Security Now! #1044 - 09-23-25

The EU's Online Age Verification

This week on Security Now!

• Consumer Reports on Windows 10 updates. • Waste (not fraud or abuse) within DoD Cyberoperations. • China's DeepSeek produces deliberately flawed code. • WebAssembly v3.0 officially released. • Firefox v143 updates and new features. • Firefox for Android now offers DoH. • A nearly terminal flaw in Microsoft's Entra ID. • Chrome hits its 6th 0-day this year. Emergency update. • DRAM (now DDR5) still vulnerable to RowHammer. • SAMSUNG kitchen refrigerators begin showing ads. • China says no to NVIDIA. • 300 more (new) NPM malicious packages found and removed. • The EU is already testing **proper** online age verification.

Wikipedia: *"**Irony** is the juxtaposition of what, on the surface, appears to be the case with what is actually or expected to be the case."*

Security News

Consumer Reports on Windows 10

Exactly one week ago, as we were recording last week's podcast, the famous Consumer Reports site publicly posted under the headline *"Consumer Reports calls on Microsoft to extend support for Windows 10"*. I was surprised to recognize the name of the author of the piece, since I didn't know that I knew anyone at Consumer Reports, especially someone whose knowledge and opinions I greatly respect. Consumer Reports' piece was written by TWiT's well-known long time podcast co-host, Stacey Higginbotham. In Consumer Reports name, Stacy wrote the following:

September 16, 2025

***To: Satya Nadella**, Microsoft Corporation, One Microsoft Way, Redmond, WA 98052*

Dear Satya Nadella, Consumer Reports is concerned about Microsoft's decision to end free ongoing support for Windows 10 next month. This decision will strand millions of consumers who have computers that are incompatible with Windows 11, and force them to pay $30 for a one-year extension of support, spend hundreds on a new Windows 11-capable computer, or do nothing and see the security and functionality of their computer degrade over time. This latter option is particularly problematic as it risks harming the consumer as well as co-opting the machine to perpetuate attacks against other entities, risking national security.

Four years ago when Microsoft released Windows 11, it announced that support for Windows 10, which was released in 2015, would end on October 14, 2025. Microsoft also said that because of the hardware requirements of Windows 11 — namely a Trusted Platform Module 2.0 and a 64-bit processor— that some consumers would need to upgrade their computers since their current machines would not be capable of running Windows 11. Despite this announcement in 2021, computers incapable of running Windows 11 were still available for sale in 2022 and 2023.

Even if Microsoft partners and retailers stopped selling machines that were not able to be updated to Windows 11 at the time of the launch, our research shows that many consumers would still be trying to use the incompatible machines today. Based on a Consumer Reports member survey of 100,606 laptop and desktop computer owners (Jan-Mar 2025), over 95% of all laptop and desktop computers purchased since the beginning of 2019 and owned for no more than 5 years were still in use when members were surveyed. Moreover, 20% of our members who owned a Microsoft laptop reported owning them for at least 4 years, compared to just 13% of our members who owned any other brand of laptop for that length of time. We see similar trends when looking at all Windows OS-compatible computer brands in our sample (Acer, ASUS, Dell, HP, Lenovo, Samsung, and Intel), as 15% of our members who own a Windows OS-compatible laptop or desktop brand have owned them for at least 4 years, compared to just 12% of our members who own a laptop or desktop brand that is typically not Windows OS-compatible. Based on these findings, we posit that our members who have purchased Windows OS-compatible computers, on average, tend to keep them for longer lengths of time than owners of other computers. Thus, it's clear that consumers purchased machines before Microsoft announced the hardware needs for Windows 11 expecting to be able to operate them through the next Microsoft OS transition.

The decision to make Windows 11 incompatible with existing hardware, and to do so with only four years notice is incompatible with consumer expectations and Microsoft's own history. Microsoft has long focused on backwards compatibility for Windows, ensuring it can run on older hardware. This means that consumers could expect to be able to run the latest version of

Windows for at least a dozen years and maybe more. If you bought a PC with Windows 7 preinstalled in 2010, you were able to upgrade it to Windows 8 in 2012 and then Windows 10 in 2015, and many of those devices can still run Windows 10 in 2025.

During the Windows 11 launch, and in subsequent announcements, Microsoft argued that the hardware requirements would boost the cybersecurity of Windows machines. Microsoft claims that "Windows 11 is the most secure operating system we've ever built," and noted that a 2024 report commissioned by Microsoft showed that new Windows 11 PCs have seen a 62% drop in security incidents and a 3x reported reduction in firmware attacks. This is laudable, except there are still a large number of Windows 10 users, and a large number of existing machines that are physically unable to be upgraded to Windows 11 because of the hardware-based security features.

*As of August, 46.2% of people worldwide are **still** using Windows 10, which is about 646.8 million people based on Microsoft's own estimates of 1.4 billion people using Windows as an operating system. There are also an estimated 200 million to 400 million PCs worldwide that cannot be upgraded to Windows 11. This is an incredibly high number of stranded Windows 10 machines. Microsoft in its own blog post warns that, "While these devices will continue to function, they will no longer receive regular security updates, making them more vulnerable to cyber threats, such as malware and viruses."*

Arguing that Windows 11 is an essential upgrade to boost cybersecurity while also leaving hundreds of millions of machines more vulnerable to cyber attacks is hypocritical, especially while charging consumers $30 for a mere one-year extension to preserve their machine's security. Microsoft has touted a free support option for consumers, but to obtain that support consumers must choose to use Microsoft products such as Bing search or Xbox gaming to earn the 1,000 Microsoft Rewards points necessary to access free support. Tying free support to unrelated Microsoft products forces consumers to jump through unnecessary hoops just so Microsoft can eke out a bit of market share over competitors.

Consumer Reports asks Microsoft to extend security updates for free to all users who are unable to update their machine while also working to entice more people to get off Windows 10.

When more consumers upgrade to Windows 11 through software updates or because they have now purchased a new machine capable of running the software, we also ask that Microsoft create a partnership to provide recycling of those machines to consumers abandoning their hardware.

For the last quarter century Microsoft has been up front about the 10-year lifecycle of its operating systems, but as it made the move from Windows 10 to Windows 11 it broke the backwards compatibility that so many consumers have depended upon as they shopped for their computers. When Microsoft announced in late 2021 that it would require specific hardware components that hundreds of millions of PCs on the market would not have, it left consumers who had recently made a purchase of incompatible hardware behind.

Consumer Reports calls on Microsoft to extend support for Windows 10 to allow those consumers to catch up.

Sincerely, Stacey Higginbotham
Policy Fellow, Consumer Reports

Everyone knows that Microsoft's claims that Windows 11 runs better on existing hardware than Windows 10 implicitly means that Windows 11 does not truly require newer, faster and better hardware. We all also know that all of that nonsense about TPM 1.2 vs 2.0 is just that – nonsense. Many years ago we spent a podcast examining the differences between the two. While 2.0 contains the advances we would expect to have made over time, those are evolutionary, not revolutionary and they are not needed for the delivery of the security guarantees provided by TPM 1.2 – and Microsoft knows that.

