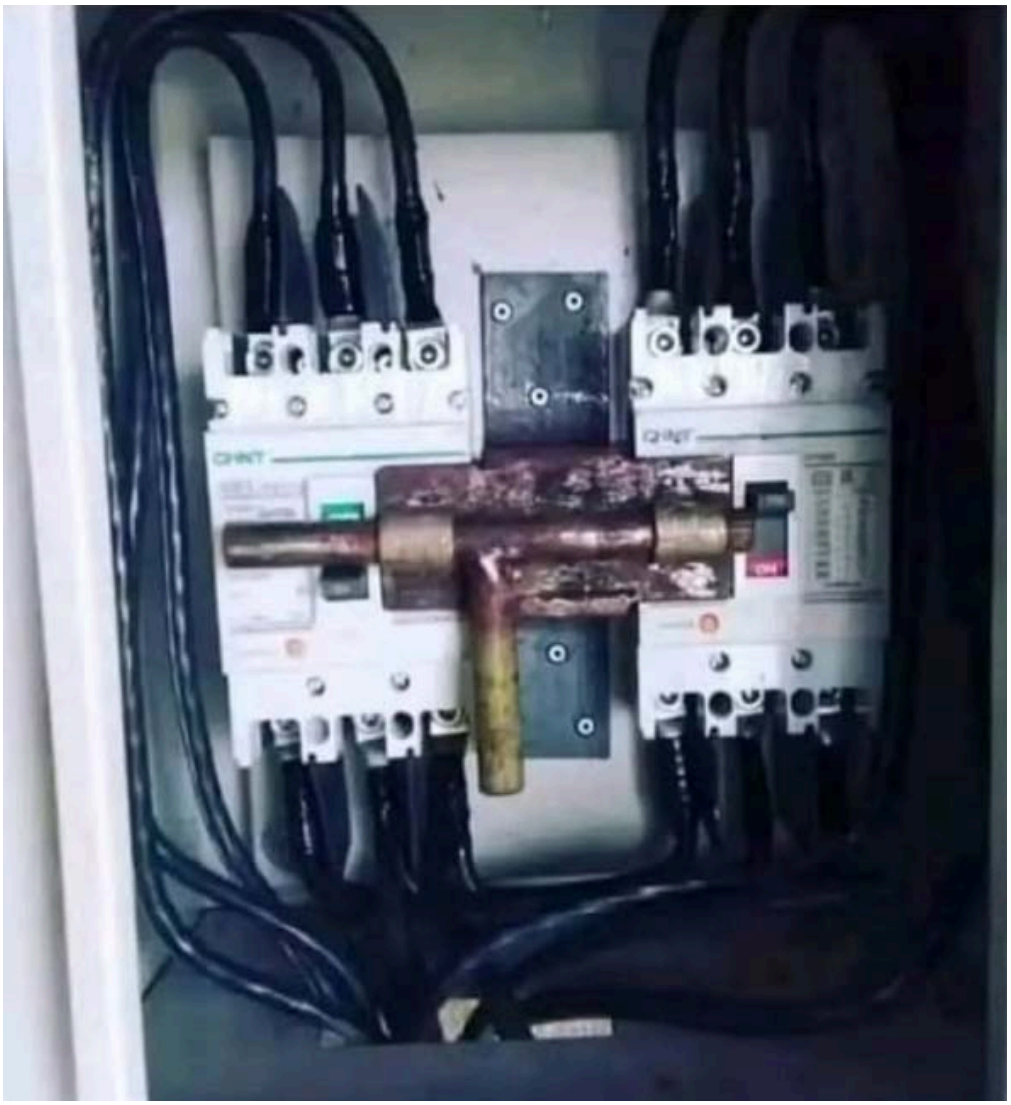
Security Now! #1048 - 10-21-25

Mic-E-Mouse

This week on Security Now!

• The long awaited lawsuit to block Texas SB2420. • Embattled Texas SB2420 also impacts Google Play. • At long last, NIST modernizes their password policy. • Scattered LAPSUS$ Hunters demise was exaggerated. • China claims that the NSA has been hacking them. • Half of all geosynchronous satellite traffic is unencrypted. • The AWS outage highlights the rising risk of Internet monoculture. • A terrific collection of listener feedback and... • Could your PC's mouse have much bigger ears than you know?

When an interlock must be **very clear** and must absolutely, definitely, **never** fail...



Security News

Texas Sued over SB2420

Our coverage of the pending enactment of the new Texas SB2420 legislation galvanized our listeners and generated quite a bit of feedback. I mentioned last Tuesday that there was still no sign of any legal challenge to that legislation. But then last Friday, to no one's surprise, that situation changed. Ars Technica's headline read: *"Big Tech sues Texas, says age-verification law is "broad censorship regime""* Ars gave it the teaser: *"Texas app law compared to checking IDs at bookstores and shopping malls."* Here's what they wrote:

> *Texas is being sued by a Big Tech lobby group over the state's new law that will require app stores to verify users' ages and impose restrictions on users under 18.*
>
> *The lawsuit brought by the Computer & Communications Industry Association (CCIA) alleges: "The Texas App Store Accountability Act imposes a broad censorship regime on the entire universe of mobile apps. In a misguided attempt to protect minors, Texas has decided to require proof of age before anyone with a smartphone or tablet can download an app. Anyone under 18 must obtain parental consent for every app and in-app purchase they try to download—from ebooks to email to entertainment."*
>
> *The CCIA said in a press release that the law violates the First Amendment by imposing "a sweeping age-verification, parental consent, and compelled speech regime on both app stores and app developers." When app stores determine that a user is under 18, "the law prohibits them from downloading virtually all apps and software programs and from making any in-app purchases unless their parent consents and is given control over the minor's account," the CCIA said. "Minors who are unable to link their accounts with a parent's or guardian's, or who do not receive permission, would be prohibited from accessing app store content."*

Yep. As we understand it, that's all completely true and it's exactly the law's intent. Ars continues:

> *The group said, the law requires app developers "to 'age-rate' their content into several subcategories and explain their decision in detail," and "notify app stores in writing every time they improve or modify the functions, features, or user experience of their apps." The lawsuit says the age-rating system relies on a "vague and unworkable set of age categories."*
>
> *The lawsuit claims: "Our Constitution forbids this. None of our laws require businesses to 'card' people before they can enter bookstores and shopping malls. The First Amendment prohibits such oppressive laws as much in cyberspace as it does in the physical world."*
>
> *The lawsuit was filed in US District Court for the Western District of Texas. CCIA members include Apple and Google, which have both said the law would reduce privacy for app users. The companies recently described their plans to comply, saying they would take steps to minimize the privacy risks.*
>
> *The Texas App Store Accountability Act is similar to laws enacted by Utah and Louisiana. The Texas law is scheduled to take effect on January 1, 2026, while the Utah and Louisiana laws are set to be enforced starting in May and July, respectively.*

And here's something new and interesting, Ars also wrote:

The Texas law is also being challenged in a different lawsuit filed by a student advocacy group and two Texas minors.

*Attorney Ambika Kumar of Davis Wright Tremaine LLP said in an announcement of the lawsuit: "The First Amendment does not permit the government to require teenagers to get their parents' permission before accessing information, except in discrete categories like obscenity. The Constitution also forbids restricting **adults'** access to speech in the name of protecting children. This law imposes a system of prior restraint on protected expression that is presumptively unconstitutional."*

That's interesting, but that argument was also tried in the argument against Texas HB1181. Here are a few choice and chilling tidbits from those proceedings:

"The First Amendment leaves undisturbed States' traditional power to prevent children from accessing speech that is obscene from their perspective. Because no person — adult or child — has a First Amendment right to avoid age-verification the statute requires only intermediate scrutiny."

