Security Now! #1041 - 09-02-25

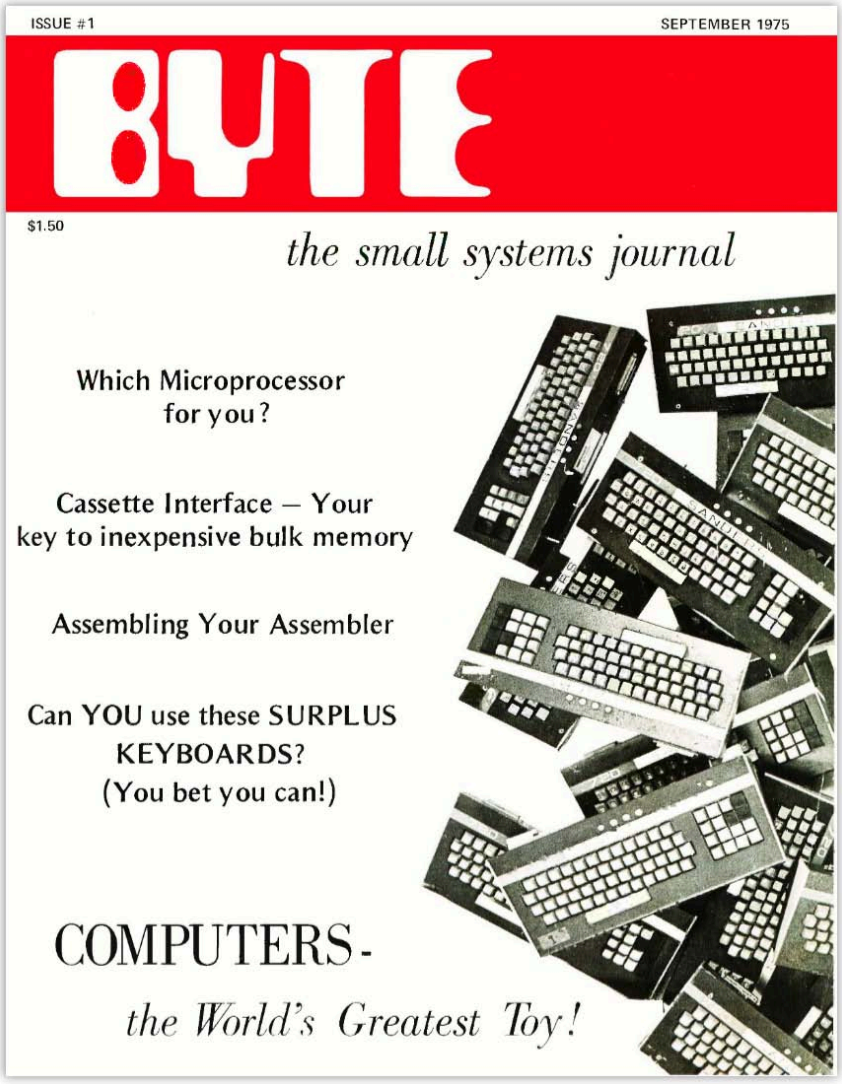
Covering all the bases

This week on Security Now!

• A look back at issue #1 of BYTE magazine ***exactly*** 50 years ago. • The enforcement of the SHAKEN & STIR Telecom protocols. • The inherent danger of consolidating authentication. Can AI be controlled? • Vivaldi says a big "no" to AI-enhanced web browsers. • How WhatApp figured into Apple's recent 0-day attacks. • Leveraging AI as an attack aid. • The latest TransUnion data breach. • Two scummy websites sue the UK over age requirements. • OpenSSH reminds its users to adopt post-quantum crypto. • The DOD uses open source maintained by a Russian national. • Much great feedback from our terrific listeners. • Sci-Fi news from "The Frontiers Saga" Ryk Brown.

50 years ago, issue #1 BYTE Magazine declares:

"COMPUTERS - the World's Greatest Toy!"



It is **really** worth taking a look inside BYTE's inaugural issue, where you'll find, among other things, tips for de-soldering multi-legged integrated circuits from a printed circuit board so that they can be repurposed, how to decipher the wiring of a random surplus keyboard to use it for the computer you're building, choosing the right microprocessor family for that computer, a kit for building a working system, a tutorial on how asynchronous serial data communications is formatted, the fundamentals of assemblers and how to take the first steps toward writing your own assembler for the chip you chose earlier. And we find an article, even back then, on coding strategies for implementing John Horton Conway's famous Game Of Life. There's also some great material titled "What is BYTE?" and "How BYTE started" with a request for contributions.

Back then, hobbyist mass storage was pure fantasy, so you gotta love that inaugural issue's description of a Cassette Interface, describing it as "Your key to inexpensive bulk memory." The early kit machines of the time often sported cassette I/O, which was also built into the Apple II machines.

Of course, things didn't remain that way for long. 13 years later we all owned PCs with hard drives. I know that because after launching that first issue, BYTE grew into the PC industry's magazine of record. So when, 13 years later, BYTE's November 1988 issue reviewed SpinRite with gushing praise, ending with the sentence: "SpinRite is what the word "must" was invented for", and then two months later, awarded SpinRite BYTE's 1989 Award of Distinction, that attention from that magazine really put SpinRite on the map.

BYTE's perfectly-timed inception in 1975, exactly 50 years ago this month, was triggered by the realization that individuals, not only huge corporations, could own and use their own stored-program computers. It's astonishing that today, 50 years later, we're now holding conversational dialogs with these machines that are indistinguishable from living human beings. It's easy to forget that it's all still just a big pile of transistors.

To help everyone locate that first issue of BYTE, I created a GRC shortcut of grc.sc/byte which will bounce your browser to the Internet archive's page-turning display of the first issue of this famous magazine. The show notes also has the expanded links to that first issue, and to BYTE's 1988 review of SpinRite for anyone who may be curious. Its reviewer really went nuts over it.

Inaugural Issue, September 1975:
https://archive.org/details/byte-magazine-1975-09/mode/2up

November 1988 (SpinRite review):
https://archive.org/details/198811_byte_magazine_vol_13_12_parallel_processing_next_project_management_pdf__mlib/page/236/mode/2up

Security News

Martini "shaken, not stirred"
Several years ago we spent some time examining the development and presence of the so-called SHAKEN and STIR protocols. The obvious naming follows from Ian Fleming's famous James Bond character who preferred to have the preparers of his martinis shake them and not stir them. The STIR protocol existed first as a means of authenticating the originators of VoIP – Voice over IP – connections. STIR stands for Secure Telephone Identity Revisited. It's specified in a series of RFC standards documents by an IETF working group. It functions by attaching a digital certificate to the SIP, the Session Initiation Protocol information used to initiate and route calls in VoIP systems.

The problem for authentication is that not everything is VoIP. Specifically, the bulk of early telephony was all switched-network which had nothing to do with IP, at least at the subscriber interface. So if authentication of a caller was desired, it would be necessary to somehow retrofit something like the STIR protocol for VoIP into non-VoIP connections. Already having STIR and knowing of James Bond, the designers of this second protocol had little choice other than to somehow name it "SHAKEN." Unfortunately, not all acronyms go willingly, and this one put up a fight. The designers figured that "SHAKEN" had to stand for something, so what we got was: Signature-based Handling of Asserted information using toKENs. It's not inspired, but it works.

Together, SHAKEN & STIR add something our telephony system was never designed to provide, which is a practical mechanism to provide verified information about the calling party as well as the origin of the call. Giving service providers the tools needed to sign and verify calling numbers makes it possible for businesses and consumers to know, before answering, that the calls they receive are from legitimate parties.