I thought that one point Stacy made was particularly important. Microsoft is once again claiming that Windows 11 is their most secure operating system ever. As we learned from Windows XP, of which they made the same claim, later proven to be laughable, only time can judge the security of any system. But if Windows 11 is more secure, and if Microsoft cares about the security of their users, then user security will be severely compromised by Microsoft's plan to allow Windows 10 security updates to lapse, thus leaving those many hundreds of millions of Win10 machines unprotected, versus either continuing to offer those machines security updates, or allowing those older machines to update to Windows 11.

In any event, BRAVO, Stacy! Thank you for using Consumer Reports' well-deserved reputation for this good cause. We've watched as Microsoft's previous decisions on this matter have shifted over time. So I'd say it's reasonable to hope they might simply allow all Windows 10 machines to continue receiving security updates for the next three years. All they need to do is flip a switch in Redmond.

Waste (not fraud or abuse) within DoD CyberOperations

The favorite targeting phrase of those who wish to trim the operating costs of the United States government is *"Waste, fraud & abuse."* Last Wednesday, the U.S. GAO, the Government Accountability Office, published a report detailing the size and scope of U.S. Department of Defense Cyberspace Operations... and it's breathtaking. While the report does not address fraud or abuse, it's about as diplomatic as it could be on the waste front, because there sure does appear to be a ton of cyber-waste. The summary in the report's subheading reads: "About 500 Organizations Have Roles, with Some Potential Overlap". Right. ***500*** cyber-related organizations have sprung up within the DoD. And that doesn't count the 9,500 contractors.

The report said that *"According to data provided by Department of Defense (DOD) components, DOD has established organizations that contain about 61,000 military and civilian personnel (and over 9,500 contractors), to conduct cyberspace operations."* I have no idea how anyone would even begin to unwind that. But before anything could happen, the will to do something needs to be present. So far, the U.S. Department of Defense has remained unscathed and untouched by the broad and sweeping cost- and personnel-cutting measures that marked the beginning of the current administration. However, the DoD's reaction to this report's recommendations were positive even though those recommendations were quite modest. Under "Recommendation" the report concluded:

> *GAO is recommending that DOD assess whether (1) similar cyberspace training courses provided by the services can be consolidated and (2) there are opportunities to increase mission effectiveness and cost savings by consolidating DOD cybersecurity service providers. DOD concurred with both recommendations and identified actions it will take to implement them.*

So, consolidate cyber-training and consolidate cybersecurity providers. At least that sounds like a start.

China's DeepSeek may (deliberately) produce flawed code

In a report that's both sad and predictable, the Washington Post's story headline was: *"AI firm DeepSeek writes less-secure code for groups China disfavors"* with the sub-head: *"Research by a U.S. security firm points to the country's leading player in AI providing higher-quality results for some purposes than others."* A summary of the The Washington Post's story reads:

> *The Chinese artificial intelligence engine DeepSeek often refuses to help programmers or gives them code with major security flaws when they say they are working for the banned spiritual movement Falun Gong or others considered sensitive by the Chinese government, new research shows.*

Commentary about The Post's coverage wrote that *"The DeepSeek AI engine returns code with security flaws if it determines that the coder is associated with a specific minority group. According to the Washington Post, programmers from Tibet and Taiwan received code of lower quality. DeepSeek also flatly refused requests if queries hinted that the code would be used by the Islamic State or the Falun Gong movement."*

While we've seen that technological advancements are eventually abused, this might have set a new land speed record. What a shame.

WebAssembly officially moves to v3.0

Version 3 of the WebAssembly specification is now officially live, though our two favorite browsers, Chromium-based Chrome and Firefox have already been incrementally incorporating its new features as they've been formalized. What's interesting is that Apple's Safari is the real laggard here. I have no idea why. But this has become a trend for Safari which has been consistently lagging behind most of the new standards for years.

I took a look at WebAssembly. Though it's a stack-based architecture, it has a procedural structure with argument passing and traditional high-level control flow primitives. I'd love to have some reason to need it. But its only real performance advantage comes from processor-intensive things, such as mining cryptocurrency in a browser. If I were ever to use a web browser as a front-end for some headless code, I'm certain that any heavy computational lifting would be done in native Intel assembly language and the browser side would just be pure user-interface. And if that were the case, regular JavaScript is just as fast and far more maintainable. Stack-oriented languages, FORTH being the most famous, make for very efficient intermediate languages – the Java language's VM and Microsoft's .NET CLR – common language runtime – are good modern examples. But they are not fun to write in and they are nearly impossible to later read.

I know that the W3C is composed of a great many committees of contributors, but I wish they would devote all of their time to giving us fully private online minimum age-assertion for the web. The entire world needs that much more desperately than more capable stack machine interpreters for our browsers.

Firefox v143.0
And speaking of web browsers, one week ago Firefox moved from v142 to v143. I've launched Firefox every single day since then and it wasn't until I explicitly went to Help / About that I was offered v143.0.1. Version 143 repaired a pair of sandbox escapes that had been found and reported in Firefox's 2D canvas rendering component and there was one memory safety bug. Those were the only three "High" priority security improvements. The rest were moderate or low. So no big emergency. V143 does bring some new features — I'll save the best two for last:

- On Windows, Firefox now supports running websites as web apps pinned directly to the taskbar. These are sites that you can pin and run as simplified windows directly from the taskbar without losing access to your installed add-ons. However, this feature is not currently available for Firefox installs from the Microsoft Store.

- Tabs can now be pinned by dragging them to the start of the tab strip, making it easier to keep important sites within reach.

- Copilot from Microsoft can now be chosen as a chatbot to use in the sidebar for quick access without leaving your main view. Oh, joy. It's unclear to me how many people who have chosen to use Firefox rather than succumbing to Edge, over and above all of Microsoft's clearly (and repeatedly) stated objections, would choose to chat with Copilot over any of the many alternatives, but for what it's worth, that can now be done from the URL's search bar.

- When a site asks for camera access, what the chosen camera is seeing can now be previewed "in vitro" inside the permission dialog. This can come in handy when needing to switch among multiple cameras.

- The Firefox address bar can now display important dates and events. Mozilla elaborated that this gripping new feature supports displaying events (e.g. "Mother's Day") in the United States, United Kingdom, Germany, France, and Italy regions. *(Hmmm. Mozilla, I have a thought! How about some privacy-enforcing age verification? Could we please have that instead of Mother's Day reminders?)*

- Firefox 143 now also supports Windows UI Automation, which improves support for accessibility tools such as Windows Voice Access, Text Cursor Indicator and Narrator.

And I said that I was going to save the best two for last...

- Firefox has expanded its Fingerprinting Protection by reporting constant values for several more attributes of user's computers.

- When downloading a file in Private Browsing mode, Firefox now asks whether to keep or delete it after that session ends. You can adjust this behavior in Settings.