And, from the Supreme Court's opinion:

*"Submitting to age verification **is** a burden on the exercise of [adults'] right. But, adults have no First Amendment right to avoid age verification and the statute can readily be understood as an effort to restrict minors' access."*

So it sure does look to me as though this ground was well covered, argued and decided by the litigation over HB1181. I'm sure we're going to find out soon. Ars Technica continued:

Davis Wright Tremaine LLP said the law "extends far beyond social media to mainstream educational, news, and creative applications, including Wikipedia, search apps, and internet browsers; messaging services like WhatsApp and Slack; content libraries like Audible, Kindle, Netflix, Spotify, and YouTube; educational platforms like Coursera, Codecademy, and Duolingo; news apps from The New York Times, The Wall Street Journal, ESPN, and The Atlantic; and publishing tools like Substack, Medium, and CapCut."

I'm sure they're correct and that is exactly the law's intent. It's a feature, not a bug. They wrote:

Both lawsuits against Texas argue that the law is preempted by the Supreme Court's 2011 decision in Brown v. Entertainment Merchants Association, which struck down a California law restricting the sale of violent video games to children. The Supreme Court said in Brown that a state's power to protect children from harm "does not include a free-floating power to restrict the ideas to which children may be exposed."

The tech industry has sued Texas over multiple laws related to content moderation. In 2022, the Supreme Court blocked a Texas law that prohibits large social media companies from moderating posts based on a user's viewpoint. Litigation in that case is ongoing. In a separate case decided in June 2025, the Supreme Court upheld a Texas law that requires age verification on porn sites.

That last decision is what we've been referring to previously. January 1st is exactly 70 days away from today – so 10 weeks. Not a lot of time for this to be resolved.

Google Play Responds

With this date fast approaching, we know that Apple has informed their developers that new APIs would be available *"later this year"*, even though there's not much left of this year to be later than. Meanwhile, Google just posted something similar for their Play Store App developers. Under their headline *"Changes to Google Play for upcoming app store bills for users in applicable US states"* they wrote:

> *A few US states, currently Texas, Utah and Louisiana, have recently passed verification laws requiring app stores to verify users' ages, obtain parental approval and provide users' age information to developers. These laws also create new obligations for developers who distribute their apps through app stores in these states. The effective dates for these laws, applicable for both developers and Google Play, are quickly approaching and present short implementation timelines across the ecosystem.*
>
> *While we have user privacy and trust concerns with these new verification laws, Google Play is designing APIs, systems and tools to help you meet your obligations. Given the significant implications of these changes across the ecosystem, we are working to keep Play a trusted experience for everyone while also providing you information to support your preparations. Our plan to support you*
>
> *The first app store bill to take effect is Texas's SB 2420 on 1 January 2026.* ***We understand that significant work may be needed for you to make changes to your apps.*** *To help you, we plan to provide:*
>
> - *A new Play API: For users in these states, your app will be able to receive users' age verification or supervision status, age ranges and other applicable signals.*
> - *Play Console features: You will have the ability to notify Google Play of a significant change in Play Console without publishing a new version of your app. Additionally, you will also get a report in Play Console showing when a parent revokes approval for your app.*
> - *Trust and safety requirements: To protect users, your use of this new API must comply with Google Play's requirements governing how data from the API must be handled.*
>
> *More details on these features and requirements will be shared in the coming weeks. Planned dates and next steps (subject to change)*
>
> - *October 2025: Requirements and a detailed integration guide with example code for the new Play API will be published for you to get started.*
> - *1 January 2026: The new Play API will be live for applicable users in Texas when the Texas SB 2420 bill takes effect.*
>
> *If you would like to learn more or have any additional questions, please contact our support team.*

We all know that I'm not an attorney. But no one needs legal training to get a definite sinking feeling from reading the opinion of the Supreme Court in the previous very similar challenge to Texas HB1181. The Court supported the requirement that anyone wishing to view age-restricted content could reasonably be asked to prove their age, even if doing so required them to reveal their identity and would certainly have the effect of limiting access to content even among those whose age would make such access legal.

The Supreme Court said: *"Adults have no First Amendment right to avoid age verification."* All that said, though, the law is a complex instrument and there could well be other factors in play with SB2420. We won't know until we do.

NIST catches up with "Password Haystacks"

As all of our longtime listeners will recall that about 13 years ago, back in 2012, after spending some time on the podcast examining and sharing the details of what was then modern password cracking using high-speed hardware assisted hashing systems, I hit upon the idea that a password's ***length*** was far more important to its provision of cracking resistance than its ***complexity***.

The idea was that if some hashing system was going to be trying every possible password of a certain assumed minimum length, and then increase its guessed length after exhausting all possible passwords of the initial length, then the easiest means of preventing this form of password cracking would simply be to use longer passwords so that anyone attempting to brute force crack the password would give up.

The essential revelation was that if all possible passwords were going to be checked, it made no difference what characters those passwords contained since they would all be checked eventually. The only thing that mattered was the password's length. This could also be summed up in that time-honored way: Size does matter.

Searching for a name for this concept, someone in GRC's newsgroups suggested the proverbial *"needle in the haystack"* which I loved and the *"Passwords Haystacks"* page was born. That simple webpage at GRC helped people appreciate the power math behind the idea of longer passwords – and that was around 9.3 million visits ago.

I'm mentioning this today because, though it took 13 years for NIST – the U.S. National Institute of Standards and Technology – to catch up with this idea, they finally have. Friday before last, MalwareBytes picked up on this news with their headline: *"Your passwords don't need so many fiddly characters, NIST says"* They wrote:

> *It's once again time to change your passwords, but if one government agency has its way, this might be the very last time you do it.*
>
> *After nearly four years of work to update and modernize its guidance for how companies, organizations, and businesses should protect their systems and their employees, the US National Institute of Standards and Technology has released its latest guidelines for password creation, and it comes with some serious changes.*
>
> *Gone are the days of resetting your and your employees' passwords every month or so, and no longer should you or your small business worry about requiring special characters, numbers, and capital letters when creating those passwords. Further, password "hints" and basic security questions are no longer suitable means of password recovery, and password length, above all other factors, is the most meaningful measure of strength.*
>
> *The newly published rules will not only change the security best practices at government agencies, they will also influence the many industries that are subject to regulatory compliance, as several data protection laws require that organizations employ modern security standards on an evolving basis.*

In short, here's what NIST has included in its updated guidelines:

- *Password "complexity" (special characters, numbers) is out.*
- *Password length is in (as it has been for years).*
- *Regularly scheduled password resets are out.*
- *Passwords resets used strictly as a response to a security breach are in.*
- *Basic security questions and "hints" for password recovery are out.*
- *Password recovery links and authentication codes are in.*

The guidelines are not mandatory for everyday businesses, and so there is no "deadline" to work against. But small businesses should heed the guidelines as probably the strongest and simplest best practices they can quickly adopt to protect themselves and their employees from hackers, thieves, and online scammers. In fact, according to Verizon's 2025 Data Breach Investigations Report, "credential abuse," which includes theft and brute-force attacks against passwords, "is still the most common vector" in small business breaches.

