depends on the heap layout. This vulnerability is reminiscent of the well-known OpenSSL Heartbleed vulnerability."

Or how about this one, which describes something they found in a different satellite: "OPS-SAT uses a flash file system to store files." And I don't know which OS that uses. Maybe they say. Oh, I think it's another FreeRTOS. "OPS-SAT uses a flash file system to store files, including the firmware image. Existing TeleCommands allow to create new files and write to them, providing the capability to upload a malicious firmware image onto the satellite. To change the filesystem path pointing to the current image, critical commands must be enabled, which is a global Boolean value in the satellite's settings. Crucially, changing this flag can be done via a TeleCommand that does not require verification. Hence, external attackers can conduct arbitrary firmware updates, which allows them to seize control over the satellite.

"Interestingly, similar critical functionalities are also hidden behind the same flag, indicating that engineers were aware of its critical importance, but decided not to implement further protection." Okay, so anybody can flip the flag which is protecting this. And once you do, it's not protected, as are other important functions. And once it's not protected, then you're able to upload your own firmware, name it what you want, and then change the path to the current image, causing the satellite to switch to it.

And here's the last one I'll share, a problem in a widely used library. "A widely used," they write, "a widely used space" - we have the space SDK. That would be the SSDK, I guess. "A widely used space SDK utilizes the UFFS library, which implements a low-cost flash file system." I'm sure that's what FFS, you know, Flash File System. "The library is used on roughly 75 spacecraft. And according to the library's author" - who I guess is proud - "is also used by NASA." They wrote: "We identified a stack-based" - I guess that would be a space stack based - "buffer overflow vulnerability in the file renaming procedure, where the name of the new file is copied to a buffer of static size..."

Leo: Oh, oh, oh.

Steve: I know, "without any size check."

Leo: Oh, lord.

Steve: "Resulting" - now, again, this library is used in roughly 75 spacecraft, and NASA is using it - "Resulting in arbitrary code execution. We experimentally verified that this vulnerability can be exploited to gain arbitrary code execution. In OPS-SAT this function is only exposed in an inaccessible UART debug-port, posing no security threat to OPS-SAT in its current state. Still, moving files is a reasonable file system interaction to be exposed via TeleCommands to semi-privileged attackers. Hence, any of the other roughly 75 spacecraft implementing such functionality are also likely to be vulnerable."

Okay. By this point, everyone should have an idea by now of, like, what's been going on. These guys were not kidding when they characterized the satellite industry's security as lagging behind by several decades. Thanks to an attitude of, well, "We are not the PC industry, we are not connected to the Internet, and you can't talk to our birds without special equipment," the security concerns that all of us on the ground here have been fighting for the past several decades and has created endless fodder for this podcast, doesn't appear to have sunk in at all.

Sure, there are instances of mistakes that have not been caught, like these guys. But the most glaring insanity are deliberately designed commands which are insanely powerful and lacking in any authentication, assuming that those commands will never be issued by anybody because they're not connected to the Internet. They require a ground station. That assumption may have been useful 10 years ago, but it holds today. They implicitly assume that no bad guy will ever be able to get their hands on a radio, even now that Amazon and Microsoft will happily lend you one of theirs.

So I sincerely hope that this work, and others similar to it, have or will come to the attention of all of the relevant parties. The good news is that down here on the ground, where we have the Internet, and it's been connecting everyone to everyone else since its beginning, we have had to develop highly, insanely well, you know, peak security awareness. And so hopefully that will rub off on all of the space-bound guys.

Leo: You know, I just always assumed that NASA put a lot of effort into secure code and testing and all of that stuff. Maybe NASA does, but obviously there's a lot of commercial space going on.

Steve: Right, right. You know. And Leo, come on, would Elon delay the launch of a Starlink?

Leo: No comment.

Steve: Just launch it now. We'll fix it in orbit.

Leo: We'll fix it in orbit.

Steve: That's right.

Leo: That should be the name of this show, "We'll Fix It in Orbit."

Steve: We'll fix it in orbit.

Leo: Steve Gibson, you're the best. We look forward to Tuesday all week long so we can all listen and hear your words of wisdom.