That's a nice feature for Private Browsing mode. The presumption being that if you're in that mode, just as you do not wish to have your browser permanently record where you go and what cookies you'll definitely be given, you may also not want anything you might download to persist.

I suppose it's not bad that Firefox expanded its Fingerprinting Protection by reporting constant values for several more attributes. But that didn't prevent the EFF's "Cover Your Tracks" site from locking onto my updated browser and reporting that its fingerprint was unique. So, Mozilla, please keep working on that one.

FF for Android offers DoH
One last piece of news on the Firefox front is that last week's Firefox for Android, which is now available, offers its own native DoH – DNS over HTTPS – support for resolving domain names into IP addresses using an authenticated and encrypted TLS connection.

This is not a huge deal because native DoT DNS resolution was added to Android seven years ago in 2018 with the release of Android 9 and native DoH resolution was added two years later in 2020 with Android 11. So even without Firefox adding its own native DoH support, all of its DNS lookups could have been securely encrypted using Android's native DNS since 2018. Still, it's nice to have alternatives and now it's there.

A very bad Entra ID flaw
The Register's headline last Friday was *"One token to pwn them all: Entra ID bug could have granted access to every tenant"* – that means any SharePoint Online or Exchange Online account, including access to other resources hosted in Azure. In other words, this would pretty much be as bad as it could get. Before I go further, I'll share what The Register reported:

A security researcher claims to have found a flaw that could have handed him the keys to almost every Entra ID tenant worldwide. Dirk-jan Mollema reported the finding to the Microsoft Security Research Center (MSRC) in July. The issue was fixed and confirmed as mitigated, and a CVE was raised on September 4. It was an alarming vulnerability involving flawed token validation that can result in cross-tenant access. Mollema wrote: "If you are an Entra ID admin that means complete access to your tenant."

*There are two main elements to the vulnerability. The first, according to Mollema, is undocumented impersonation tokens called "Actor tokens" that Microsoft uses for service-to-service communication. There was a flaw in the legacy Azure Active Directory Graph API that did not properly validate the originating tenant, allowing the tokens to be used for cross-tenant access. Mollema wrote: "Effectively, this means that with a token I requested in my lab tenant I could authenticate as any user, including Global Admins, in **any** other tenant."*

*The tokens allowed full access to the Azure AD Graph API in **any** tenant. Any hope that a log might save the day was also dashed because requesting an Actor token does not generate a log. And even if it did, they would be generated in the attacker's tenant instead of in the victim tenant, which means that no record of the existence of these tokens is made or retained.*

The upshot of the flaw was a compromise of any service that uses Entra ID for authentication, such as SharePoint Online or Exchange Online. Mollema noted that access to resources hosted in Azure was also possible. Microsoft's swiftness in resolving the issue is to be commended, even if it's unfortunate that it was present in the first place. Mollema also noted that Microsoft had not detected any abuse of the vulnerability with its internal telemetry.

Mollema called this "the most impactful vulnerability I will probably ever find," and it's difficult to dispute the claim. The CVE for the issue rates it as "Critical" with a "Low" Attack Complexity metric and a CVSS score of 10.

To reiterate, according to Microsoft, the vulnerability has been fully mitigated, and users do not need to take any further action. Still, before the vulnerability was found, there existed, in Mollema's words, "one token to rule them all."

What I question every time we encounter something like this, that could have truly wreaked havoc upon the world, is whether those who would do us harm already knew about it and were thus quite upset by its chance discovery and unilateral removal from their secret arsenal?

The other question that naturally occurs is, if this was just found, what else is still lurking out there that bad guys may have found and are hoping the good guys don't stumble upon?

I would feel much more comfortable knowing that there was some chance that all of the big bad problems were being found and might eventually all be discovered. The reason that's unlikely is that Microsoft refuses to ever leave anything alone and they apparently introduce new problems at the same rate as they and others are finding and removing them. For example: What we don't know and never will know, is whether this flaw has existed from the start? Was it always in there? Or did it get introduced sometime later when someone came along and changed some things without a full understanding of the consequences?

Chrome's 6th 0-day this year with in-the-wild exploitation

Last Wednesday, Chrome was quickly updated to end the abuse of a critical type confusion bug in the V8 JavaScript and WebAssembly engine. Chrome in the Stable channel was updated to 140.0.7339.185 for Windows and Linux, and .186 for Mac.

This update seems worthwhile to obtain since it fixed four different vulnerabilities, every one of them designated as high:

- CVE-2025-10585: Was this one, a type Confusion in V8. It was discovered and reported by Google's TAG team, their Threat Analysis Group the day before on the 16th. So Google wasted no time getting Chrome updated to fix that bad boy.
- CVE-2025-10500, a use after free flaw earned its reporting researcher $15K.
- CVE-2025-10501 was a use after free in the WebRTC system. It's discovered is now $10K richer.
- The reward for discovering and reporting CVE-2025-10502, a heap buffer overflow in ANGLE has not yet been set.

It's interesting that the other bugs had been known by Google for as many as six or seven weeks. But despite all of them having similar ratings of "High" severity, it wasn't until the reporting of that type confusion in V8 and WebAsm, which their own TAG team reporting discovering from its active exploitation, that Google essentially instantaneously fixed it and pushed out the Chrome update which also incidentally fixed the others are Google apparently felt weren't worth brothering to update the world over.

DDR5 – Still vulnerable to RowHammer attacks.

Last week Google Security posted the news which should not surprise us much that the latest DRAM remains vulnerable to RowHammer attacks. From the start it was clear that RowHammer attack susceptibility represented a fundamental and intrinsic vulnerability which was inherent in the fact that the push for insane levels of performance and memory density had forced the reduction of dynamic RAM noise margins and cell charge capacity down to the level that, while, yes, it still generally works, it can now be made to fail if you're clever about how you go about doing that.

Google wrote:

Rowhammer is a complex class of vulnerabilities across the industry. It is a hardware vulnerability in DRAM where repeatedly accessing a row of memory can cause bit flips in adjacent rows, leading to data corruption. This can be exploited by attackers to gain unauthorized access to data, escalate privileges, or cause denial of service. Hardware vendors have deployed various mitigations, such as ECC (Error Correction Code) and TRR (Target Row Refresh) for DDR5 memory, to mitigate Rowhammer and enhance DRAM reliability. However, the resilience of those mitigations against sophisticated attackers remains an open question.

To address this gap and help the ecosystem with deploying robust defenses, Google has supported academic research and developed test platforms to analyze DDR5 memory. Our effort has led to the discovery of new attacks and a deeper understanding of Rowhammer on the current DRAM modules, helping to forge the way for further, stronger mitigations.

I'm not going to spend a lot more time on this since we have deeply and thoroughly covered the multiple RowHammer discoveries and the futile attempts to solve the problems. I have a link in the show notes to Google's full posting for anyone who might want a full update: https://security.googleblog.com/2025/09/supporting-rowhammer-research-to.html

Skipping all of that, we get to Google's "Lessons Learned" where they write:

We showed that current mitigations for Rowhammer attacks are not sufficient, and the issue remains a widespread problem across the industry. Those mitigations do make it more difficult "but not impossible" to carry out attacks, since an attacker needs an in-depth understanding of the specific memory subsystem architecture they wish to target.