MalwareBytes then went into some additional detail which I want to share since it was interesting and relevant:

Here's what some of NIST's guidelines mean for password security and management.

1. The longer the password the stronger the defense
"Password length is a primary factor in characterizing password strength," NIST said in its new guidance. But exactly how long a password should be will depend on its use. If a password can be used as the only form of authentication (meaning that an employee doesn't need to also send a one-time passcode or to confirm their login through a separate app on a smartphone), then those passwords should be, at minimum, 15 characters in length. If a password is just one piece of a multifactor authentication setup, then passwords can be as few as 8 characters.

Also, employees should be able to create passwords as long as 64 characters.

2. Less emphasis on "complexity"
Requiring employees to use special characters (&^%$), numbers, and capital letters doesn't lead to increased security, NIST said. Instead, it just leads to predictable, bad passwords. "A user who might have chosen 'password' as their password would be relatively likely to choose 'Password1' if required to include an uppercase letter and a number or 'Password1!' if a symbol is also required," the agency said. "Since users' password choices are often predictable, attackers are likely to guess passwords that have previously proven successful."

In response, organizations should change any rules that require password "complexity" and instead set up rules that favor password length.

3. No more regularly scheduled password resets
In the mid-2010s, it wasn't unusual to learn about an office that changed its WiFi password every week. Now, this extreme rotation is coming to a stop.

According to NIST's latest guidance, passwords should only be reset after they have been compromised. Here, NIST was also firm in its recommendation—a compromised password must lead to a password reset by an organization or business.

4. No more password "hints" or security questions
Decades ago, users could set up little password "hints" to jog their memory if they forgot a password, and they could even set up answers to biographical questions to access a forgotten password. But these types of questions—like "What street did you grow up on?" and "What is your mother's maiden name?"—are easy enough to fraudulently answer in today's data-breached world.

Password recovery should instead be deployed through recovery codes or links sent to a user through email, text, voice, or even the postal service.

5. Password "blocklists" should be used
Just because a password fits a list of requirements doesn't make it strong. To protect against this, NIST recommended that organizations should have a password "blocklist"—a set of words and phrases that will be rejected if an employee tries to use them when creating a password.

"This list should include passwords from previous breach corpuses, dictionary words used as passwords, and specific words (e.g., the name of the service itself) that users are likely to choose," NIST said.

So, this qualifies as **big news**. What NIST says matters, since it drives official corporate policy. Although NIST has slowly been coming around, through the years we've heard from so many of our listeners whose employers have been enforcing NIST's earliest ridiculous guidelines which required passwords to be changed regularly every 60 to 90 days. I've obviously invested a great deal of time thinking about this stuff, and I have **never** understood what problem that was supposed to solve and why it would have any effect other than reducing security. It's not as if passwords were osmotically seeping out of the storage location that held them, so that a new password should be put into effect before the entire previous password had time to finish fully seeping out. None of that ever made any sense.

So now, things are significantly more sane. We have new official NIST guidelines that can be waved around in front of the IT department of anyone's employer and used to retire those now-obsolete periodic password change requirements. For ease of access, I've made the new NIST guidelines this week's GRC shortcut of the week. So anyone can retrieve those guidelines by putting GRC.SC/1048 into the browser, which will bounce you over to the NIST website to view **"NIST Special Publication 800-63B"**: https://pages.nist.gov/800-63-4/sp800-63b.html

News of Scattered LAPSUS$ Hunters demise was greatly exaggerated
A few weeks back I reported that the group Scattered LAPSUS$ Hunters had declared itself done and was disbanding. Some of last week's news brought that claim into question. And now we have pretty clear evidence that the group remains a going concern.

Last Thursday, Joseph Cox with the highly respected 404 Media group published a short piece with the headline *"Hackers Dox Hundreds of DHS, ICE, FBI, and DOJ Officials"* and the sub-head *"Scattered LAPSUS$ Hunters—one of the latest amalgamations of typically young, reckless, and English-speaking hackers—posted the apparent phone numbers and addresses of hundreds of government officials, including nearly 700 from DHS."*

Not much more is known about this at this time, but I wanted to formally take back any suggestion that Scattered LAPSUS$ Hunters had disbanded. All of the evidence suggests that was never true.

Did the NSA hack into China?
I've often bemoaned the lack of any news of offensive U.S. cyber operations being carried out by the U.S. and aimed at our cyber-adversaries (of which we have a few). Just to be clear, I would much prefer that no one was attacking anyone. But since we've been buried in reports of Russian, North Korean and especially China's state-sponsored cyber attacks against the West, I'll admit that it was not unwelcome to encounter and Associated Press headline: *"China accuses US of cyberattack on national time center"* — That's kind of welcome news, though it might have been more useful if it's both true -*and*- the U.S. hadn't been caught.

Here's what the Associate Press reported out of Beijing the day before yesterday:

> *China on Sunday accused the U.S. National Security Agency of carrying out cyberattacks on its national time center following an investigation, saying any damage to related facilities could have disrupted network communications, financial systems and power supply.*
>
> *The Ministry of State Security alleged in a WeChat post that the U.S. agency had exploited vulnerabilities in the messaging services of a foreign mobile phone brand to steal sensitive information from devices of the National Time Service Center's staff in 2022. It did not specify the brand.*
>
> *The U.S. agency also used 42 types of "special cyberattack weapons" to target the center's multiple internal network systems and attempted to infiltrate a key timing system between 2023 and 2024, it said. It said it had evidence but did not provide it in the post.*
>
> *It said the time center is responsible for generating and distributing China's standard time, in addition to providing timing services to industries such as communications, finance, power, transport and defense. It had provided guidance to the center to eliminate the risks.*
>
> *It said: "The U.S. is accusing others of what it does itself, repeatedly hyping up claims about Chinese cyber threats."*
>
> *Western governments in recent years have alleged hackers linked to the Chinese government have targeted officials, journalists, corporations and others. The ministry's statement could fuel tensions between Washington and Beijing, on top of trade, technology and Taiwan issues.*
>
> *The U.S. Embassy did not immediately comment.*

As we know, it's certainly true that the West has been moaning about Chinese state sponsored attacks for many years. So I'm not unhappy to finally hear Chinese authorities complaining that the NSA has similarly been crawling around inside **their** networks for many years, too. It would be better to have peace maintained for reasons other than mutually assured destruction. But if that's the only way we can have peace in a world with mutually aggressive governments then at least we should have some peace even though it might be somewhat less stable than it could be.

Security through obscurity?
When I heard the news of this next story, my first thought was that it was a classic example of security through obscurity. Our listeners know that I've sometimes decried the pronouncements of online tech-weenies whose sole chant, issued to anyone who hides anything, is "security through obscurity is no security." It's as if, after being exposed to that one concept they feel like a security expert every time they echo it.

Such flippant remarks are annoying because actual security mechanisms are not so simple. For example, the gold standard of flexible encryption is public key crypto. Its power is that one of its two keys is made public by design. But we go to extreme lengths to keep their matching private keys secret. Is that "security through obscurity?" No. **It's security through secrecy.** Since all security inherently depends somewhere upon secrecy and secrets, the actual security provided by any security system depends upon our ability to keep those dependent secrets, a secret.

I started off saying that when I heard the news of this next story I was put in mind of "security through obscurity", because, in contrast to the misuse of that phrase, there are certainly some instances where a system was just assumed to be secure only because no one had ever even bothered to check to see if anyone had locked the door.