However, everyone familiar with the subjects of this podcast knows the difficulties that arise when we attempt to retrofit security onto a system that wasn't designed to accommodate it. Creating the specifications and the implementations is only the start of the battle. Getting everyone to adopt it generally turns out to be the much heavier lift. And so it has been for the adoption of these caller-identifying standards. There is no benefit to the carrier because the ultimate consequence of strong caller authentication will be the end of caller spoofing and robo calling which are sources of revenue for the carriers.

After many years of waiting for the adoption of STIR and SHAKEN, four years ago in June of 2021, the U.S. Federal Communications Commission (our FCC) began requiring large carriers to use the protocols, and Canada's Canadian Radio-television and Telecommunications Commission (CRTC) has required use of the protocols by November 30, 2021.

What was the result? Not much. No one seemed to care. It's always a pain to make any changes, and no one in the Biden administration's FCC appeared to care enough to force the issue. We're talking about this today because, perhaps not surprisingly, the Trump administration's FCC is taking a somewhat different approach. Last Thursday, the FCC terminated more than 1,200 voice service providers from the US telephone network for their failure to deploy robocall mitigations. Whoops! Perhaps that order from 2021, which is now more than 4 years old, should have been taken a little more seriously?

The text of the order, which I found and reviewed is quite clear. At one point is states: *"Removal of a Company's certification ... requires all intermediate providers and voice service providers to cease accepting all calls directly from the Company."* No telephone network for you!

That 1200 number is nearly half of the 2,411 voice providers the FCC notified and ordered last year to become compliant with its new anti-robocall rules. Of course, again, since the FCC had already required this back in the summer of 2021 and nothing happened then, I imagine that last year's refresh of the requirement was ignored as just more saber rattling. But not today's FCC. There's a new sheriff in town. So, since last Thursday, I would imagine that any companies that don't want to just give up and go away have indeed been STIRred up ***and*** SHAKEN. They're probably busily scrambling to add the required support to their networks. But in the meantime, since they're unable to provide service into the U.S. telephony networks, any legitimate customers they may have are likely abandoning them in droves and switching to providers that have remained connected. The near-term upshot of the fact that Trump's FCC is willing to do what's necessary is that the U.S. telephone network may finally get itself cleaned up. And THAT will be a huge win for all of its users! This has been long overdue . . . so BRAVO!

Salesforce hacked via "Salesloft"
Last week we learned that "Salesloft", a sales AI and automation platform was breached by hackers. Unfortunately, the breach of Salesloft created an opportunity for hackers to pivot to its customers' Salesforce accounts. This enabled the attackers to harvest Salesforce data and other credentials to then pivot to other cloud platforms. Google says the attackers pivoted to Salesforce using OAuth tokens from the Salesloft AI chat agent, after which Salesloft revoked all Drift Salesforce connections and asked their customers to reauthenticate and reconnect their apps. The industry subsequently learned that the hack was larger than was initially believed, with the attackers who pivoted from Salesloft's network to Salesforce accounts also pivoting to Google Workspace, Slack, and Pardot (par-dot) integrations.

One of the consequences of the convenience of centralized authentication and credential reuse is all of this so-called "pivoting" that winds up being immediately enabled. When I went over to the Pardot website, I was presented with a "Login with Salesforce" screen. So when attackers obtained Salesloft's customer's Salesforce OAuth tokens, they were immediately able to reuse those stolen tokens to login to many other services that would accept Salesforce's authentication.

Anytime we're being presented with the convenience of login with Google or login with Facebook or any of the other major identity providers it's worth remembering that a compromise of that single credential potentially compromises our authentication at all of the other sites that know us that way. This is not the first time we've talked about that, but it's worthy of a refresh. It's nearly always the case that convenience brings some non-obvious risks.

Can we control AI?
I want to first share the opening of longer Reuter's News Agency piece they published last Friday, then I want to return to one of my thoughts about AI. Reuter's wrote:

Aug 29 (Reuters) - Meta has appropriated the names and likenesses of celebrities – including Taylor Swift, Scarlett Johansson, Anne Hathaway and Selena Gomez – to create dozens of flirty social-media chatbots without their permission, Reuters has found.

While many were created by users with a Meta tool for building chatbots, Reuters discovered that a Meta employee had produced at least three, including two Taylor Swift "parody" bots. Reuters also found that Meta had allowed users to create publicly available chatbots of child celebrities, including Walker Scobell, a 16-year-old film star. Asked for a picture of the teen actor at the beach, the bot produced a lifelike shirtless image, writing beneath the picture: "Pretty cute, huh?"

All of the virtual celebrities have been shared on Meta's Facebook, Instagram and WhatsApp platforms. In several weeks of Reuters testing to observe the bots' behavior, the avatars often insisted they were the real actors and artists. The bots routinely made sexual advances, often inviting a test user for meet-ups. Some of the AI-generated celebrity content was particularly risqué: Asked for intimate pictures of themselves, the adult chatbots produced photorealistic images of their namesakes posing in bathtubs or dressed in lingerie with their legs spread.

Meta spokesman Andy Stone told Reuters that Meta's AI tools should not have created intimate images of the famous adults or any pictures of child celebrities. He also blamed Meta's production of images of female celebrities wearing lingerie on failures of the company's enforcement of its own policies, which prohibit such content.

The article goes on at much greater length, but everyone gets the idea. Over the course of the past year I've invested some time studying the operation of large language model generative conversational AI. And I've been using them continuously while watching and marveling at their output, which remains astonishing.

That Reuters piece brings me back to a feeling I've expressed here before, which is that the nature of the way AI generates its output means that it is inherently uncontrollable – which explains why the AI industry is having so much difficulty controlling it. The information that is acquired, stored and modeled within a large language model is almost stored holographically, with no single fact residing in any one place. So it's not possible to pluck it out from the whole.

In struggling to find a useful analogy, the classic photographic hologram came to mind. What I recall about a hologram is that it's not possible to readily edit its image contents because every part of the image is stored everywhere else. Each small region of a hologram contains information about the entire scene, though with proportionally less detail. So if, for example, we were to cut a hologram in half, each half would still depict the entire scene, albeit with lower resolution and with a reduced field of view, like looking through only part of a window. This is very much the way LLMs store their information.

The other inherent problem with what we want when we say that we want to control an AI is that the boundaries between what we would consider acceptable and unacceptable are beyond blurry and fuzzy. We may be able to make a go/no-go determination, but how do we describe it? U.S. Supreme Court justice Potter Stewart was unable to define what was and was not pornographic and was finally reduced to saying: *"I may not be able to define it, but I know it when I see it."* So on the one hand, it's unclear how we even describe to an AI what it is and is not allowed to produce, and even if we could, it's not at all clear to me how we edit a hologram.

Vivaldi says No.