Current mitigations based on TRR and ECC rely on probabilistic countermeasures that have insufficient entropy. Once an analyst understands how TRR operates, they can craft specific memory access patterns to bypass it. Furthermore, current ECC schemes were not designed as a security measure and are therefore incapable of reliably detecting errors.

Memory encryption is an alternative countermeasure for Rowhammer. However, our current assessment is that without cryptographic integrity, it offers no valuable defense against Rowhammer. More research is needed to develop viable, practical encryption and integrity solutions.

Google has been a leader in JEDEC standardization efforts, for instance with PRAC, a fully approved standard to be supported in upcoming versions of DDR5/LPDDR6. It works by accurately counting the number of times a DRAM wordline is activated and alerts the system if an excessive number of activations is detected. This close coordination between the DRAM and the system gives PRAC a reliable way to address Rowhammer.

PRAC? P. R. A. C. stands for "Per Row Activation Counting" and if you're ever in need of a quick example for which the word "kludge" was coined you need look no further. It's too bad that the word "DESPERATION" has too many letters to serve as the abbreviation for some means of solving this problem since "desperation" is what it's come down to if your solution is to add hardware counters into your DRAM memory's wordline activations as a means of detecting when someone may be "yanking your line" with malicious intent.

What a mess. But props to the original researchers at Carnegie Mellon University who, 11 years ago, back in 2014, discovered this nightmare and brought it to the world's attention.

SAMSUNG screen-enhanced refrigerators to begin showing ads
I've always found it interesting – and certainly depressing – that science fiction, when depicting a futuristic dystopia, invariably shows it filled beyond brimming with monstrous bright and flashing animated holographic 3D advertisements. It's always way beyond garish. Those scenes show us the presumed consequences of commercial consumerism without any boundaries where he who shouts the loudest attracts the most customers.

Anyone who had seen some of that Sci-Fi might have wondered whether the manufacturer of a residential kitchen refrigerator which touted its overly large touch screen, might ever succumb to their baser instincts, finding themselves unable to resist the temptation to make just a few more after-sale dollars by assaulting the owners of those refrigerators, many of whom had purchased those connected cold storage boxes for as much as $2,000, with a series of unsolicited product advertisements on their device's screens.

If you answered "yes, of course they would" – sadly, you would be correct. Samsung has begun displaying advertisements on the screens of its large-format display refrigerators. While they do not give users the option of declining, I suppose the device could be removed from the Internet.

China now banning NVIDIA chips
It's somewhat difficult to keep up with the daily back and forth of current import and export policy. The last I had heard was that NVIDIA had scored a huge win with China after NVIDIA's CEO, Jensen Huang, reported a very productive oval office meeting with Donald Trump. But, as I said, it's been difficult to stay current. The latest news is that China's government has now told their companies to stop purchasing NVIDIA chips. According to the Financial Times, companies were told to stop tests and cancel orders. The move is reportedly part of Beijing's efforts to boost the local semiconductor sector and cut its dependence upon US suppliers such as NVIDIA. Also, Chinese officials again accused the US of attempting to sneak backdoors to NVIDIA chips. We previously covered and shared Jensen's very clear and adamant statement that it would never under any circumstances compromise the integrity of its chips with secret backdoors. In that statement he reminded the world what a disaster the Clipper Chip had been.

300 more NPM packages taken down
I'm sure that I hardly need to caution any of our listeners about the dangers inherent in the use of packaged libraries found on open and open-source software repositories such as NPM. But last week, 300 more malicious NPM packages were found and taken down.

Please be careful.

Listener Feedback

Greg James

Steve, I was reviewing your observations regarding post-support Windows 10 updates and 0Patch. Reading the fine print of their FAQ's they state:

"In case the subscription is terminated without renewal, or the trial expires without purchase, all micropatches on computers associated with the subscription get un-applied until a new subscription is established for these computers."

https://support.0patch.com/hc/en-us/articles/360016654080-Does-a-PRO-or-Enterprise-license-grant-me-permanent-ownership-of-downloaded-micropatches-What-will-happen-when-my-subscription-ends

From my perspective, this is a fine example of holding us hostage. Also, their annual subscription for the "Pro" version, required to get Microsoft's security patches beyond the zero-day that 0Patch provides for free, amounts to the same $30/year that Microsoft charges – albeit 0Patch is willing to hold us hostage for "at least" 5 more years for the privilege of staying with Win 10. Just thought you'd like to know if you didn't already.

I was not aware of the fact that the patches applied by 0patch are only in place as long as the 0patch subscription remains valid. So I'm glad to know that and my feeling is that fact ought to not be buried in a FAQ. It ought to be made very clear – though I don't know that they don't make it clear. I don't know either way.

The way that I can see it sort of making sense, at least from their perspective, is that none of the 0patches ever modify any of Microsoft's files on disk. As we know, 0patch only applies patches in RAM, and it's a clever solution. It means that they are never modifying Microsoft's files, so their digital signatures are never broken. And it means that flaws can be patched on-the-fly without any need to reboot a machine. When this is a busy server on which others are depending, that can be a real win. So thanks, for the heads up about that, Greg.

Nic Neidenbach

Heya Steve & Leo, While listening to Security Now #1043, I was compelled to send some feedback about user training in regards to phishing scams in email.

It doesn't surprise me that the training was proving ineffective as I regularly see employers send emails with links that the employee often has to click. Things like alert notifications, announcements, meeting requests and even choosing yearly benefits. Then there are emails from vendors which can have all kinds of actionable tasks that require clicking on a link. GoDaddy, for instance, sends an email about domain renewals with links to the details.

Sadly the training can't just be simple like "don't click on links in emails". Instead, it's more complicated, the challenge is teaching them how to recognize a safe link. Or even better that instead of clicking on a link, go to the site and navigate to where you need to go manually.

Thanks, -Nic (Spinrite Owner and Listener since eps 1)

I think Nic's point is a very good one. I'm glad he made it. He's 100% correct. When I consider all the links I receive for one good purpose or another through email, it's clear that *"don't click on anything you receive in email"* is an impossible nonsense recommendation. So what we really mean is *"only click on the safe links"* and *"never click on any malicious links"* – but since phishing attacks are deliberately designed to make bad links appear good, that's no help either.

So this brings us back to my most recent thought, which is that the networks of enterprises great and small need to be designed to be strongly resistant to these sorts of mistakes which will be made by insiders. I think this means that the principles of *"least privilege"* need to be designed into the way any company's networks operate.