Researchers from the Universities of San Diego and Maryland thought to aim a commercial off-the-shelf satellite dish upward – which, you know, being an antenna dish for talking to satellites in the sky is sort of the obvious direction to point it. What they discovered is perhaps the best definition of "security through obscurity" imaginable – talk about not locking the door! Apparently, because most people do not have their own satellite dishes aimed at the sky – and even when they do it's hooked to some box that's selecting only what it should – an astonishing amount of important data is not encrypted and is in no way protected! Obscure? Kinda. Secure? Not even a little bit.

Details of what they discovered were recently announced by the Universities. The Summary of their findings reads:

> *We pointed a commercial-off-the-shelf satellite dish at the sky and carried out the most comprehensive public study to date of geostationary satellite communication. A shockingly large amount of sensitive traffic is being broadcast unencrypted, including critical infrastructure, internal corporate and government communications, private citizens' voice calls and SMS, and consumer Internet traffic from in-flight wifi and mobile networks. This data can be passively observed by anyone with a few hundred dollars of consumer-grade hardware. There are thousands of geostationary satellite transponders globally, and data from a single transponder may be visible from an area as large as 40% of the surface of the earth.*

Wow. Unencrypted in-the-clear data being blindly and widely beamed down to us from above, including *"critical infrastructure, internal corporate and government communications, private citizens' voice calls and SMS, and consumer Internet traffic from in-flight wifi and mobile networks."* ... all apparently happening only because no one ever thought to look up before.

Under their topic *"What type of network traffic was exposed?"* they broke it down into six categories:

- **Cellular Backhaul**
  We observed unencrypted cellular backhaul data sent from the core network of multiple telecom providers and destined for specific cell towers in remote areas. This traffic included unencrypted calls, SMS, end user Internet traffic, hardware IDs (e.g. IMSI), and cellular communication encryption keys.

- **Military and Government**
  We observed unencrypted VoIP and internet traffic and encrypted internal communications from ships, unencrypted traffic for military systems with detailed tracking data for coastal vessel surveillance, and operations of a police force.

- **In-flight Wi-Fi**
  We observed unprotected passenger Internet traffic destined for in-flight Wi-Fi users on airplanes. Visible traffic included passenger web browsing (DNS lookups and HTTPS traffic), encrypted pilot flight-information systems, and in-flight entertainment.

- **VoIP**
  Multiple VoIP providers were using unencrypted satellite backhaul, exposing unencrypted call audio and metadata from end users.

- **Internal Commercial Networks**
  Retail, financial, and banking companies all used unencrypted satellite communications for their internal networks. We observed unencrypted login credentials, corporate emails, inventory records, and ATM networking information.
  (You know ... it appears that "China" should be the least of our worries!)

- **Critical Infrastructure**
  Power utility companies and oil and gas pipelines used GEO satellite links to support remotely operated SCADA infrastructure and power grid repair tickets.

The researchers' paper, which will be published in the *"Proceedings of the 32nd ACM Conference on Computer and Communications Security (CCS '25), Taipei, Taiwan. ACM"* is titled: *"Don't look up: There are sensitive internal links in the clear on GEO satellites."* I've included a link to their full paper in the show notes. But just to give everyone a bit of additional flavor for the content of the data that's constantly pouring down over everyone' head, here's what the paper's Abstract explains:

> *Geosynchronous (GEO) satellite links provide IP backhaul to remote critical infrastructure for utilities, telecom, government, military, and commercial users.*
>
> *To date, academic studies of GEO infrastructure have focused on a handful of satellites and specific use cases. We perform the first broad scan of IP traffic on 39 GEO satellites across 25 distinct longitudes with 411 transponders using consumer-grade equipment. We overcome the poor signal quality plaguing prior work and build the first general parser that can handle the diverse protocols in use by heterogeneous endpoints.*
>
> *We found 50% of GEO links contained cleartext IP traffic; while link-layer encryption has been standard practice in satellite TV for decades, IP links typically lacked encryption at both the link and network layers. This gives us a unique view into the internal network security practices of these organizations. We observed unencrypted cellular backhaul traffic from several providers including cleartext call and text contents, job scheduling and industrial control systems for utility infrastructure, military asset tracking, inventory management for global retail stores, and in-flight wifi.*

In other words, no one really took the trouble before now to look closely at what was going on. These guys did and what they discovered was a profound lack of security.

Satellite Television has always been encrypted because that was part of its business model. Pirating early satellite TV was a cottage industry. But what we see of the IP – Internet Protocol – traffic is the same thing we see of the Internet itself. As we know, the Internet's networking, just like internal corporate networking – at the link layer – is still today and always has been entirely unencrypted. Encryption was added as an afterthought only where it was deemed necessary.

So what appears to have happened is that satellite links have been used as simple network extenders, extending the reach of industrial, corporate, major retail and even military networks through satellite links, where those links themselves have never been, and to this day remain, completely in-the-clear and unencrypted.

The 18-page paper is chock full of really interesting tidbits. It's fantastic work, and I could easily spend several podcasts detailing all of the nuances and motivations that they discovered. But there's much more that needs our attention. The researchers acted responsibly and worked to notify all of the affected parties – and they were many. If shining a very bright light on this doesn't get it fixed, then nothing else will. And it appears that perhaps nothing will.

https://satcom.sysnet.ucsd.edu/docs/dontlookup_ccs25_fullpaper.pdf

The risk of a networking monoculture

We've often commented that security and other risks accrue anytime everyone is using the same solution. This is generically referred to as a dependence upon a monoculture. Diversity brings huge benefits. We've worried about the world becoming "Chromium browser centric" where all web browsers are essentially based upon a single code base. So far, Safari and Firefox have been maintaining their own.

And one of the most powerful design benefits of the Internet's autonomous packet routing architecture has been its resilience in the face of trouble. If links to one router go down, packets can "route around" the trouble, taking different paths to still reach their destination.

Problems can arise when this massively decentralized and inherently resilient design is eschewed in the pursuit of market dominance. Much as I love Cloudflare and so much of the work they do, I'm also always made a bit nervous by the outsized power they inherently wield by virtue of their size and the percentage of the world that's being serviced by a single organization. This has nothing to do with who they are. I think they're great. But what they have grown into is not the Internet way.

That's every bit as true for Amazon's AWS services as it is for Cloudflare, and just yesterday the entire Internet learned exactly what can happen when the aggregated services offered by a single provider are inadvertently withdrawn from the world.

The Verge's headline yesterday was: *"Major AWS outage took down Fortnite, Alexa, Snapchat, and more."* with the subhead: *"The cause of the AWS outage is currently unclear."* The first trouble I experienced was when I attempted to get to the IMDB website and received a "503 Bad Gateway" error. But it was The Guardian's coverage and their take on yesterday's serious outage events that resonated most for me.

The Guardian's headline was: *"Amazon Web Services outage shows internet users 'at mercy' of too few providers, experts warn."* with the subhead: *"Crash that hit apps and websites around world demonstrates 'urgent need for diversification in cloud computing'"*. Sure thing. Unfortunately, economics is driving this, and it's taking us in the wrong direction. Here's what The Guardian wrote:

> *Experts have warned of the perils of relying on a small number of companies for operating the global internet after a glitch at Amazon's cloud computing service brought down apps and websites around the world.*

The affected platforms included Snapchat, Roblox, Signal and Duolingo as well as a host of Amazon-owned operations including its main retail site and the Ring doorbell company.