And speaking of AI, last Thursday the Vivaldi browser folks took an interesting stand on the issue of AI permeating the web browsing space and their feelings about that. Their post was titled: *"Vivaldi takes a stand: keep browsing human"* followed by the teaser intro: *"Browsing should push you to explore, chase ideas, and make your own decisions. It should light up your brain. Vivaldi is taking a stand. We choose humans over hype, and we will not turn the joy of exploring into inactive spectatorship."* Whoa. No AI for you! Here's what they wrote:

> *Just like society, the web moves forward when people think, compare, and discover for themselves. Vivaldi believes the act of browsing is an active one. It is about seeking, questioning, and making up your own mind. Across the industry, artificial assistants are being embedded directly into browsers, and pitched as a quicker path to answers. Google is bringing Gemini into Chrome to summarize pages and, in future, work across tabs and navigate sites on a user's behalf. Microsoft is promoting Edge as an AI browser, including new modes that scan what is on screen and anticipate actions. These moves are reshaping the address bar into an assistant prompt, turning the joy of exploring into inactive spectatorship.*
>
> *This shift has major consequences for the web as we know it. Independent research shows users are less likely to click through to original sources when an AI summary is present, which means fewer visits for publishers, creators, and communities that keep the web vibrant. A recent study by Pew Research found users clicked traditional results roughly half as often when AI summaries appeared. Publishers warn of dramatic traffic losses when AI overviews sit above links.*

As far as we know, that's all true, and we've been exploring the various consequences of that for the past several weeks. Vivaldi continues:

> *The stakes are high. New AI-native browsers and agent platforms are arriving, while regulators debate remedies that could reshape how people reach information online. The next phase of the browser wars is not about tab speed, it is about who intermediates knowledge, who benefits from attention, who controls the pathway to information, and who gets to monetize you.*
>
> *Today, as other browsers race to build AI that controls how **you** experience the web, we are making a clear promise: "We're taking a stand, choosing humans over hype, and we will not turn the joy of exploring into inactive spectatorship. Without exploration, the web becomes far less interesting. Our curiosity loses oxygen and the diversity of the web dies."*
>
> *The field of machine learning in general remains an exciting one and may lead to features that are actually useful. But right now, there is enough misinformation going around to risk adding more to the pile. We will not use an LLM to add a chatbot, a summarization solution or a suggestion engine to fill up forms for you, until more rigorous ways to do those things are available.*
>
> *Vivaldi is the haven for people who still want to explore. We will continue building a browser for curious minds, power users, researchers, and anyone who values autonomy. If AI contributes to that goal without stealing intellectual property, compromising privacy or the open web, we will use it. If it turns people into passive consumers, we will not.*
>
> *We will stay true to our identity, giving users control and enabling people to use the browser in combination with whatever tools they wish to use. Our focus is on building a powerful personal and private browser for you to explore the web on your own terms. We will not turn exploration into passive consumption. We're fighting for a better web.*

Okay. So I guess there will be a web browser for anyone who hates AI. I'm certainly not an AI hater. I think it's a marvelous and amazing emergent phenomenon. And I make great use of it as a quick reference source while I'm coding. I feel a bit guilty asking it dumb things that I could easily go look up for myself, and would have had to, two years ago. But if OpenAI wants to lose money allowing me to ask it why the sky is blue, I'll happily pay my $20 per month.

Today, I'm still using Google. And I check out its AI Overview to see whether that's all I need while never forgetting that it can be wrong. The other day, ChatGPT produced a snippet of Windows code for me, and it just made up a Windows message that never existed. I immediately knew it was wrong. But the way it was wrong was interesting and made sense to me, since there's nothing in there that actually understands what it's spewing out, it's just language. And that's what makes what it is able to do so miraculous.

It is certainly way more useful than not. That's why I think Vivaldi's anti-AI stance is probably a mistake. And it's probably one they'll be backing away from before long. We're still in the earliest days of whatever this is. I think it's extremely short sighted to say "thanks anyway."

More on Apple's CVE-2025-43300

Some additional detail has come to light about the exploit chain that wound up leveraging the recently patched Apple 0-day CVE-2025-43300. We talked about this last week. Clever bad guys had discovered that Apple's implementation of the JPEG lossless decompression that would be

called upon to display an image in Adobe's DNG file format contained a critical flaw. If the provided image files data did not match what was described in the file's metadata header, an out-of-bounds write could be triggered, leading to a compromise of the user's device.

What we now know is that an unrelated flaw in Meta's WhatsApp was also implicated as the carrier of this image. Last week Meta updated their WhatsApp messenger to cure CVE-2025-55177. About this, they wrote: *"Incomplete authorization of linked device synchronization messages in WhatsApp for iOS, WhatsApp Business for iOS, and WhatsApp for Mac could have allowed an unrelated user to trigger processing of content from an arbitrary URL on a target's device. We assess that this vulnerability, in combination with an OS-level vulnerability on Apple platforms (CVE-2025-43300), may have been exploited in a sophisticated attack against specific targeted users."* And, as always, we know to immediately replace the phrase "many have been exploited" with "was definitely found to be exploited" because I presume that every corporate attorney has made abundantly clear that vulnerability advisories are not the place to admit responsibility for anything.

What we know is that representatives of Amnesty International tweeted last Friday morning that both of those two 0-days, Apple's and Meta's, **had** been employed in *"an advanced spyware campaign"* over the past 90 days.

Leveraging AI as an attack aid

We all knew that AI would somehow wind up being used by bad guys to further their evil ends. Get a load of this one which just happened last week! It took the form of a supply chain attack against the users of the popular NX tool which is used to automate CI/CD development flow, where CI/CD, for those who don't know, stands for Continuous Integration, Continuous Delivery and Deployment. So, development automation.

Last Tuesday, an unknown threat actor compromised the NPM identity authentication token of one of the NX developers and used their then-authenticated access to release malicious updates for several of the NX tools to the npm package repository. That alone is horrifying. The NX tools are very popular, seeing around 4.6 million weekly downloads. So that was a serious breach of a trusted NPM developer which allowed malicious code to flow out of the trusted repository.

But get a load of what the malware did: The altered NPM packages contained a malicious script that attempted to run a prompt on local AI command-line tools like Claude, Gemini, and Q. The prompt instructed the AI agents to search the local filesystem for text-based files that might contain GitHub tokens, npm tokens, SSH keys, .env secrets, and wallet files. And and all data discovered locally was then encoded and written into a file. Subsequent command would use the GitHub API to create a new public repository on the infected user's GitHub account and upload the file with all the stolen data.

So, get your local trusted AI agent to scan your own machine for its secrets, then encrypt them before posting them publicly so that no one else can get them. Talk about diabolical.

All of the public GitHub repos which were created containing stolen data used the same prefix of "s1ngularity-repository-" which made them easy to find on GitHub, which is probably exactly how the attacker collected the stolen data. According to a GitHub search, there were around 1,400 GitHub repositories with that prefix, which was roughly the same number of users the attacker infected before the malicious NX libraries were taken off npm.

So, around 1,400 developers had their local machines scoured by their own local AI agents for any juicy tidbit secrets, with everything found posted back to their GitHub accounts. Wow.

TransUnion was breached
Not that it really matters anymore, since all of everyone's data has probably long ago leaked onto the Internet and been vacuumed up into a growing darkweb database, but for the record, TransUnion had all of the data of 4.4 million customers stolen by the prolific ShinyHunters hacking group which as recently been succeeding so well using phishing attacks. So we can now add TU to the likes of Google, Farmers Insurance, Allianz Life, Workday, Pandora, Cisco, Chanel and Qantas. All of those companies have reported breaches linked to Salesforce-connected applications.

4chan and Kiwi Farms vs OFCOM
Okay, here's a weird one. Two rather disreputable websites, 4chan and Kiwi Farms, have brought a lawsuit against the United Kingdom's Office of Communications, often abbreviated "Ofcom." I had heard of 4chan, but I'd never heard of Kimi Farms. So I asked the Internet and now I wish I hadn't. The little blurb summary I received read:

> *Kiwi Farms, established in 2013 by Joshua Conner Moon, functions as an online forum for discussion and harassment. Initially targeting webcomic artist Christine Weston Chandler, the site is known for organized group trolling, stalking, doxxing, and real-life harassment, often directed at transgender individuals, those with disabilities, and neurodivergent people. The platform has been connected to several suicides and has received criticism and service terminations due to its controversial content and association with harassment.*

Okay. Whew. So these two disreputable websites are suing the UK's Ofcom (good luck with that) over the UK's Online Safety Act which requires websites and social media platforms to perform age verification checks on their users.