Glenn Hochberg

Hi Steve, I was listening to episode 1043 today, and when you were discussing how it's impossible to train users enough not to click on potentially malicious links, I recalled that when I worked for a large corporation (I retired earlier this year) they had at least a partial solution to this problem. They employed a third-party product that would filter all the incoming email and replace any links with encoded links to the third-party vendor's website. When a user would click a link in their email, the vendor site would look up the forwarded URL in their constantly-updated database of malicious websites, and either reply with a security warning page with a link to apply to get the referenced URL added to the white list if necessary, or else they would forward the user on to the validated URL. No doubt this is not a completely foolproof system, but it certainly helps. Thought I'd bring this to your attention if you were not already aware of this.

Thanks for all you and Leo do. I am a long-time listener (since sometime in your first year I think) and a TWIT subscriber, and look forward to listening to Security Now each week. I spent the last 20 years of my career in cybersecurity at that large corporation, and there were many listeners there. -Glenn

The solution provided by that vendor makes a lot of sense. One thing we've seen is that something as simple as the registration age of the domain referenced by a link's URL can provide a highly reliable signal to any threat detector.

And notice that early knowledge of any new threats is provided by the links that they are filtering on their customer's behalf. If such a third-party vendor has many customers, all of the links being filtered on behalf of all of their customers will allow them to compile and maintain a central "bad links" database. It's very much the way Gmail has a huge advantage by having so much visibility into so many of its users. Any new spammer will be seen very quickly.

Fabio in Switzerland

dear steve, i'm a longterm listener since episode 1 and spinrite owner. my 10 year old imac 27" 5k finally gave up and i bought a new mac studio. i m using one external 2tb ssd where i have all my photos stored (1.38TB used) and one new external 12TB WD My Book with my videos (5.6TB used). i'm doing time machine backups and use 3 different drives, 2 offline and in 2 different locations. i bought the drives in different years, hoping to get different productions batches and these are all wd my books with 14TB. i don't remember, but these

drives are for sure 6-8 years old and i'm thinking of adding another drive to my backup set.

i'm thinking of buying a external wd my book 18TB and i wonder how you judge the different technologies used in the different drive size 8, 10, 12, 114, 16, 18, 20, 22, 24 and 26tb for the usage as backup drive? chatgpt tells me, that wd 8-12tb seem to be the most reliable as it is most of the time a whitelabeled ultrastar drive.

any comments are highly welcome and might be also interesting to your podcast listeners. best from switzerland, fabio

I don't have any strong opinion about optimal drive size based upon experience. The only thought I have is about redundancy, in which I believe strongly. After all, that's the entire reason for backing up our data, so that we can have redundant copies elsewhere. I run double-redundant RAID 6 arrays on all of my NAS systems and on all of GRC's servers. It sounds like you have the redundancy side handled with all of those WD MyBook external drives.

The only thought I have is that it sounds as though your system of backing up has grown and evolved gradually over time, and that as a consequence it has remained somewhat manual, needing to plug drives in and out and I assume, manually run Time Machine, and so on. The advantage to the way Leo and I have set up our environments is that everything is always being backed up all the time, with versions of everything ... without us ever needing to do or to remember to do anything. It's all established once and then it just goes.

It's a different way of operating, but it might make sense for you to stop and take stock in the entire approach you have and see whether moving some drives into a RAID array of some sort, putting it on the network and setting up for continuous background backups might be an entirely different and useful way for you to think about backups. :)

Farnsworth

Hi Steve. You mentioned getting a Samsung Galaxy A15 for $39 a couple of months ago. I have one of those and would like to get another, but I can't find it or anything similar at anything close to that price point. Can you tell me where you got yours?

I went over to Amazon, which is generally my go-to retailer and I found nothing. Then I remembered that I had purchased the phone at BestBuy. So I went over there and found it for $49.99. So no longer $39, but still close. However, the phone I purchased was by Total Wireless. Best Buy carries Total Wireless, Boost Mobile and Boost Mobile and AT&T Prepaid, each of them for that $49.99 price with AT7T having a 4.8 out of 5 rating. So… For what it's worth! :)

Ryan Stoops

Hi Steve, I've been a podcast listener for about 10 years, and I am immensely grateful for all the work you put in to keep your audience informed about the latest security topics. Like other listeners, I have also used Security Now for CPEs on my CISSP.

I was very interested in the segment you did on Memory Integrity Enforcement. But I have been an Android (currently Samsung Galaxy) user since the last days of webOS and the Palm Pre. Can the advances Apple has made be replicated or adapted to secure Android devices? Are the references to "the unique strengths of Apple silicon hardware" just marketing fluff or do I have to acknowledge their security prowess and grudgingly switch ecosystems? Thanks, Ryan

Nothing that Apple has done would be impossible to replace. But Apple has a huge advantage over Google and Samsung with Android because they control all of their systems' hardware, its OS and much of their devices' supporting applications such as photos and messenger and Safari. We've seen that these other apps form the attack surfaces which attackers leverage for access to deeper underlying flaws.

Also, expanding upon a hint of what I said last week, an argument could be made that Apple has become somewhat like Ahab with the White Whale in its obsession over these flaws. On the one hand, I salute them for taking this stand and for really ***really*** saying ***"NO!"*** to **any** intrusion into their system, whether it be great or small; but my lord has this been done at great expense.

It's a testament to... I'm not sure what. Stubbornness? Some form of insanity? Ahab famously said *"I'd strike the sun if it insulted me."* Somewhere inside Apple are people who apparently feel similarly about having their device's security breached. But I wonder whether, when they began, they appreciated what it was going to take to fully pull it off, as they now have? And that work is not finished. It never will be. This insanely high level of security will require maintenance. It still needs to be watched, maintained and probably extended and evolved over time.

So I think my point here is that in today's world, with the hardware we have and software being created as it is, the actual cost of absolutely and utterly hardening a powerful and deeply connected consumer computing product – the way Apple just has with iOS 26 and their A19 chips – and then maintaining that level of security, is astonishingly high. This goes way past the point of diminishing returns.

It's a price so high that it almost didn't make sense for Apple to pay it, and I cannot imagine that either Google or Samsung are capable of caring enough to make the same sort of investment. And it's not clear that they should. The payback for them would be quite difficult to justify because a strong argument could be made that their Android devices are very nice and their security is "very good" and they ought to be content to keep them patched, yes, forever playing catch up, but also operating far more economically, than Apple.

The EU's Online Age Verification

I am sure that everyone who's been listening to this podcast for the past few years, and especially for the past few months, will be well aware of my extreme interest in – and perhaps even my preoccupation with – solving the problem of online Internet age verification.

As we know, I was interested enough in the somewhat related problem of online Internet identity authentication to have spent seven valuable years of my life fully developing a solution and solving that problem. While online age verification and identity authentication are somewhat related, the problem of age verification brings some trickier bits.

In the case of online Internet identity authentication, it's not one's actual identity that's being authenticated. What it actually is, is the ability to later prove that you have returned – that you are the same anonymous identity that you previously established with a remote website. To accomplish that, there's no need to ever rely upon any *"identity anchor"*. If we use the original username and password authentication we're simply saying *"Someone has returned who knows the username and password that were previously established, thus you should assume that it's the same individual."* And when we use either SQRL or Passkeys, we're simply saying *"Here's a public key for which I have the private key. Now and at any point in the future, I will sign any unique random challenge you might send me to prove to you that I continue to hold that public key's matching private key."* In other words, at no point are we asserting anything beyond the fact that we have returned.

