Identity, Decentralized identity and verifiable credentials, Privileged access management, IAM Technologies

The State of Identity in 2024: Passkeys, deepfakes and IAM-PAM convergence

Paul Wagenseil June 10, 2024

Related Events

CYBERCAST

Identity Resilience: The Missing Piece to Securing Your Identities

On-Demand Event

CYBERCAST

Identity security and user experience – there shouldn't be a trade-off

On-Demand Event

Getty Images

Three main trends dominate identity and access management (IAM) in 2024. First, regular IAM solutions are borrowing access controls from privileged access management (PAM) platforms to the extent that IAM and PAM seem to be converging.

Second, the identity industry is operating under the assumption that passkeys, the cryptography-based passwordless authentication tokens, will quickly be adopted by both consumers and enterprises. Among identity professionals, the question of whether passkeys will replace passwords seems to be not if, but when.

Finally, the rapid advances in AI-driven deepfake technology have reached the point where humans can't tell the difference on a video stream between a real human and a deepfake. This has enabled at least one spectacular multi-million-dollar heist this year, and identity-verification providers are scrambling to keep ahead of the deepfakers.

IAM is the new PAM

In many organizations, highly privileged users like network administrators and financial officers are subject to additional access controls that ordinary users don't encounter. These highly privileged users may use the regular IAM interface to log

into their endpoints and email accounts. But when it comes time to access sensitive areas, they may have to log into a PAM interface, sometimes with a different username and password.

Under the hood, the PAM system enforces a stricter set of policies than an IAM system. User behavior is more carefully monitored and logged. Passwords need to be stronger and may be rotated more frequently, and multi-factor authentication (MFA) is almost always required. Special permissions may be granted only to accomplish a particular task, then revoked when the task is completed, a practice known as just-in-time (JIT) access.

The explosion in remote work during the COVID-19 pandemic and the rapid adoption of cloud computing have blurred the lines between ordinary and highly privileged users, and created new avenues of attack.

Adversaries don't need to break into a system if they can log in using stolen or cracked credentials. And when any IT staffer can easily spin up a new cloud instance, misconfigurations and muddied access controls can result in low-privileged employees gaining entry to sensitive areas.

As a result, many of the practices and controls of PAM are migrating over to IAM. Mandatory MFA is just the beginning. The newer IAM solutions may rigorously monitor and log all user activity, force users to log in again when accessing new areas and enforce the principle of least privilege so that a user has only those permissions necessary for their job.

Some IAM deployments are experimenting with just-in-time access, and others are going even further and implementing zero standing privileges, which grants no user permanent special permissions — all access to sensitive areas is just-in-time.

Organizations are also encouraging the use of hardware security keys by all staffers (which can be costly) or device-bound passkeys, which, unlike passwords or weaker factors of MFA, cannot be phished.

"Passwords should no longer be the golden key, and sessions should no longer give you permanent access," said Sean O'Dell, senior staff security engineer of identity security at Disney, in a speaking session at the Identiverse 2024 conference last month.

Quoting identity-security expert Ian Glazer, O'Dell added, "User accounts should have no standing access rights. They should not be able to do anything except log in."

The presumed preponderance of passkeys

At Identiverse, FIDO Alliance Executive Director and CEO Andrew Shikiar declared that the organization's goal was to "make passkeys inevitable." More than a dozen speakers at the conference delved into passkeys, but none we heard expressed any doubts about whether passkeys would soon become the dominant authentication standard.

Instead, the focus seemed to be on proper management of passkeys, especially in the enterprise. Apple, Google and Microsoft have stressed the consumer angle of device-bound passkeys, but hardware security keys like a Yubikey or Titan key are also FIDO 2.0-compliant passkeys and have been used in enterprises for several years.

Device-bound passkeys are a convenient alternative to passwords and may be strong enough to replace MFA, but only when implemented on Windows. As with a

hardware key, the private-key part of a passkey on a Windows laptop or desktop isn't synced and exists only on the device.

Not so with passkeys on Apple or Android devices. They can be synced in the cloud, either through the Google password manager or the Apple Keychain. This makes the passkeys recoverable if a device is lost, but it raises security concerns despite Google and Apple's insistence that their encryption of stored passkeys is safe.

At Identiverse 2024, two speakers from a very well-known technology company said that Apple's announcement of Keychain passkey syncing made their security chief "[soil] the bed." As a result, the company now subjects passkeys to contextual MFA challenges like any other form of authentication.

Other speakers brought up inconsistent passkey implementation standards. Some entities asking for authentication don't require the user to state their intent to use a passkey, which could make it easier for a bad actor to use a stolen passkey.

Some of the two dozen passkey authenticators will export passkeys in plaintext if the user chooses to migrate to a different authenticator, creating an opportunity for theft. And there's currently no way to tell if a passkey has been migrated and potentially duplicated.