More than 1,000 companies worldwide were affected, according to Downdetector, a site that monitors internet outages, with 6.5m reports of problems from users, including more than one million reports in the US, 400,000 in the UK and 200,000 in Australia.

In the UK, Lloyds bank was affected as well as its subsidiaries Halifax and Bank of Scotland, while there were also problems accessing the HM Revenue and Customs website on Monday morning. Also in the UK, Ring users complained on social media that their doorbells were not working.

In the UK alone, reports of problems on individual apps ran into the tens of thousands for each platform. Other affected platforms around the world included Wordle, Coinbase, Duolingo, Slack, Pokémon Go, Epic Games, PlayStation Network and Peloton.

By 10.30am UK time, Amazon was reporting that the problem, which first emerged at about 8am, was being resolved as AWS was "seeing significant signs of recovery". Referring to the US east coast region, at 11am it added: "We can confirm global services and features that rely on US-EAST-1 have also recovered."

Experts said the outage underlined the dangers of the internet's reliance on a small number of tech companies, with Amazon, Microsoft and Google playing a key role in the cloud market.

Dr Corinne Cath-Speth, the head of digital at human rights organisation ARTICLE 19, said the outage underlined the dangers of placing too much digital infrastructure in a small number of hands. She said: "We urgently need diversification in cloud computing. The infrastructure underpinning democratic discourse, independent journalism, and secure communications cannot be dependent on a handful of companies."

Cori Crider, the executive director of the Future of Technology Institute, a thinktank that supports a sovereign technology framework for Europe, said: "The UK cannot keep leaving its critical infrastructure at the mercy of US tech giants. With Amazon Web Services down, we've seen the lights go out across the modern economy – from banking to communications."

Madeline Carr, professor of global politics and cybersecurity at University College London, said it was "hard to disagree" with warnings about the over-reliance of the global internet on a small number of companies. "The counter argument is that it's these large hyper-scaling companies that have the financial resources to provide a secure, global and resilient service. But most people outside of those companies would argue that is a risky position for the world to be in."

Amazon reported that the problem originated in the east coast of the US at Amazon Web Services, a unit that provides vital web infrastructure for a host of companies, which rent out space on Amazon servers. AWS is the world's largest cloud computing platform.

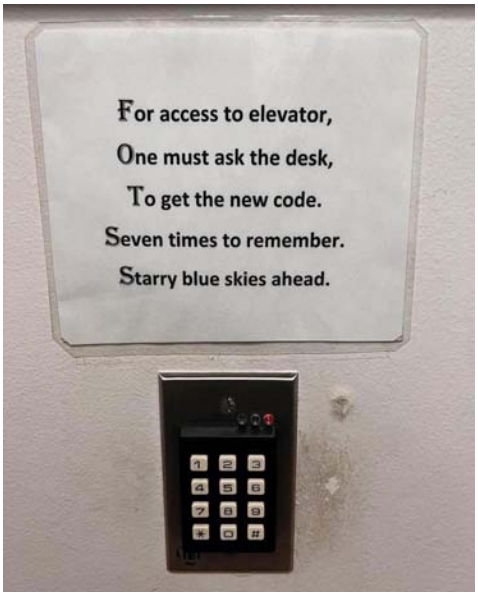
Shortly after midnight (PDT) in the US (8am BST), Amazon confirmed "increased error rates and latencies" for AWS services in a region on the east coast of the US. The ripple effect appeared to hit services around the world, with Downdetector reporting problems with the same sites on multiple continents.

Cisco's Thousand Eyes, a service that tracks internet outages, also reported a surge in problems on Monday morning, with many of them located in Virginia, the location of Amazon's US-East-1 region where AWS said the problems began and where AWS has a number of datacentres.

Rafe Pilling, the director of threat intelligence at the cybersecurity firm Sophos, said the outage appeared to be an IT issue rather than a cyber-attack. AWS's online health dashboard referred to DynamoDB, its database system where AWS customers store their data. He said: "When anything like this happens, the concern that it's a cyber incident is understandable. AWS has a far-reaching and intricate footprint, so any issue can cause a major upset. In this case it looks like it's an IT issue on the database side and they will be working to remedy it as an absolute priority."

The UK government has said it is in contact with Amazon over Monday's internet outage. A government spokesperson said: "We are aware of an incident affecting Amazon Web Services, and several online services which rely on their infrastructure. Through our established incident response arrangements, we are in contact with the company, who are working to restore services as quickly as possible."

Listener Feedback



It's: " 4127* "

I was tempted to title today's podcast *"You forgot to press star"* after reading one of our listener's humorous bits of feedback. Several less-senile and more sharp-eyed listeners than I, posted to GRC's Security Now! newsgroup and many listeners sent feedback about something I missed last week. I do hope this is not a sign of our early onset dementia. We saw that the first word of each of the first **four** lines of the notice over the keypad gave us the code 4127. And I did wonder about that superfluous seeming last line which read *"Starry blue skies ahead."* I assumed it was added to the end of the little poem for the purpose of making the rest seem more poetic and perhaps less obvious. Wrong.

What was less obvious, at least to me, was that the keypad also had *"Star"* and *"Pound sign"* keys. So *"Starry blue skies ahead."* was a similarly subtle instruction (too subtle for me apparently), to end the *"4127"* code input by pressing the *"Star"* key. ***Duh!!***

Stephen Palm

It seems like this was inappropriately focused on Apple products and specifically iPhones. It should be noted that Google, Microsoft, some Linux distributions, Amazon, Docker, Synology, Netgear routers, Game consoles, Modern digital cameras like Sony, HP printers, Smart TV's and a lot more all have a marketplace where you can shop and pay for an app or expansion or upgrade of some sort. Even some cars. The legislation is doomed.

And now we know that that legislation's constitutional legality has been challenged even though, as I noted earlier, my guess is that it's as likely to survive as HB1181 did before it. Stephen's note made me curious about SB2420's legal definition of an "App Store" and, indeed, it's frighteningly broad. The legislation reads:

(2) "App store" means a publicly available Internet website, software application, or other electronic service that distributes software applications from the owner or developer of a software application to the user of a mobile device.

This means that it is, at least, constrained to platforms that distribute software applications to mobile devices. And we know what the legislation's intent is. It's squarely aimed at the major app stores for Apple iPhones and Android smartphones. So it's probably less dire than Stephen was suggesting. And on the receiving end, the legislation defines "Mobile Device" as:

(4) "Mobile device" means a portable, wireless electronic device, including a tablet or smartphone, capable of transmitting, receiving, processing, and storing information wirelessly that runs an operating system designed to manage hardware resources and perform common services for software applications on handheld electronic devices.

So that's also pretty tightly specified and it means that as Stephen enumerated, Synology NAS, Netgear routers, game consoles, modern digital cameras, printers and smart TVs would not be swept up by SB2420. It's only meant to govern mobile phones and pads. This, of course, doesn't minimize the mess this is going to create, but at least it's not everything else in the world, too.

Jason Tschohl

Hi Steve and Leo, First thank you for 20 great years of Security Now! I've been a listener since the very beginning. I just finished listening to SN 1047 and I'm confused about something. F-Droid is worried about Google's changes to the Play Store, but they seem very quiet about SB2420. Wouldn't SB2420 be even more detrimental to F-Droid than the changes to the Play Store? Thanks! -Jason

Yes. The home page of the F-Droid site asks the question *"What is F-Droid?"* and answers it:

F-Droid is an installable catalogue of FOSS (Free and Open Source Software) applications for the Android platform. The client makes it easy to browse, install, and keep track of updates on your device.