Even just the term *"Age Verification"* indicates that it's something more. The user of a properly operating age verification system need not have ever visited a verifying site before. So it's out about having returned. The first time they visit any site that wishes to verify that they are of at least a certain age, such a system should be able to challenge them to prove they are above a certain age. The user should see that challenge pop-up on their client and then elect to permit their Internet client to assert the truth of that minimal age assertion on their behalf – but only if that assertion is actually true for them.

And that's the tricky bit. Any age verification system must be very tightly bound to them – to their real world physical identity. This is another way in which it differs from any fully anonymous Internet authentication system. If we chose to, we could give a friend our username and password, our one time password token key or even our passkey. In other words, traditional Internet identity associations are transferable because they are not intrinsically about **us;** they are all only about the reassertion of the possession of some secret – a secret that could be shared with anyone else.

So, to my mind, the biggest challenge to solving this problem will not be technology. As I've noted, all of the technological pieces exist and can be deployed without much trouble. The challenge will be the establishment of a true identity anchor – the link between the age verifying technology and its user's true real world age.

Let's now look at a bunch of news to see what's been going on and where the world stands:

Brazil joins the Age Verification party
On the topic of age verification, under their headline *"Brazil enacts sweeping bill requiring online age verification, safeguards for children's data"* The Record informs us that Brazil has joined the UK, writing:

> *Brazilian President Luiz Inácio Lula da Silva on Wednesday signed a law requiring digital service providers to verify the ages of users and adhere to strict new data protection and privacy requirements for children and adolescents.*
>
> *Brazil's **Digital ECA** mandates that tech companies take "reasonable measures" to block young users from accessing content which features violence, porn, sexual exploitation, drugs or gambling, as well as content that encourages self harm.*
>
> *The law requires that **"reliable"** age verification mechanisms be used to ensure users of digital services containing inappropriate content are over age 18. Self-declaration is no longer adequate as part of the law. It also orders that tech companies set up a "parental supervision mechanism" to ensure adults can "limit and manage the use of the service, the content accessed and the processing of personal data carried out."*
>
> *Platforms also cannot process children's personal data in a way that violates their privacy or use their data for targeted advertising. The measure, which overhauls a 1990 law, will take effect in March.*
>
> *Human Rights Watch organization wrote in a prepared statement: "Brazil has stepped forward as the first country in Latin America to pass a dedicated law to protect children's online privacy and safety." In June 2024, Human Rights Watch reported that personal photos belonging to Brazilian children were used to create artificial intelligence systems which were turned into deepfakes of other children being abused.*

This news that Brazil had joined the UK in legislating that self-declaration of one's age would no longer be sufficient, one has to wonder what the legislators who passed this new law imagined would happen? Six months from now, websites peddling violence, pornography, sexual exploitation, drugs or gambling will face fines of USD $9.44 million or up to 10% of their Brazilian revenue, if they do not prevent underage children from accessing their adult content.

In other words, what we're seeing everywhere is that the laws that have long applied only in the physical world, not in cyberspace, are finally starting to be applied to both commercial and free online services in the cyber realm. And, when these laws are tested with appeals to courts having final-say jurisdiction, they are being upheld under the theory that the greater good will be served. And, at least in the US, that requiring mature citizens to prove their physical age by divulging their real world identity is not unduly burdensome.

Brazil's passing of this legislation last week while bragging that it was the first Latin American country to protect the children, got me wondering what the W3C might be doing to get an acceptable solution into the hands of the world's web browsers and websites.

And, as it happens, I found a page at the W3C with the headline: *"Upcoming: IAB/W3C Workshop on Age-Based Restrictions on Content Access"*. The page, which was posted in the middle of July, says: *"W3C announced today the IAB/W3C Workshop on Age-Based Restrictions on Content Access, 7-9 October 2025, in London, UK."* ... which is exactly two weeks from today.

Upcoming: IAB/W3C Workshop on Age-Based Restrictions on Content Access
The workshop announcement says:

The Internet Architecture Board (IAB) and World Wide Web Consortium (W3C) are convening a workshop to examine the technical and architectural implications of different approaches to implementing age-based restrictions on access to online content.

The young are often unprepared for the sorts of things they might find online. Maturity, education, and the guidance of responsible adults can help children navigate online interactions, but age is often regarded as the best indicator of how able a person is to cope with exposure to content.

Increasing interest is being shown in the implementation of regulation that restricts what content young people can access online. A recurring theme in these efforts is that it is no longer considered sufficient to rely on self-assertions of age. A number of jurisdictions have enacted—or are in the process of enacting—laws that take steps to provide stronger guarantees that children are not exposed to certain content.

This workshop seeks to perform a thorough examination of the technical and architectural choices that are involved in solutions for age-based restrictions on access to content. We do not expect to identify a single candidate solution, even if that might be an ideal outcome. The goal is to build a shared understanding of the properties of various proposed approaches.

In general, access restrictions are achieved by selectively blocking or filtering. RFC 7754 (Technical Considerations for Internet Service Blocking and Filtering) provides a more general framework for how to think about restrictions on communications. This workshop will build on that work. In particular, it will seek to examine the specific technical considerations that apply when content is legally accessed by some people and restricted for others based primarily on their age.

Individuals interested in participating in this activity can indicate their interest by submitting a short position paper. Position papers do not represent either the IETF or W3C. In some cases, an expression of interest is sufficient.

Topics of interest, as identified by the program committee, include:

- *Surveys of the common features of regulation on age restrictions*
- *Analysis of the technical requirements that might apply*
- *Identification of other key factors to consider in the design of a technical architecture, including, but not limited to, privacy, equity of access, market dynamics (such as centralization), vulnerability to circumvention, cost, accuracy, jurisdiction/geolocation, and censorship*
- *Details of possible technical architectures, whether in whole or part:*
  - *For determining the age of people*
  - *For identifying content that might need to be restricted*
  - *For controlling access to identified content*
- *Comparisons of different technical architectures*
- *Examination of how technical architectures might interface with or rely upon regulation or other governance structures*
- *Feasibility of different approaches*
- *Exploration of the ramifications of choosing different technical architectures*

Reading through that, I became rather disheartened, since it is exactly this W3C group that will need to produce the standards that we are – right now this very moment – in desperate need of having, yet they still appear to be quite a long ways away from even having a rough working specification of anything. Their announcement of these meeting ended by adding:

> *Input on other relevant subjects is welcome. Papers that are submitted will be used in developing a workshop program. Position papers from those not able to attend the workshop are also encouraged. Submissions can be made by emailing papers to age-workshop-pc@iab.org. Participants can choose their preferred format, though short PDF submissions (around five A4 pages) are preferred.* ***Submissions will be published with attribution*** *unless the submission clearly indicates a preference that the submission be kept private or published anonymously.*

I was pleased to see that submitted position papers would be published since this workshop will be held in person in London, not via the Internet, and it will not be broadcast or recorded.