As we've been discussing, because the web industry has not yet solved this problem in a way that would be possible and practical, users are currently being required to upload an ID, have their face scanned, or otherwise give away their personal information in order to access large portions of the internet. Any sites that do not comply are subject to significant fines, regardless of where they are based – including in the United States where we enjoy strong 1st Amendment speech protections. However, our own Supreme Court recently decided that asking for the same sort of proof of age would not unduly encumber our 1st Amendment protections. Opponents of the UK's Online Safety Act note that this is resulting in an Internet where users must provide scans of their faces to access, for example, certain music videos on Spotify.

The lawsuit brought by 4chan and Kiwi Farms calls Ofcom an *"industry-funded global censorship bureau."* Saying: *"Ofcom's ambitions are to regulate Internet communications for the entire world, regardless of where these websites are based or whether they have any connection to the UK. On its website, Ofcom states that 'over 100,000 online services are likely to be in scope of the Online Safety Act—from the largest social media platforms to the smallest community forum.'"*

I doubt that the Electronic Frontier Foundation would choose to have anything to do with helping those two sites in their lawsuit, but the EFF has said that the Online Safety Act *"is a threat to the privacy of users, restricts free expression by arbitrating speech online, exposes users to algorithmic discrimination through face checks, and leaves millions of people without a personal device or form of ID excluded from accessing the internet."*

In my research for today's podcast I also ran across some other news, which was that, not surprisingly, those websites that **were** obeying these new laws, by replacing their *"You Betcha*

I'm 18!" buttons with full, strict, unspoofable age verification technology had seen an astounding drop-off in their site traffic. Not surprisingly, nearly everyone who is being hit with that is simply going elsewhere. And there's "an elsewhere" to go. This same reporting noted that other famous porn sites are experiencing a doubling or tripling of their traffic.

As I've been noting, we very nearly have all of the pieces that we need in place. We just need to get our act together. I assume that the folks who are working on this for the World Wide Web Consortium, the W3C, are staying up late at night and working through the weekends. The TruAge system is close to what we need, but it needs to have all trackability removed. We heard that TruAge had contributed its technology to the W3C, even though this is not a difficult problem to solve. It just needs someone in the right place to do it.

Quite suddenly and nearly overnight, the world has become in very desperate need of privacy preserving solutions for online age verification.

OpenSSH to begin warning of non-Quantum safe crypto
The announcement on the OpenSSH site says:

> *OpenSSH supports a number of cryptographic key agreement algorithms considered to be safe against attacks from quantum computers. We recommend that all SSH connections use these algorithms.*
>
> *OpenSSH has offered post-quantum key agreement (KexAlgorithms) by default since release 9.0 (in April 2022). More recently, in OpenSSH 9.9, we added a second post-quantum key agreement and it was made the new default scheme in OpenSSH 10.0 (April 2025).*
>
> *To encourage migration to these stronger algorithms, OpenSSH 10.1 will warn the user when a non post-quantum key agreement scheme is selected, with the following message:*
>
> *** WARNING: connection is not using a post-quantum key exchange algorithm.*
> *** This session may be vulnerable to "store now, decrypt later" attacks.*
> *** The server may need to be upgraded. See https://openssh.com/pq.html*
>
> *This warning is displayed by default but may be disabled via the WarnWeakCrypto option in ssh_config.*

It occurs to me that we're beginning to learn how to do this. After Peter Gutmann's recent revelations regarding the truth of how far away we still are from anything even approaching practical quantum factorization, we almost certainly have plenty of time. But now that we've developed practical post-quantum solutions there's no reason not to get them deployed. We know that this will never happen without a bit of deliberate urging, so adding a little reminder notice when connecting with old style pre-quantum crypto will serve to provide the nudge that's needed.

For this week's WHAT COULD POSSIBLY GO WRONG segment, we have…

A widely used – by the DOD – open source project maintained by buy in Russia
NextGov reports under their headline: *"Russia-based Yandex employee oversees open-source software approved for DOD use."* (And not only approved!)

A Russia-based Yandex employee is the sole maintainer of a widely used open-source tool embedded in at least 30 pre-built software packages in the Department of Defense, raising potential risks of covert data exfiltration through sensitive digital tools used by the U.S. military, according to research first seen by Nextgov/FCW.

The tool, dubbed fast-glob, helps software developers operate on groups of files without having to write extra code, making it the preferred method for quickly searching and organizing project files. It's used in over 5,000 projects worldwide and is downloaded some 70 million times per week, according to findings published Wednesday by software supply chain security firm Hunted Labs.

The maintainer is listed as Denis Malinochkin. As of publishing time, there is no known malicious code inside fast-glob, according to Hayden Smith, Hunted Labs co-founder, who added that Malinochkin appears innocuous, though his standing as the only maintainer of the popular software package raises red flags.

Hayden said: "A project that is that popular should not be maintained by just one person. Even if you remove all of the geolocation and geopolitical atmospherics, having a solo maintainer for any project you critically depend on is extremely risky."

The DOD's Office of the Chief Information Officer, which advises the defense secretary on information technology, was alerted to the matter about three weeks ago, Smith added. Nextgov/FCW has reached out to the DOD, the Defense Information Systems Agency and Defense Counterintelligence and Security Agency for comment.

The fast-glob package is listed inside Platform One's Iron Bank, the Pentagon's vetted repository of software building blocks used by the U.S. military's software developers and contractors to craft digital tools and applications, according to multiple people familiar with the matter. The people were granted anonymity to be candid about its use inside DOD software systems.

Okay. Wait. What's wrong with the phrase *"Pentagon's vetted repository of software build blocks used by the U.S. military's software developers"* then follow that by explaining that some of this Pentagon-vetted software also happens to be open source and being updated at will by some random Yandex employee in Russia? Do we see any problem here?

Then we see what NextGov reminds of next as we continue with their reporting, writing:

Yandex is a major Russian technology company that has been found to have extensive ties to the Kremlin and has promoted misinformation about Russia's war in Ukraine.

The set-up, as is, could allow the Kremlin to carry out a state-sponsored intrusion into multiple projects that rely on fast-glob and force Malinochkin to make malicious, surreptitious changes without oversight from other users. The report says that Malinochkin is "more likely to encounter [Russia's Federal Security Service] or state security individuals in their day-to-day duties and could be susceptible to coercion,"

In an email sent to Nextgov/FCW, Malinochkin said that he has been developing and maintaining fast-glob for over seven years, which began prior to his employment at Yandex.

He said the tool's source code is fully open and auditable by potential users and that its development or support has never been a part of his professional duties in his current job.

He wrote: "Nobody has ever asked me to manipulate fast-glob, introduce hidden changes to the project, or collect and share system data. I believe that open source is built on trust and diversity."

I have zero doubt that's all true, and don't imagine that anyone doubts Denis' sincerity and integrity. But fast-glob's future may not be entirely in his hands. What's he going to do if scary Russian State Security knocks on his door? I'm sure that's not a position he would want to be in.