"You should be using passkeys," said Dean Saxe, senior security engineer with AWS Identity and co-chair of the FIDO Alliance Enterprise Deployment Working Group, at Identiverse 2024. "Passkeys are better than passwords. But passkeys are not risk-free."

All this talk at Identiverse of inevitable passkey dominance seemed a little unreal, however. Outside of tech circles, how many times have you heard anyone even

mention passkeys?

Most non-tech people wrestle with implementing MFA properly, if they use MFA at all. Many companies, even large banks, still offer only texted, emailed or voice-called one-time-codes as the second MFA factor. Even some of the best-known online services won't accept passkeys as a single factor, though many accept them as a second factor.

Passkeys are great, they're easy to use, and despite the security concerns, are safer than passwords. But the general public appears to be a long way off from adopting passkeys. The digital-identity industry might want to focus more on educating consumers and companies about passkeys before it worries about the next steps.

Fake it till you make it

If you're an American taxpayer and you want to set up an online account with the Internal Revenue Service, get ready to jump through some hoops. You've got to send over images of your driver's license or passport, and then either take a selfie with your phone or sit down for a live video interview with an outsourced IRS representative.

Many hiring processes for remote work operate the same way. The goal is to make sure that you are who you say you are, and not some impostor assuming your identity, or someone using an entirely made-up identity.

But now, with the rapid acceleration of deepfake technology, it's getting harder for the IRS and potential employers, not to mention ordinary people, to be sure of whom they're talking to.

Not only can images of driver's licenses easily be faked, but still photographs of faces can be convincingly and inexpensively grafted onto those of others, even in video feeds. An iProov study found that face-swapping deepfake attempts to bypass remote verification grew by more than 700% in 2023.

Earlier this year, a financial officer at multinational firm was duped into sending thieves $25 million after the crooks deepfaked several company executives on a live conference call.

"When people present online, either to have their identity verified, or maybe to authenticate themselves, or just when they turn up on a video conference," iProov founder and CEO Andrew Bud told us at the Identiverse 2024 conference, "there is no longer any reason to believe that you're looking at who you think you're looking at."

Yet the same advances in processing technology that permit cheap, convincing deepfakes also benefit defenders. Bud told us that iProov uses the subject's screen to shine a random pattern of colored light onto the subject's face, which can then be analyzed by iProov's verification algorithms.

Other companies quickly validate driver's license and passports with lookups in public databases or use spectral analysis to distinguish an original photo from a copy. They can also aggregate dozens of data points about a subject, ranging from geographical location to the age of the subject's email address, to build a profile and assess its validity — a process that AI assistants such as Microsoft's Copilot can perform in seconds.

"The task is to make sure that a remote person is whom they claim to be, that they're the right person, that they're the real person, and that they're there right now

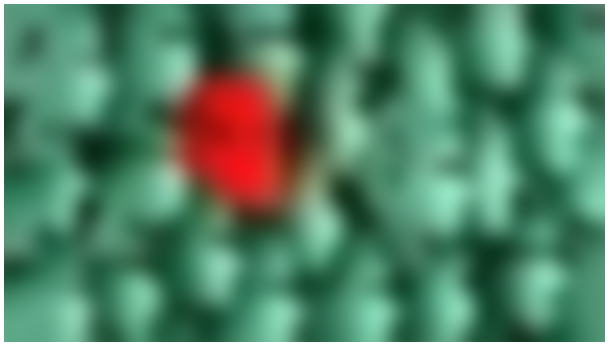
in the comfort of their own living room in an untrusted environment on an untrusted device," explained Bud.

(Editor's Note: This is part of a series of articles to feature the 15 Top Cybersecurity Trends of 2024 & 2025)

Paul Wagenseil

Paul Wagenseil is a custom content strategist for CyberRisk Alliance, leading creation of content developed from CRA research and aligned to the most critical topics of interest for the cybersecurity community. He previously held editor roles focused on the security market at Tom's Guide, Laptop Magazine, TechNewsDaily.com and SecurityNewsDaily.com.

Related



AI/ML

AI to further fuel accelerated synthetic identity fraud growth

SC Staff June 27, 2024

The report noted that synthetic identity fraud could be combated by public sector organizations through the implementation of omnichannel verification, or the corroboration of identities through multiple approaches.

SSO/MFA

Why MFA alone will no longer suffice

Mike Britton June 27, 2024

Here are four shortcomings of MFA in preventing account takeovers – and what to do about it.

PRIVACY

Pegasus servers sequestered in Poland

SC Staff June 26, 2024

The Pegasus spyware tool was sequestered by Polish prosecutors as part of the country's investigation into the previous government's alleged widespread abuse of the commercial surveillance tool.

ABOUT US

- SC Media
- CyberRisk Alliance
- Contact Us
- Careers
- Privacy

GET INVOLVED

- Subscribe
- Contribute/Speak
- Attend an event
- Join a peer group
- Partner With Us

EXPLORE

- Product reviews
- Research
- White papers
- Webcasts
- Podcasts