So we have what appears to be a very early stage workshop being held in London where deeply philosophical questions will be addressed, as if for the first time, such as "what do we really mean when by age verification?" – I'm glad I won't be there since I'd be jumping up and down asking people to please just write some code, already.

The better news is that the EU appears to be somewhat ahead in this regard. Early last month, Spain announced that it would be using the W3C's existing "Verifiable Credentials" (VC) solution. The announcement said:

> W3C Verifiable Credentials (VCs), are the future of verification, with Member States continuing to embrace this powerful and versatile technology. Spain has recently released technical specifications for their new online age verification system, aimed at controlling the age of users seeking to access online adult content.
>
> In the last few years, different specialists have come to the conclusion that the easy and free access to online adult sexual content is harming kids and teenagers' mental health and their social and relational skills. Therefore, Spain is planning to limit minors' access to this type of content by implementing an online age verification procedure. This system will use W3C Verifiable Credentials and focus on a protocol for verifying the age of majority without disclosing personal information that could identify or track the user. By applying this data model, the content providers can verify the age of the user without accessing any other personal data, thus minimising the data disclosure and adhering to General Data Protection Regulation (GDPR) principles.

That all sounds like exactly what we want. Spain's announcement explains the basis for their decision under the subhead: *"Why are W3C Verifiable Credentials the right choice for online age verification?"* They write:

> *W3C Verifiable Credentials are a digital document format that can represent a wide range of information or claims about an entity (such as a person, organisation, or device) that can be cryptographically verified. These credentials are designed to be secure, tamper-evident, and privacy-preserving, allowing the holder to present them to verifiers with a high level of trust.*

W3C Verifiable Credentials are the future of verification because they offer:

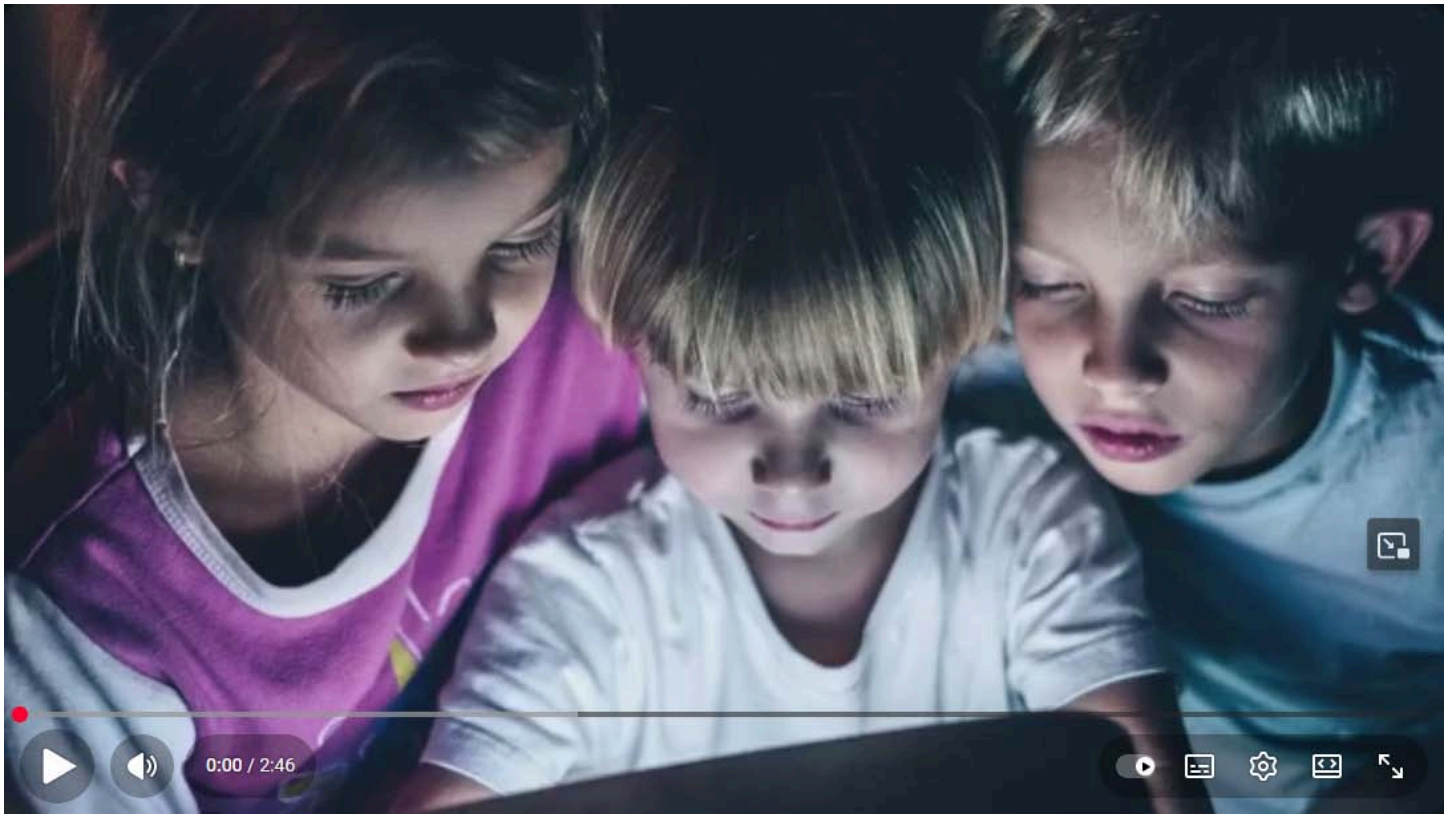
- *Unmatched Security: Advanced cryptographic methods make W3C VCs tamper-proof and trustworthy. They could also comply with signature schemes of the eIDAS regulation for secure digital transactions and ensure the provenance of information.*

- *Enhanced Privacy: When sharing a VC, users can choose to share only the necessary information, embedded in credentials, without revealing more than required (e.g., proving the user is above a certain age without sharing the full date of birth). This safeguards the privacy of users' personal information and empowers citizens' sovereignty over their information by allowing them to govern the access to their personal data, something that until recently was not conceivable for many due to the nature of information sharing processes.*

- *Portability: Verifiable Credentials can be seamlessly stored and linked to digital wallets and be presented when needed.*

The key requirement of Spain's online age verification system is the privacy and untraceability of users' activity, when presenting their age for verification online. This makes W3C Verifiable Credentials data model the perfect choice for such use-case. Their technical solution follows the OpenID For Verifiable Presentations (OpenID4VP) specification, ensuring secure and private verification of age credentials. Additionally, the framework includes trust management via whitelists, which ensures only trusted entities can issue or verify these credentials.