But this raises an intriguing loophole question: The F-Droid app itself would first need to be obtained from the Google Play store. And for that any and every minor-age person would need a parent's approval. But the F-Droid app itself offers an installable catalogue of FOSS applications for Android. So, technically, it's an application which accesses a repository – it's not a store. So the letter of the law doesn't quite encompass the F-Droid case. But to Jason's point, I would not want to be in F-Droid's shoes here, because one thing Texas SB2420 does clearly state is that each and every software download and installation ***must*** receive parental consent. The F-Droid app, once obtained, allows for unrestricted application use from F-Droid's repository.

Flemming Hansen in Denmark

EU chat control would be useless: In my view it would be relatively straightforward to bypass the proposed EU chat-control measures: an individual could encrypt an illicit image on a desktop computer, transmit the encrypted file via an app subject to the chat-control, and the recipient could then decrypt it on a computer to restore the original image. / Kind regards

Right. Not nearly as convenient, but clearly true. It's a variation on the old theme of *"If the use of encryption is criminalized, only criminals will use encryption."* In this case, of course, it's the use of smartphone to converse that's

Ray Noemer

Thought I'd let you know I just purchased 6.1. I've owned previous versions for many years and it saved my butt (data) many, many times. I realize I could take advantage of the upgrade path, but I would rather support your work and the effort that goes into your weekly podcast, so ... I bought 6.1. Keep up the great work, please!!, ray

I chose to share that, not because I expect anyone else to do the same, but because I wanted to give Ray's generosity wider recognition. While I appreciate his extra purchase, my plan is to give everyone new stuff to purchase which will hopefully benefit their lives much as SpinRite has been able to for the past 36 years. To that end, I'm working every day to get the DNS Benchmark wrapped up and ready, after nearly 10 months of work on it. So thank you again, Ray.

Duncan

Hi Steve and Leo - long time listener, propeller-head and SpinRite user (which paid for itself a hundredfold by restoring my daughter's crashed MacBook hard drive weeks before her final school exams!)

I've been listening with interest to your coverage of the age verification topic, alongside developments in the imminent Australian social media restrictions, planned for December 2025. While I'm sure your listeners want to protect the innocence and mental health of our children, they also appreciate the technological challenges involved and the fact that any solution will require all adults to verify their age, not just minors. My reason for writing is to make a point that seems to have been overlooked in this whole debate - the older brother loophole.

The existing laws around the globe were drawn up in a physical world, where it is possible to physically identify someone entering an adult pub, club or movie theatre or purchasing alcohol, cigarettes, magazines or other restricted activities. However, in the physical world, there was nothing to stop an older brother or friend purchasing alcohol, cigarettes, movies or magazines and sharing those with minors after purchase. We all know this happens in real life. Away from the "point of sale" there's nothing that can be done about this, apart from vigilant parenting or Big Brother policing in your own home.

The technological world is no different. You can put all of the electronic age restrictions you want on minors themselves, but you can't stop them watching or reading information on their older brother or friend's phone, computer or TV or the unlocked iPad sitting in the family living room. People often talk about savvy kids using VPNs to override national or regional restrictions, but there will be endless other ways for older brothers/friends to "lend" their age verification, credentials or device to a minor that make the whole exercise futile from the start, with the obvious cost and risk to everyone else's privacy.

I can't envision a feasible technological solution to this problem until our devices are constantly surveilling their viewers' eyeballs or brains to ensure no minors are watching their screens at any point in time. I look forward to you covering this Big Brother world in episode 1984!

Hopefully this brings another angle to your ongoing analysis of this interesting challenge. Keep up the great work! Regards, Duncan in Sydney, Australia

Duncan's note about the need for continual surveillance in the cyber world reminded me of something I encountered while researching this topic. The U.S. state of Tennessee has the "Protect Tennessee Minors Act" (SB 1792 / HB 1614) which includes the requirement for an explicit periodic re-verification of a user's age. Specifically, Tennessee's law, which is also currently in effect and has also resulted in content blackouts, defines an "age-verified session" as the lesser of the user's current session or 60 minutes after age was last verified. This requires

sites to re-verify the age of every visitor at least hourly. The only reason that requirement would have been added to the law would have been to prevent exactly this sort of "leaving the door unlocked" access, under the assumption that someone other than the original age-permitted user might have access to the site handed off to them. 1984, indeed.

Matt Storms

Is it possible that Discord needed to keep the age verification data as proof of verification (In case of audit or lawsuit, or proof of compliance with regulations)

That's a great question. Looking at the recent legislation regarding age-gated access to Internet content, there's very clear and explicit language stating that any and all personally identifying information (PII), including image or data derived from images, **must be deleted** immediately after it has been used for age verification. And even Discord's own support information says:

"Discord and k-ID do not permanently store personal identity documents or your video selfies. The image of your identity document and the ID face match selfie are deleted directly after your age group is confirmed, and the video selfie used for facial age estimation never leaves your device."

Unfortunately, for those more than 70,000 users whose identity documents Discord acknowledged were leaked, this doesn't appear to be true, and given how sensitive people understandably are about having their identity documents leaking onto the Internet, coupled with how litigious the world has become, this might be a mistake that gets Discord's provider into some very hot water.

While the fine print of whatever agreement k-ID might have its users click on might provide a legal loophole and some maneuvering room, what little good news there is amid all of the recent age-gating legislation at least stipulates that whatever information is used for the determination must be immediately deleted once that determination has been made. It would be great if that were to happen.

Brian Orme

Steve, I'm listening to 1047 right now and had to pause it to send you a note.

I am the father of three kids. My youngest is a teenager and my older two are now adults. While this new Texas law is at least a step, it won't help much. I'm hopeful that an age validation standard will be established that is secure and simple. This is a hard problem, since it hits the center bullseye of the definition of PII.

Raising my older two, there is one obvious fact. Our children are not like us, who grew up without the internet. Kids grew up with the internet like we grew up with electricity. They live, eat, and breathe it. They can get around everything! They buy reloadable credit cards at dollar general, to appear as adults. My 18 year old son told me he simply used my birthday whenever he registered for a service to get around all the filters. Same last name.

On that note, the problem with this new law is that they are locking the gate on the two foot tall fence, while neglecting to lock the house doors. Once kids have a child friendly app installed, the problem is what happens inside the app and developers' neglect of monitoring their own services. This is especially true when developers incorporate the app with some ability for users to communicate among themselves.

It was recently discovered that a friend's son was being groomed via PINTEREST CHAT by a woman halfway across the United States. I'm thankful for his Mother's perception, who noticed behavior changes and took action. But who would have ever thought when their child asked permission to install Pinterest, that this age-appropriate app would have the ability to cause such harm. The same obviously goes for Minecraft, Roblox, and many many other apps.

The age requirement in this, and most cases, is truly useless. Require all the age verification you want. It will not help the issue, except for a small fraction of extreme apps and websites. The complexity for parents to set up child accounts, thus far, is so frustrating that even myself, a certified security professional, just gave up. A case in point, while auditing my subscriptions recently, I realized that I was paying for three separate Spotify family accounts. I don't have answers - just some parental observations trying to raise kids in this digital world.