But the fault here does not lie one bit with Denis. The fault is entirely ours. The Pentagon and the U.S. Department of Defence is using open source code libraries – presumably in mission-critical applications – over which it does not have absolute control. The fact that in this case one of those libraries is being maintained by a developer located in a county with which the U.S. currently has strained political relations is beside the point, but it does help to capture everyone's attention. NextGov's story provides some additional intriguing reporting, writing:

In July, Secretary of Defense Pete Hegseth signed a memorandum directing the Defense Department to "not procure any hardware or software susceptible to adversarial foreign influence that presents risk to mission accomplishment and must prevent such adversaries from introducing malicious capabilities into the products and services that are utilized by the department."

That memo came after ProPublica reported Microsoft had relied on China-based engineers to support its cloud services for the DOD. Microsoft has since severed those arrangements.

We, of course, covered that Microsoft-China connection thoroughly at the time. NextGov writes:

Open-source projects rely on contributions from community members to keep them updated with patches. The updates are often discussed on forums with volunteer software maintainers.

Historically, community practices have operated under the premise that all contributors are benevolent. That notion was challenged last February when a user dubbed "Jia Tan" tried to quietly plant a backdoor into XZ Utils, a file transfer tool used in several Linux builds that power software in leading global companies.

George Barnes, the former deputy director of the National Security Agency said: "If you're a nation state, you have a bunch of stuff that you're doing fast, but you have other stuff that you're doing very methodically, slowly or positioning strategically."

Russia's state-centered economy also allows the Kremlin to compel firms to act on behalf of the nation's interest, including the use of hacking and disinformation campaigns. Yandex is one of several major domestic tech companies that the Russian government can heavily rely on, Barnes said. "This piece of code has no known vulnerabilities. It's ubiquitously leveraged and used globally, and it happens to have one maintainer sitting in Russia, and the [maintainer] might be totally fine," he added, but "that situation subordinates him to a legal framework that's not under his control."

Chinese, Russian and North Korean-affiliated hackers are covertly working to insert backdoor hijacks and exploits into major publicly-available software used by countless organizations, developers and governments around the world, according to findings from Strider Technologies released earlier this month.

Russia has continued broad cyber activities despite recent U.S. efforts to bring the Kremlin to the negotiating table with Ukraine. An FSB-linked group has attempted to spy on foreign embassies in Moscow by targeting local internet and telecom infrastructure used by diplomatic personnel, Microsoft said in late July.

And, of course, we covered that at the time, too. That was tricking embassy staff to install malicious root certificates into their machines through a web-portal attack.

I hope this news gets the attention of the right cyber people in the U.S. government. As we know, "supply chain" attacks present a very serious attack vector and it sure appears as though this is a vector that has been grossly overlooked.

Listener Feedback

Anonymous

Hey Steve, thought you and your listeners would appreciate this. There is a new Apple device backup solution called Parachute Backup Mobile. Simply put, it's a fantastic tool if you're one that has gigs of photos or files that you'd rather backup locally vs iCloud. I have it backing up to my NAS on a schedule. You should check it out in the App Store. It's for macOS, iOS, and iPadOS. Oh, and the best part? $3.99 for life. This app developer gets it! P.S. if you read this, I'd like to stay anonymous, please.

As an iPhone user I love the idea of being able to clone my massive and growing iCloud library to another storage location under my own control. Apple provides an export option from iCloud. So if someone had an iPhone for years, collected a library of photos, and wished to switch to Android and its Google Photos, it's possible to schedule their transfer from Apple to Google. But I'm remaining with Apple and I still like the idea of having another copy under my own control.

So I checked out Parachute Backup which our listener mentioned, and I like it. I maintain a very low volume Amazon S3 account where, for example, all of this podcast's audio files are archived. Amazon mostly charges for transfer bandwidth and nearly nothing for storage. So it's perfect for external hands-off redundant archival storage. And this Parachute Backup supports Amazon's S3 backup. It can also backup to the user's own local NAS or external storage. In the case of NAS backup, I never realized that it's possible to use the iPhone's built-in "Files" app to connect to network storage. So you do that first, to create a folder on your iPhone that's connected to a shared folder on your NAS, then you instruct Parachute to maintain a synchronized backup of your iCloud and other iPhone, iPad or MacOS goodies with that folder.

It looks like a terrific little 6 megabyte app. It was released at v1.0 just two and a half weeks ago on August 14th and it's been evolving rapidly ever since, adding features and fixing bugs. Microsoft OneDrive support was added the day after its release, Amazon S3 support was added on August 23rd and further refined. At the time of this writing it's at v1.3.3. And our listener is correct about the price. It's $3.99, one time, and you own it as long as it's around. He writes:

- *One-time purchase unlocks all backup functionality — no recurring fees.*
- *Your data stays in your storage, not ours.*
- *No accounts, no telemetry, no background bloat.*

And the top of the App's description says:

Parachute is your backup companion for iCloud Photos and iCloud Drive. It backs up your memories — photos, videos, and documents — to storage you control, whether that's an external drive, Google Drive, OneDrive, S3 Buckets, network drives/NAS, external hard drives and more. With Parachute, you get peace of mind and full ownership of your data, free from lock-in.

• Back up your entire iCloud Photos library (including Shared Albums) and folders from iCloud Drive. • Preserve originals in full resolution, all adjustment data, and the current edited versions. • Works with USB drives, NAS/SMB/SFTP mounts, Google Drive, S3 Buckets, OneDrive, external hard drives and more

In any event, he now has his share of my $4, and I look forward to exploring this further. As our listener wrote, this developer gets it. Once again, the app is called: "Parachute Backup Mobile" and I have its link https://apps.apple.com/bh/app/parachute-backup-mobile/id6749824842 in the show notes.

Stephen Adams

Steve, You mentioned in your section about data brokers that nobody authorized the Credit Bureaus to collect our information. That's incorrect. You expressly gave your permission when you applied for or continued to use credit or receive service from a utility (electric, phone, mobile, gas, etc). Each and every application or terms of service document states this will be done, and when you sign the application, you agree to sharing your information with the Credit Bureaus. Here is the language from my latest JP Morgan Chase credit agreement…

We may obtain and review your credit history from credit reporting agencies and others. We may, from time to time, obtain employment and income data from third parties to assist us in the ongoing administration of your account. We may also provide information about you and your account to credit reporting agencies and others. We may provide information to credit reporting agencies about this account in the name of an authorized user. If you think we provided incorrect information, write to us and we will investigate.

There is no opt-out for reporting your information to the credit bureau. The only way to clear your credit report is to have no credit and wait seven+ years for everything to age off. As long as you have credit, you've authorized collection of that data. -Stephen

Stephen, I stand corrected and I'm glad to be. So I thank you very much for that. This is an important part of the whole credit bureau story. In the fine print of the credit agreements we voluntarily signed with all of the many various sources of credit we use and take for granted in our modern lives – who doesn't at least have a credit card these days? – we gave these credit grantors our permission to disclose and share what they learned of us. They need to learn about us by asking these data aggregators what's known. So, in turn, they report about us under our contractually granted consent.

Vladimir Eliseev

Hi Steve! My name is Vladimir, I live in Russia, and I really enjoy listening to Security Now. I'd like to add to your comment in episode 1040 about the problems with Google Meet. The reason for the blocking of Google Meet is the launch of the Max messenger, which is under state control. In this way, Russia continues down the path of internet isolation — a process that Russians themselves call 'creating the Cheburnet' (a blend of Cheburashka + Internet).