Blueprint for an age verification solution to help protect minors online. Short version:
https://www.youtube.com/watch?v=7FYfbSr6wz8 https://grc.sc/1044



Before I talk about that video I want to share a few representative comments that were left about the video after it was posted:

- Orwellian government here we go...
- "Due to local laws, we are temporarily restricting access to this comment until the EU estimates your age"
- Whoa amazing I love censorship in the Western world, so progressive
- Didn't realize I was living in North Korea all along
- I love having to have to deal with this garbage because parents can't just be good at being a parent!
- Please no. Stop with this nonsense. 1984 should be a warning, not a blueprint.
- Does anyone have a link or petition to vote against this?
- Hell no! I hate this! Any petition to sign against this?!?
- Age of no privacy, the cyberpunk timeline might be real.
- Perfect. Restrict most of the internet and create a surveillance state because some parents are too dumb to watch their children.

At some point I would imagine that some of these outraged comment-leaving people are going to wish to go somewhere on the Internet containing content that cannot be legally viewed by minors within their country, province or state. Without something like what this video shows us, the laws have changed to now require all such websites to proactively verify every single visitor's age. As we've seen, "self-declaration" no longer cuts it. The *"Yes, I'm 18"* button, ridiculous as it always was, is being tossed into the wastebin of Internet history.

This change in the law will require these commenters to produce some form of proof of age. The problem with that is that anything we have today requires the disclosure of a true real world identity. Within the EU, UK and US, one must be at least 18 years old to obtain a credit card. So it might be that until we have something better, providing proof of age with a valid credit card would work. But that's certainly not anonymous, and I would never want some sleazy website to have mine.

My point is, while I completely understand and sympathize with the sentiments of these people, the truth is that the Internet has been a cyber-world exception from the laws and responsibilities of the real world, and that is finally changing. These people are likely living within democracies in which their elected government legislators have recently decided that if they want to continue to have access to adult material online they're going to have to **prove** that they're old enough.

No, as for what that video showed, I am very impressed. To the EU's credit, they got it all exactly right, 100% without caveat. What that video shows is exactly how the system needs to work. The comment attached to that EU YouTube video which was posted two months ago, says:

> *[The European] Commission is developing a harmonised approach to help online platforms implement a user-friendly and privacy-preserving age verification method. This blueprint launches a pilot phase during which a software solution for age verification will be tested and further customised in collaboration with Member States, online platforms and end-users. Denmark, France, Greece, Italy and Spain will be the first to take up the technical solution in view of taking it up in their national digital wallets or publishing a customised national age verification app on the app stores. Market players can also take up the software solution and further develop it.*

So, someone owning an iOS or Android smartphone – remember that I purchased that lovely new Samsung smartphone for $40 – downloads their country's approved age verification application. They then provide that app some form of proof-of-age. It might be their existing digital ID, passport, or other information.

This information is collected along with an assertion of age, and provided to the app's associated certifying agency. The certifying agency uses its private key to sign what is known as an "over age token credential". This is a formally designed and structured JSON object.

I have a sample of one in the show notes:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/age/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "urn:uuid:188e8450-269e-11eb-b545-d3692cf35398",
  "type": ["VerifiableCredential", "OverAgeTokenCredential"],
  "issuer": "did:key:z6MkkUbCFazdoducKf8SUye7cAxuicMdDBhXKWuTEuGA3jQF",
  "issuanceDate": "2022-03-24T20:03:03Z",
  "expirationDate": "2022-06-24T20:03:03Z",
  "credentialSubject": {
    "overAge": 21,
    "concealedIdToken": "zo58FV8vqzY2Z...rX8o46SF"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-08-07T21:36:26Z",
    "verificationMethod": "did:key:z6MkkUbCFazdoducKf8SUye7cAxuicMdDBhXKWuTEuGA3jQF
      #z6MkkUbCFazdoducKf8SUye7cAxuicMdDBhXKWuTEuGA3jQF",
    "proofPurpose": "assertionMethod",
    "proofValue": "z4mAs9uHU16jR4x...RSu9jSxPCF"
  }
}
```

The textual JSON object provides context with URLs from w3.org and w3id.org.

It identifies the data as being a *"VerifiedCredential"* and an *"OverAgeTokenCredential"*. It indicates the *"issuer"* of the credential, the *"issuanceDate"* and *"expirationDate"*, and the *"credentialSubject"* is listed: *"overAge": 21* or 18 or whatever.

At first I was annoyed that the syntactical term used is "overAge". My first thought was that it should be "AtOrOverAge". But then I realized that birthdays are anniversaries. So when someone reaches their 18th birthday they're not 18. Each birthday marks the END of that year of their life. So anyone who is 18 is over 18 since they're now into their 19th year.

After specifying the context, the issuer, the issuance date, the credential's expiration date and the credential's subject being an assertion of age, the remaining information contained in the object is its proof of validity.

Significantly, nowhere, anywhere, in the credential is there anything that identifies the individual.

But there are some serial numbers. As we know, anytime we have a digital signature we need to have some sort of guaranteed unique entropy data to make each signature unique. So I dug around to see exactly what we going on, and I found definition of an *"overAgeTokenCredential"*:

This *"overAgeTokenCredential"* is called a Privacy-preserving single-use tokenized age credential. Its definition says:

> *A privacy-preserving single-use tokenized age credential that can be used during an age-gated transaction. The receiver of this credential can verify both the age category of the holder that delivered this credential and know that the credential has been digitally signed by an age verification authority without being able to track the individual using the token. The age verification authority is the only entity that can map the single-use token back to an individual. This process is manual, and only occurs if a legal subpoena for information is filed in a court of law during a legal proceeding. An individual that uses these tokens will utilize a different token per transaction, which protects their privacy among anyone engaging in an age-gated transaction with the individual while meeting regulatory burden for age-gated transactions that require that a proof of age was checked. This credential is either presented electronically over the Internet, or displayed as a single-use QR Code at a point of sale.*

In other words, anyone relying upon these age-assertions – such as the sleazy website – will be absolutely and utterly blind to every visitor's identity. There's nothing for them. But the original issuer of the *overAgeTokenCredential* will always have the means, if compelled legally, to map the use of any credential they've signed back to whatever form of proof-of-age they were given when the credential was originally created.

The other thing that I noticed in their demo video was that the use of biometrics was optional with a 6-digit PIN being the normal default. That allows for more freedom for "borrowing" someone else's age without needing them to be present when their age is asserted than I was expecting.

I also encountered a mention of the use of someone's profile as a camera-based biometric. The idea, presumably, was that a profile reveals the forehead slope, eye location and features of their nose, mouth and chin, while not revealing their identity as much as a full frontal facial image.

One thing we know for sure, as we move forward with this, is that we cannot ask users to have multiple incompatible age verification apps in their phones where, for each one, they need to separately prove their age. This could all become a huge mess if the entire Internet does not quickly standardize upon a single common solution that will provide everyone, meaning every jurisdiction that requires some form of proof of age, with an acceptable solution.

There is no sign that we're going to obtain absolute subpoena-proof age verification, but at least the sites we visit will have no way of tracking or unmasking anyone. And the existing W3C work on Verifiable Credentials looks like the way this problem is going to be resolved. We may not have long to wait!