These new requirements will be ineffective until developers and store owners:

1. *Make it stupid simple for parents to create and manage family accounts.*
2. *Enable parents visibility and proactive notifications into what's actually happening INSIDE the apps.*
3. *Force developers to either shutdown or actively monitor (and be held accountable) for their in-app communication services.*

Until these things happen, this age verification service will only be an annoying speed bump. Thank you for all you and Leo do each week! /Brian

I thought the points Brian made were certainly good ones. I'll be interested to see how Internet-savvy minors arrange to circumvent these new restrictions. But Brian's point about the social networking content carried by otherwise innocuous apps was clearly important. It's unclear how that will eventually be addressed, but it seems that it would need to be. We know that apps such as Facebook or 'X' do not, in and of themselves, have an age-specific rating. It's the content they communicate that these Texas legislation appears to be completely naive about. As we know, the state of Mississippi deal with this by legislating against any social media of any kind, but even then, what about interactive communications among game players? This is one slope that seems beyond slippery.

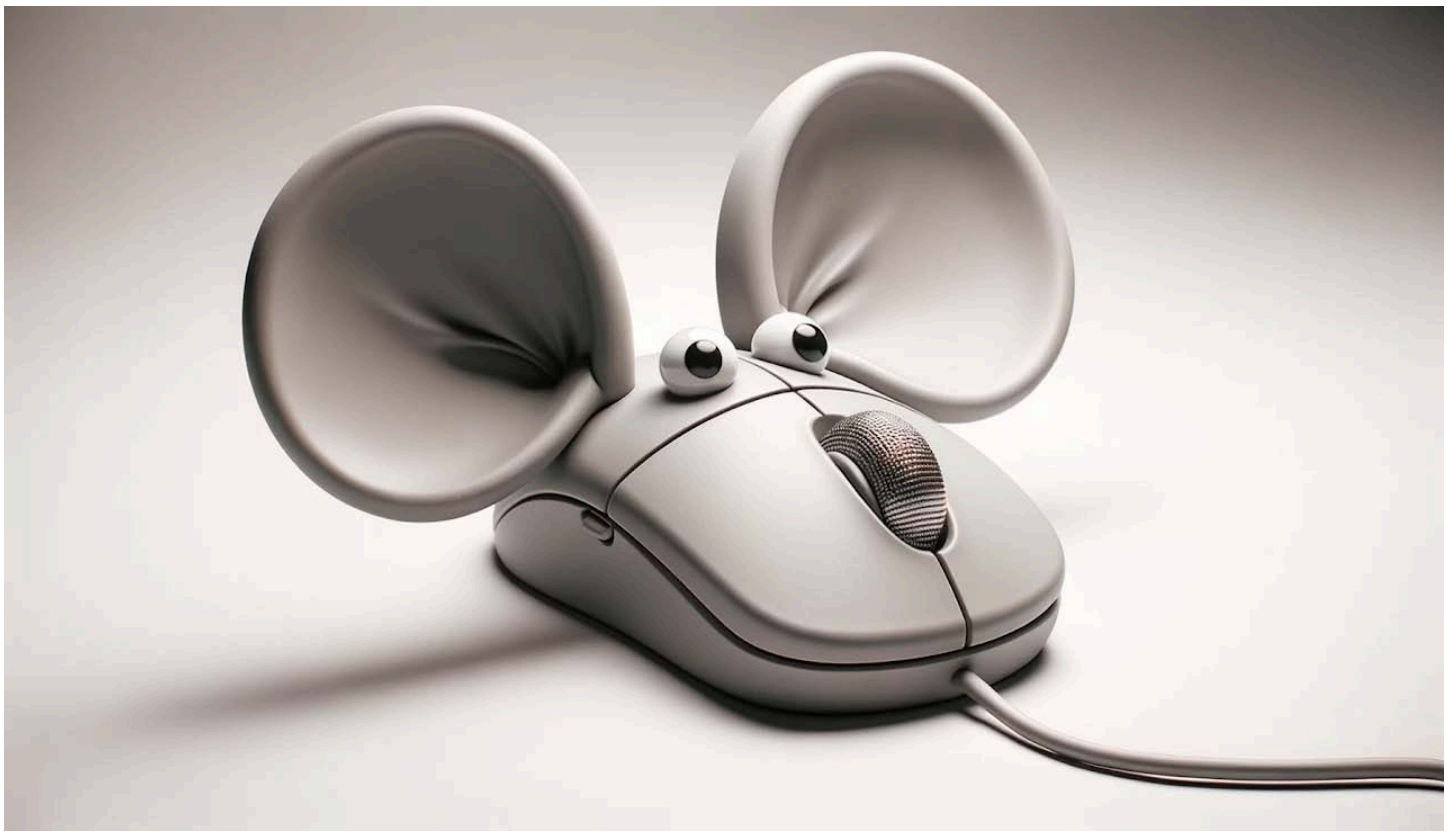
The Diplomat

Season 3 on Netflix

Leo and I are both huge fans of a "The Diplomat". So much so that we've probably mentioned it previously. So I just wanted to make sure that anyone who feels as we do knew that Netflix released its entire 8-episode third season last Thursday, October 16th. It may not be for everyone. Nothing is. But if it is for you, as it is for Leo and me, it's so astoundingly good that almost feels like it should be a guilty pleasure.

Mic-E-Mouse

Is your computer's high-resolution mouse eavesdropping on you?



https://sites.google.com/view/mic-e-mouse

Through the years of this podcast we've had a lot of fun examining a range of bizarre and often surprising side-channel attacks that have been able to exfiltrate a surprising amount of information from the surrounding environment. It turns out that not only can you bounce a laser interferometry beam off a vibrating window to recover the spoken audio on the other side of the glass inside a room a long ways away, but a laser can also be, and has been, bounced off a large plant leaf, a balloon, a bag of chips, and even an exposed lightbulb innocuously hanging in the room. We've seen keyboard keystrokes recovered with the aid of an inconspicuously placed nearby smartphone, and we've even seen the reflections of WiFi used to locate people moving around inside a room on the other side of a solid wall. We've seen the power supply's fan speeds controlled to change its sound to transmit low-bandwidth information and the sounds made by its switching power supply similarly modulated for the covert transmission of information.

So, perhaps we should not be overly surprised to learn that today's contemporary desktop mouse, thanks to the ever growing demands of high-speed gaming, has become so sensitive to its surroundings that it, too, is able to detect, pick up and transmit the sounds of ambient conversations. A team of five researchers in the Department of Electrical Engineering at the University of California, Irvine have worked to create "Mic-E-Mouse" — a mouse turned into a microphone (of sorts) thanks to its ability to perceive the room's vibrations. I say "of sorts" because of what these guys had to go through to make this work at all.