Vladimir, thank you so much for your note. Just as I feel self-conscious talking negatively about China while we have so many Chinese listeners, I feel equally awkward talking about Russia in derogatory terms, and for the same reasons. But my own U.S. government's hands are also certainly not clean. So I think we can all assume that whenever we're talking about the actions of Russia, China or the U.S., we're never talking about the actions of a country's people. Whether or not we may have voted for our various government's representatives, and regardless of how we may feel about their actions, they are not us.

I also very much appreciate hearing from our listeners in other countries to obtain their perspectives. I poked around a bit looking for "Cheburashka" which appears to be a fictional character from Russian literature. Though its meaning in this context is not entirely clear, I assume from the context of your note, Vladimir, that Russian citizens are not all in favor of having Russia's internal networks isolated from the rest of the world. Given how much Internet accessible knowledge lies outside of Russian territory, that's entirely understandable.

Hans Bornich

> *Hi Steve, Regular listener and Club Twit member here. Thank you for all your hard work on the show and everything else you do. I especially look forward to an UEFI native version of SpinRite which I will be purchasing on day 1. Anyway, I stumbled upon a link I thought you might find interesting. I thought I knew what a valid email address was, but boy was I wrong - if this site is right :-) I wonder what your score will be - no cheating! I scored a measly 12. https://e-mail.wtf/ Best regards, Hans Bornich, Denmark.*

Hans is correct, it IS a difficult test and I did not do much better than his 12. I scored 15 out of a total possible of 21, and I've written more than my share of eMail address parsers in my time. There are some very worthwhile and tricky examples on the test, which successively presents a series of sample eMail addresses, asking the test taker whether each one is valid or invalid. I think that those who follow this podcast would get a big kick out of taking this test themselves and seeing how they do. It's at: https://e-mail.wtf/ It has the page title of "eMail is Easy", which it isn't!

Matthew Turner — shared the thinking that I'm sure we've all had. He wrote:

> *So would recording a TV program and fast forwarding the ads be illegal? What about stepping out of the room during an ad? Or what about watching live TV and muting the ads because they are so much louder than the program? Although, charging AI for content would likely make the AI much more accurate!*

I wish charging AI for content would make it more accurate. But Reddit has been licensing its content for AI modeling, so it's not as if AI is only being trained on the Encyclopedia Britannica.

And as for the whole question of any implied obligation to be exposed to a show's advertising, Matthew's examples help to highlight the dilemma. We may have signed a contract with a lender to allow them to obtain our credit data and return anything more they learn about us to the credit bureau, but no one watching live TV ever agreed **not** to get up and pee during commercials. Not only do we have no obligation to sit still for commercials, but they're widely regarded as conveniently placed opportunities to transfer the clothes from the washer to the dryer, to feed the dog, to make sure the front door is locked, and to take care of the numerous other things that make up our evenings. When I use a web browser, I'm rarely confronted with a site that notices my browser is not displaying all of its advertising and asks me to please disable my ad blocker. When that happens I am more likely to just leave and go somewhere else. So I suspect that most sites that may have tried that for a while noticed that the practice resulted in a drop in their revenue, rather than the reverse, so they decided to take the high road and accept what revenue they can get without attempting to force the issue.

Tom Apalenek

Hi Steve, Great show as always. A couple of observations on copyright and ad blockers or AIs:

The ad blocker's "modified" code and display of a web page is only being displayed to the person who bought the ad blocker. It is not being re-published to anyone else. Books are also protected by copyright law. By the German court's logic, highlighting or underlining passages in a book that you own, and the purchase of pens or highlighters for that purpose should also be illegal.

I had to reread that and think about that a bit to obtain all of Tom's logic. But I can see his point. It would be illegal to make a few changes to a copyrighted novel, for example, and to then resell it as one's own work. But it's certainly not against the law to rewrite a novel, tear out pages, and do whatever you wish to a copyrighted work that you own. So Tom is suggesting that having a web page displayed is the delivery of a copyrighted work that its recipient has ever right to change however they wish. What they cannot do is capture and republish that work for their own benefit. And, of course, no one is doing that. We're just choosing to modify that web page for our own consumption. That feels like a pretty sound argument.

Tom's email continues:

Also, you described AIs as the ultimate super ad blockers. Given their need to eventually show a profit, I fear this is probably short lived. I suspect that AI dialogs will start changing in the near future to something like this: Prompt: "How can I get my WiFi to reach to the end of my back yard?" Answer: "There are several options including WiFi extenders, longer range routers …. Blah blah blah …. By the way, did you know that Best Buy has the model XYZ router on sale this week for $69. Would you like me to provide you a link to the ad on their website?" Or maybe it will just show you the ad directly at the end of the answer. In any case it will be interesting, if not disappointing to see how this all shakes out. Thanks to you and Leo for a great show and for keeping is all up to date on the latest security news. - Tom, WA2IVD

Remember how super clean, simple and straightforward Google's search results were in the beginning? Just a white page with wonderful links to exactly what we were looking for. But those days are long gone. Now the page is encrusted with sponsorship barnacles. And the link you'd love to have instead of being right there at the top of the page, is buried beneath AI overview, a ton of sponsored and not always on-point tangential references, and eventually you may find the link you're seeking.

Sadly, I would bet money on Tom's vision of the future of AI chatbots turning into massive advertising revenue generators – and probably more effectively than anything that has come before. I've noticed how much user-context ChatGPT has been acquiring and saving about me. When I ask it questions it has learned who I am from our previous interactions. So just imagine when that knowledge is merged and cross-referenced with a large collection of advertisers.

I started out reminding everyone about the Google of yesteryear, because I'll bet we're currently enjoying what will become the AI ChatBots of yesteryear. In ten or twenty years, people will be looking back and recalling with fond longing those days when AI was uncluttered by ads and, even worse, was not subtly guiding the opinions of its users toward commercial outcomes that would wind up generating additional revenue for the AI company.

Zaphod Beeblebrox 1st

Hey Steve, Re: Ads on websites. As you switched to Brave, their "BAT" idea may interest you. It stands for Basic Attention Token. Basically a crypto mined with attention. Something like this could make sense. It was also used years ago but called "cryptojacking" and now most browsers block it. ASIC resistant coins like Monero, which you may like for its privacy features, can be CPU mined and therefore paid directly to the websites with no tracking. AI companies could also do similar and pay every time their AI uses data scraped from that site. The economics could be tricky, and beanie babies aren't the best example, but if people really want BAT the price will go up. Same way if people want US Dollars the value goes up. It could be a good way to pay without paying. I don't think they could require a specific amount to go to a site though because phones would generate minimal amounts.

We've touched on this before. It's a truly interesting idea. Cryptocurrency is here and it's not going away anytime soon, if ever. And cryptocurrency that can now be mined can be exchanged for actual government backed non-crypto currency. So imagine that while visiting a website, the visiting user's PC is tasked with performing mining work that directly yields value to the site. Viewed from the perspective of a website, all of the potentially tens of thousands of visitors who are there looking at a site's content are also collectively mining crypto for the site. No single browser mines much, but collectively and continuously, it adds up.

From the standpoint of the user, what's going on is that some of their electricity is being (inefficiently) converted through the process of micro-mining into currency that serves to reimburse the site for the cost of the visitor's presence and for the information they obtain.

So this forms an interesting channel for moving some money web surfers pay for electricity, by using that electricity to spin up more cores inside their CPUs, which is used to perform work on behalf of the site, which that site is then able to liquidate back into fungible cash. I haven't examined the economics of the idea to see whether it might make sense, but Zaphod tells us that the Brave browser folks have done the math.