Before I go any further, for the sake of strict scientific accuracy, I feel that I should note, just for the record, that this is not ***actually*** the first time we've seen someone speaking into a mouse. 39 years ago in 1986, during the movie *"Star Trek IV: The Voyage Home"* the Enterprise's chief engineer, Montgomery Scott, first picked up and spoke into the mouse of an Apple MacIntosh PC, naturally assuming it to be a microphone, and that the computer would be able to take his verbal instructions to show the molecular design of transparent aluminum. Of course, at the time that was science fiction and meant to be humorous. But as we so often see, what was once a flight of science fiction fancy has now become all too real. The researchers feel that the threat potential from covert eavesdropping and spying through mice is all too real. The Abstract of their paper explains:

> *Modern optical mouse sensors, with their advanced precision and high responsiveness, possess an often overlooked vulnerability: they can be exploited for side-channel attacks.*
>
> *This paper introduces Mic-E-Mouse, the first-ever side-channel attack that targets high-performance optical mouse sensors to covertly eavesdrop on users. We demonstrate that audio signals can induce subtle surface vibrations detectable by a mouse's optical sensor. Remarkably, user-space software on popular operating systems can collect and broadcast this sensitive side channel, granting attackers access to raw mouse data without requiring direct system-level permissions.*
>
> *Initially, the vibration signals extracted from mouse data are of poor quality due to non-uniform sampling, a non-linear frequency response, and significant quantization. To overcome these limitations, Mic-E-Mouse employs a sophisticated end-to-end data filtering pipeline that combines Wiener filtering, resampling corrections, and an innovative encoder-only spectrogram neural filtering technique.*
>
> *We evaluate the attack's efficacy across diverse conditions, including speaking volume, mouse polling rate and DPI, surface materials, speaker languages, and environmental noise. In controlled environments, Mic-E-Mouse improves the signal-to-noise ratio (SNR) by up to +19 dB for speech reconstruction. Furthermore, our results demonstrate a speech recognition accuracy of roughly 42% to 61% on the AudioMNIST and VCTK datasets.*
>
> *All our code and datasets are publicly accessible on Mic-E-Mouse website https://sites.google.com/view/mic-e-mouse.*

In other words, modern optical mice will respond to the surface vibrations of the surface they're resting on and any standard app running that the machine can monitor the mouse closely enough to exfiltrate that rough and raw vibration data to an outside eavesdropper. From there, although this is just the beginning, bring the power of today's massive data processing to bear, what the mouse has heard to cause it to report the vibrations that it has can be determined.

I'm reminded of some different data reconstruction research we covered, where the upshot was that visually blurring text in order to obscure it was no longer safe because while the text's image could not be algorithmically "unblurred", if the text's font were known – which is often not difficult – the amount of blur could be determined and modeled. At that point, a brute force attack could be launched by rapidly trying all possible underlying characters, proceeding from left to right, matching the exact "blur", until the entire hidden message was deblurred.

Similarly, even if a mouse's vibrations are nowhere near audio quality, mapping the audio that would have resulted in those vibrations solves the same problem. To put some meat on these bones, the researchers explain:

> *The proliferation of low-cost, high-fidelity sensors in consumer devices has greatly improved user experience in common computing tasks. From lower response times to more adaptive workflows, these devices have increased productivity while remaining affordable to the average consumer. The lion's share of these improvements is found in the category of user input devices, including styli, mice, and monitors. More specifically, improvements in mouse sensor technologies have allowed commercial offerings to operate with a sample rate of 4KHz, with a growing selection of products that also support 8KHz.*
>
> *Consumer-grade mice with high-fidelity sensors are already available for under 50 U.S. Dollars. As improvements in process technology and sensor development continue, it is reasonable to expect further price declines. Furthermore, mouse sensors' resolution and tracking accuracy also follow the same pattern, with steady improvements each year. Ultimately, as lower performance mice leave the consumer space, these developments lead to an increased usage of vulnerable mice by consumers, companies, and government entities, expanding the attack surface of potential vulnerabilities in these advanced sensor technologies.*
>
> *The rise in work-from-home policies has led to the widespread adoption of new technologies and practices, making it more difficult for employers and government institutions to control the physical operating environments of their workforce. While these arrangements often boost employee sentiment and productivity, the security implications of work-from-home policies are still being understood. Specifically, attacks exploiting personal peripherals on work computers, such as keyboards, microphones, styli, earphones, mechanical hard drives, and even USB devices, have become increasingly common. Even in relatively secure office environments, the threat posed by these exploits is still significant, especially for unknown or poorly understood attack vectors.*
>
> *We posit that the seemingly innocuous computer mouse is the source of yet another vulnerability. Importantly, we claim that recent advancements in mouse sensor resolution can be sufficient to enable a side-channel attack capable of extracting user speech. Through our Mic-E-Mouse pipeline, vibrations detected by the mouse on the victim user's desk are transformed into comprehensive audio, allowing an attacker to eavesdrop on confidential conversations. This process is stealthy since the vibration signals collection is invisible to the victim user and does not require high privileges on the attacker's side. Potential adversaries can collect user-space mouse signals and remotely use the Mic-E-Mouse pipeline to convert raw data packets into audio.*

I'll interrupt to observe that websites are also able to obtain mouse coordinates in real time. So it might be that visiting a site which innocuously downloads and runs some high-performance web-assembly code might now be sufficient to collect sufficient mouse vibration data to later reverse-engineer speech that was taking place during that visit. You would assume that having your microphone disconnected or muted would be sufficient. But perhaps not. The researchers continue:

> *Modern optical mice employ various methods to provide precise movement tracking under different sensitivity settings. Over the last two decades, optical mice leveraging a high-*

performance CMOS camera with an onboard Digital Signal Processor (DSP) have become the preferred design choice. Generally, optical sensors enhance reliability and fidelity through the use of self-illumination, typically from an independent diode or an integrated laser. By taking thousands of snapshots of the illuminated surface under the mouse, the DSP can then compare each successive image in order to determine the direction of movement. The rate at which this process happens is determined by the sensor's frame rate, measured in Frames Per Second (FPS). Each frame is processed via an on-chip correlation algorithm to provide a 2-dimensional displacement to the host computer. The described process can be broken down into two key elements: (i) the imaging sensors and (ii) the image processing and movement detection algorithm.

Rather than relying on expensive Charge-Coupled Device (CCD) sensors, the sensor in an optical mouse is typically a Complementary Metal-Oxide-Semiconductor (CMOS) image sensor collecting up to 30x30 pixels' worth of data per frame, where each pixel represents the intensity of the reflected light at that point. This basic mini-camera is a critical component for implementing speckle-pattern detection. Some sensor models, such as the PixArt PMW3552, capture data using an 18×18 pixel grid, while others can record up to 30×30 pixels, depending on the manufacturer's specifications. For visualization purposes, we destructively studied a PixArt PMW3552 sensor in our institutional lab. This sensor features an 18×18 CMOS pixel grid and is designed to interface directly via USB. Speckle patterns are random, granular intensity patterns produced when coherent light, such as laser light, is scattered by a rough surface. When an optical mouse is moved across a surface, the speckle pattern on the surface changes smoothly and reliably. The CMOS sensor captures these changes in the speckle pattern frame by frame and processes them to detect movement. These movement detection algorithms allow for the translation of data into corresponding coordinate deltas.

The researchers go into an extreme level of detail which should satisfy anyone wishing to deeply understand their work. Anyone listening who wants more than I'm going to share here on the podcast is invited to follow the links at the end of the show notes which points to all of their research including all of the code they developed to pull this off.

The important point I wanted to make, however, is that none of this would have been even remotely possible without what we now know of as AI. A crucial aspect of their system's success was their ability to re-train an existing OpenAI "Whisper" model using the X & Y movement outputs from actual mice. Whisper is OpenAI's open-source speech recognition system. It's specifically designed to take input material representing spoken audio and convert it into text. This team was able to cleverly retrain and repurpose Whisper to accept incredibly low-quality audio, barely recognizable as anything, and obtain up to 65% word recognition accuracy.

So we may need to be careful about what secrets we utter around our mice. You may not want to repeat important passwords out loud. Your mouse, might indeed, have very big ears!

- https://sites.google.com/view/mic-e-mouse
- https://arxiv.org/html/2509.13581v1
- https://www.csoonline.com/article/4069723/computer-mice-can-eavesdrop-on-private-conversations-researchers-discover.html