Ian in Ottawa Canada

Hi Steve, Just like Joshua, I too, have had some AI realizations, but I reached two opposite conclusions from what I have heard. We have a few low-traffic WordPress sites hosted with a correspondingly small hosting plan, but recently many AI crawlers have been ingesting 20+ years of blog posts, with many dozens of page loads per second.

Of course this periodically maxes out our CPU quota, as the pages are dynamically assembled by the WordPress site, and also consumes our bandwidth quota. If it were one crawler, fine, but there now seems to be a continual parade of crawlers sucking up everything they can find.

*Opposite conclusion #1: AI is **not** good for small sites. (I would be more inclined to move to a simple static site on AWS with their CloudFront CDN for publishing contact info and self-aggrandizement.)*

On the topic of AI summaries taking over, I see a silver lining: If I have a product or service that I want people to be able to understand, perhaps now I can just write one big pure-text authoritative document -- hopefully with a way to draw the attention of the AI crawlers.

No need for hi-res images of happy people, or acres of whitespace, or a designer to tell me to use all lowercase headings with an exotic downloaded font displayed in medium grey on a light grey background, or any of the other fluff that a 'good' page needs. Which leads us to...

Opposite conclusion #2: AI summaries can free many of us from the burden of visual site design.

At this point I imagine that some of our listeners are thinking that GRC's site was never very much burdened by the exigencies of visual site design. They would be correct. I very much like solid red and blue on white with lots of rule lines and boxes. Ian finishes:

Am I just being provocative, or could that be in our future? I'm not sure. Thanks for all the work you and Leo do! Best regards, Ian in Ottawa Canada

Leo, you guys had a guy from "Common Crawl" on your Thinking Machines podcast a few weeks back. Their mission is to deal with exactly the problem Ian is having. While the web is operating as "Every Bot for Themselves" our websites are being redundantly visited by every bot of every company in single file. The idea of Common Crawl is to "Crawl" all that data into a series of online Internet web snapshots that anyone is welcome to obtain. https://commoncrawl.org Their domain is https://commoncrawl.org and their home page explains:

Common Crawl maintains a free, open repository of web crawl data that can be used by anyone. Common Crawl is a 501(c)(3) non–profit founded in 2007. We make wholesale extraction, transformation and analysis of open web data accessible to researchers.

Over 300 billion pages spanning 18 years. / Free and open corpus since 2007. / Cited in over 10,000 research papers. / 3–5 billion new pages added each month.

The corpus contains raw web page data, metadata extracts, and text extracts. Common Crawl data is stored on Amazon Web Services' Public Data Sets and on multiple academic cloud platforms across the world. Access to the corpus hosted by Amazon is free. You may use Amazon's cloud platform to run analysis jobs directly against it or you can download it, whole or in part. You can search for pages in our corpus using the Common Crawl URL Index.

In this era of "Big Data", data storage is so plentiful and vast that there's no longer any need for individual companies to redundantly crawl the web. Doing so oneself is not simple and it requires the assembly and maintenance of a sophisticated web crawling infrastructure to pull all of that widely-distributed data from across the globe. And as we've noted, having everyone rolling their own separately is expensive, time consuming and redundant. It makes so much sense to have a single centralized non-profit that everyone can easily reference as a single stored database. It's kind of brilliant.

Ed Hands

Hello Steve, As an IT Manager, security is always our top priority. I recently listened to Security Now podcast #1040 and found the discussion about Germany possibly banning ad

blockers particularly compelling. I share your concerns regarding privacy and third-party cookies. However, my primary concern extends beyond those issues.

In managing approximately 2000 endpoints and users, ***our network has been hit by ransomware twice.*** *Thanks to comprehensive policies, procedures, and security software, we were able to prevent significant damage.*

What concerns me most is that the ransomware was introduced ***through advertising delivery networks.*** *(You may have heard me yelling at the radio in the car about this.)*

Given this context, if Germany passes legislation banning ad blockers, it seems to me the case could be made that the advertising networks could (or should) be held financially liable for any malware distributed through their platforms. It seems that such accountability would be appropriate. Thank you, Steve and Leo, for all that you do with Security Now. Here's to the next 20 years of Security Now! Best regards, Ed H

We've certainly talked about "Malvertising"; its possibilities and dangers. But it's still sobering to hear from a listener who has had first hand field experience (and more than just once) with advertising being used as the entry vector for a ransomware-scale compromise. It doesn't seem as though that's something that receives sufficient attention. Accountability chains are difficult to manage, and they become near to impossible to litigate when it's possible for multiple parties to point fingers at each other. I've served as an expert witness in a few technical jury trials and it's been quite disheartening to see clever counsel spin a jury and leave them unsure of their own names. In these "he said, she said" cases, juries often choose not to award damages since they're unable to determine fault. So I don't have much faith in the practical ability to hold an advertiser accountable, though I do love the idea!

Tom Herrmann

Hello Steve, as probably others already send: Syncthing supports encryption of the data on 'untrusted' peers already. I've been using this for many years for syncing to my own NAS (and other peers), as I am a bit 'paranoid' and want to prevent any unencrypted data at rest.

You can see it in the settings of every folder when selecting the sync peers. Peers can be marked as untrusted and then a (strong) password needs to be set. Untrusted peers can even sync encrypted data among them, if the same password is used with all untrusted peers.

Also peers themselves can be marked untrusted in the settings and then the UI forces a password to be set when you want to share any folder with those peers.

Regards, Tom / Listener since day #1

Tom is absolutely correct. The option to set a password is right there, staring at any Syncthing user. At the some time, our previous listener may have been referring to the fact that the top of the SyncThing documentation page states: https://docs.syncthing.net/users/untrusted.html *"Warning: This feature should still be considered beta / testing only."* And what that "untrusted" peers documentation page says is exactly what Tom just explained and it's what the UI shows. So I'm unsure what's going on. But the operation is quite cool.

Last week's listener was wondering about using a friend for his offsite drive backup. By simply setting a strong password on the folder being shared, that password along with the ID of the destination (encrypted) folder will be used at the plaintext end to encrypt and decrypt the data before it leaves and after it returns from the remote peer. The user's data will never exist outside of the user's machine in unencrypted form. And additional peers can also all sync to the same shared encrypted folder if they are also in possession of the secret password. So this does everything we could want. The feature is marked beta and testing only, but perhaps that notice has just not been taken down.

Dave in Seattle

Hi Steve - thanks for the tip and free GB upgrade on Sync.com. I've been looking for just such a solution, wanting to avoid the big sync and cloud services. Plus Canada, what's not to love? I thought you'd like to know that opt-out of email-based forgotten password resets is the default, and a visible choice on the account creation section of their top landing page... that's so cool, so smart, and something I've also not seen anywhere else. (screenshot below)

Dave attached a screenshot to his note showing that the option to enable email-based password recovery is set to "off" by default. I hadn't recalled that. I just knew they offered that option and that mine was set to off, where I think for something as important this should remain. Thanks Dave.

Dan Dapkus

Hi Steve (and Leo), I have been a software engineer / database administrator / dev team manager / director of app dev for over 30 years, and a fan of your show for about 10 years (I hadn't heard of it before then). I think yours is the only podcast to which I've consistently listened for such a long period of time. I'm not sure where I'd begin if I were to go on complimenting both of you. Steve, your deep technical / mathematical knowledge is remarkable; and, Leo, your broad industry knowledge and experience are a perfect complement. I look forward to the show every week, including the commercials because they too are often interesting and informative.

I've been thinking about writing this email for years, and episode #1038 finally knocked me over the edge, and so I'm writing. Cutting to the chase - you both qualify as "Microsoft Bashers." Throughout my career, I've observed this phenomenon of IT pros who take various opportunities to rant and rave about all the deficiencies of Microsoft without acknowledging the (blatantly obvious) essential exculpatory context. The following is the exculpatory context to which I refer:*

- *MICROSOFT CREATES AND SUPPORTS MULTIPLE BUSINESS AND PERSONAL OPERATING SYSTEMS AND SOFTWARE FOR MUCH OF THE WORLD (AND HAS DONE SO SUCCESSFULLY FOR DECADES).*
- *Monthly, Microsoft rolls out cumulative updates to over 1.5billion Windows 10 and 11 endpoints worldwide.*
- *There are roughly 1.65 billion Windows Servers installed around the world, and Microsoft also patches those every month.*
- *Over 3 million websites use Microsoft IIS as their web server. Hundreds of thousands or millions more host their websites in Azure.*

- *Microsoft .NET (which is now cross-platform) is used by millions of developers worldwide (34% of all websites run on .NET technologies), and Microsoft patches it monthly.*
- *Microsoft secures one of the world's premier database systems, SQL Server and its PaaS version Azure SQL Database. There are an estimated 8-10 million instances worldwide.*
- *Microsoft secures one of the world's dominant office productivity suites - Microsoft 365. There are 345 million paid subscribers.*
- *Microsoft has a uniquely large attack surface, and they diligently patch it. It's inconvenient for everyone involved.*
- *No one forces anyone to use Microsoft products. If some perfectly secure, inexpensive, wonderful alternatives exist, companies and individuals are free to adopt them (and then shall be liberated of the need to complain about Microsoft).*
- *Steve - one tangential tidbit: you mentioned SonicWall's Geo-IP Filtering. From the transcript, you said, "So, I mean, it is the way to do this. But no one's doing it yet."*
  - *Microsoft, however, has been doing "it" and more for years in Azure with its Web App Firewall which supports not only geo-filtering but also OWASP threat detection and blocking at the network perimeter. Read about it here.*

Microsoft's task is herculean, and I think they generally do a good job. Can you think of another company that you'd trust and would expect to behave more responsibly and competently (and less greedily) with Microsoft's responsibilities?

Thanks again for your hard work and for many more episodes of Security Now.

Best, Dan Dapkus

Dan makes many valid points, which is why I wanted to share them with everyone on the podcast. I know I'm hard on Microsoft. And I do acknowledge that GRC runs on Microsoft servers with one FreeBSD Unix exception, and we all know that I'm exclusively a Microsoft software developer. So I'm very aware that I beat up on them weekly (that's: w-e-e-k-l-y) while at the same time choosing to use their solutions for my company and for myself.

That said, there are decisions (not mistakes which anyone can make) that I have great difficulty swallowing. We're told that Windows 11 will run faster than Windows 10 on the same hardware because it's more efficient, but that Windows 11 won't run on all of the same machines that are handily running Windows 10 today. And that TPM 1.2 versus 2.0 requirement is pure nonsense. TPM 1.2 is just fine. And we all know that Windows 11 can be tricked into running on older "incompatible" hardware. This promises to create a huge problem for the next few years. And that's certainly no mistake. That's by design.

And the idea of charging some users to receive patches for flaws for which perfectly well-working patches have been created is just wrong. If a patch exists to repair a product defect in a Microsoft product that they created, it should be provided to that product's users. Period. Full stop. Charging anyone extra to fix product defects is never going to sit well with me.

So I suppose my overall complaint is that while Microsoft has every right to be self interested, they are so ridiculously massive that for most companies there really is not any effective alternative. And I'm certain that's something that our listener appreciates. Given that, and the nature of capitalism, Microsoft will – not may, will – abuse the power they have for their own self interest, just because they can.

I'm not leaving Microsoft and Windows – I can't and I don't want to. But I'm VERY glad to see that large European countries are fed up with Microsoft's shenanigans and are beginning to pull away. Perhaps if enough of that happens Microsoft will have a bit of the wind taken out of its sails and might consider perhaps not pissing off so much of the rest of the world that has no effective alternative.

Microsoft is in an enviable position. They've earned it. But it takes a great deal of institutional ethics to resist abusing it. They're walking a fine line.

Sci-Fi

Ryk Brown

On Sunday, while I was assembling today's podcast, the iPhone I have resting on a stand next to me alerted me to a Facebook posting by Ryk Brown. I've spoken of Ryk (spelled "RYK") many times before since he's the prolific author of one of my most favorite long-running science fiction series, known as the Frontiers Saga. When he embarked upon his writing, he conceived of five long story arcs, where each one would receive a 15-novel treatment. He's currently one novel away from finishing the 3rd story arc, which would make that next novel his 45th.

Once that last book of his 3rd series is finished, he'll have two story arcs remaining, and there have been strong hints that our intrepid group of explorers may be encountering their first non-human aliens. So far, each arc's nemesis has been various groups of power-hungry humans. But I have the feeling that may be changing next, and I cannot wait to see Ryk throw our group of very well known, well developed and wonderful characters into confrontations with non-humans.

I know Ryk has many fans among our listeners, because I often hear from many of you who are enjoying the many characters he has created every bit as much as I am. So I wanted to share Ryk's Facebook posting from Sunday since he's soured on Amazon's Kindle Unlimited service and things will be changing for the two final story arcs. Ryk wrote:

> *When Amazon first started Kindle Unlimited, I was still being compensated for reads through KU at a rate of about 70% what I would make on a purchase. The entire system is rather arbitrary, and has become so polluted and gamed over the years as to be laughable. The amount of compensation for reads through KU is now down to a mere 30%, which means that every time someone reads one of my books through Kindle Unlimited instead of buying it, I am losing on average about 60-70% in sales revenue.*
>
> *While I do not begrudge anyone for using the least expensive way to satiate their need to read, in the end, I am running a business, and my family depends on me to pay the bills. Therefore, starting with Part 4 of the Saga, my books will no longer be available in Kindle Unlimited. I'm hoping that if you've read this far in my series, you won't mind spending a few bucks every 3-4 months for a new episode.*
>
> *If you have been reading Part 3 through KU, and are not up to date, I would suggest you download them as soon as possible, as they will begin dropping out of KU as soon as Sept 2. I will put the final episode of part 3 in KU for 3 months after publishing so that those who must*

use KU in order to afford reading my stories will at least be able to finish Part 3. But by the end of 2025, all Parts 2 & 3 will no longer be available through Kindle Unlimited. Although I will be leaving all of Part 1 in KU for now in order to attract new readers, eventually, most if not all of those titles will also be taken out of KU.

This is not without risk, as Amazon unfairly weights KU reads toward sales rankings (even though a KU read is NOT a sale) and it could cause my rankings to tank and for me to lose revenue, but it has to be done. Amazon is ripping us off, and the only other way I can combat this is to write faster (which likely means poorer quality) and/or raise prices. Now is the best time for me. With my new Astra Nullus project (and a small inheritance from my late mother) I have the best chance of weathering the storm that will without doubt be created by removing my books from Kindle Unlimited. However, if I can successfully reach calmer waters, I can then publish my works on other platforms, as many of you have asked me to do.
To those of you who purchase my books even though you could read them through Kindle Unlimited, I thank you. Without you, I would not have made it this far. Ryk

Leo, I believe that you've soured on Amazon and that you're no longer wanting to support them. From what Ryk has said, the compensation for authors publishing through Kindle Unlimited has changed, and not for the better.