Strengthening identity protection in the face of highly sophisticated attacks

By
Alex Weinert
Published Dec 12 2023 09:00 AM 50.7K Views

When it comes to security at Microsoft, we're customer zero as our Chief Security Advisor and CVP Bret Arsenault often emphasizes. That means we think a lot about how we build security into everything we do—not only for our customers—but for ourselves. We continuously work to improve the built-in security of our products and platforms. With the unparalleled breadth of our digital landscape and the integral role we play in our customers' businesses, we feel a unique responsibility to take a leadership role in securing the future for our customers, ourselves, and our community.

To that end, on November 2nd, 2023, we launched the **Secure Future Initiative (SFI)**. It's a multi-year commitment to advance the way we design, build, test, and operate our technology to ensure we deliver solutions that meet the highest possible standards of security. Fundamentally, it encompasses three key engineering advances that help us meet our commitment:

1. ***Transforming software development with automation and AI***— Enhancing the Security Development Lifecycle (SDL) to integrate dynamic cybersecurity protections. This approach utilizes AI for secure code analysis, Github Copilot for auditing and testing against advanced threats, and new default settings for multifactor authentication to reduce the likelihood of breach by up to 99.22%.
2. ***Strengthening identity protection against highly sophisticated attacks***— Responding to the surge in identity-based threats, we're advancing identity protection across all products and platforms through a unified verification process for users, devices, and services. These advanced capabilities will also be available to external developers through standard identity libraries.
3. ***Setting a new standard for faster vulnerability response and security updates***—Our goal is to reduce the time it takes to mitigate cloud vulnerabilities by 50%. We will also take a more public stance against third-party researchers being put under non-disclosure agreements by technology providers. Without full transparency on vulnerabilities, the security community cannot learn collectively—defending at scale requires a growth mindset. Microsoft is committed to transparency and will encourage every major cloud provider to adopt the same approach.

Creating more resilient token signing key systems

To delve deeper into the second engineering advance—**strengthening identity protection against highly sophisticated attacks**—we've crafted a white paper focusing on the tangible actions we're taking towards more resilient identity systems and token signing keys.

As more customers understand the importance of multifactor authentication (MFA) and get ahead of the threat curve, we're seeing attackers increase the velocity of attacks on the remaining organizations that have yet to implement MFA by default. In our Secure Identities white paper, we share details on our engineering advances to strengthen identity protection, focusing on token signing key management and identity.

Explore the five categories shaping our token signing key management systems:

1. **Enhanced automation for key management (zero touch)**—Fully automate enterprise identity signing key management and

remove the ability of human error or exploitation. In the near future, we will move consumer keys to the same system.

2. **Storing and managing keys in secure hardware (HSM)**—Aim to have all identity signing keys stored in Hardware Security Modules (HSM) to make the keys invulnerable to accidental or intentional storage access.
3. **Ensuring keys are protected in memory (confidential computing service)**—Prevent keys from becoming exfiltrated even if the underlying processes become compromised —by using Microsoft Azure's confidential computing service to manage signing processes.
4. **Increasing key rotation frequency (rapid key rotation)**—More regularly and more rapidly retire and rotate keys in the identity infrastructure, so in the unlikely event a key is acquired, attackers will have little time to use it.
5. **Monitoring key usage for suspicious activity (built-in telemetry)—**Define security invariants, the things that must hold, and then explicitly build system logging, detections, and alerting to make sure we know instantly that something is behaving outside our expectations.

Read the white paper to learn more about each of the five categories and how they work together to protect customers against escalating identity attacks.

Ignite 2023: Continuously raising the identity security bar for our customers

At Ignite, I had the pleasure of sharing the stage with Mia Reyes, Director of Foundational Security at Microsoft, to present and receive live feedback on how we're strengthening identity protection. In the session titled "Boosting ID Protection Amid Sophisticated Attacks," Mia and I shared more information about the formation of the Secure Future Initiative (SFI) as well as alarming statistics and real-world incidents underscoring the dire need to reinforce identity protection. For example, we ran tests and found that on a first attempt of a malicious, unprompted simple MFA approval request, 1% of users will approve it—that's likely MFA fatigue. One way we're helping to reduce fatigue is with number matching in Microsoft Authenticator which helps MFA approvers to pause, focus on the request at hand, and then approve or deny the request. Beyond that, we recognize that we have to do more to help people. Watch the video below for a few policy updates we've released to increase MFA adoption.

MFA fatigue is only one of the many identity security issues our customers are facing, which I detail in the live session. MFA attacks can also include SIM Jacking, where a bad actor convinces a carrier to transfer your phone number, often by utilizing existing information they find online about you from social media or phishing—or even information purchased

from sellers of previously leaked and stolen data. And our customers have also seen attackers bypass MFA controls entirely using an adversary-in-the middle (AitM) approach to steal session cookies and gain access to a user's email accounts.

If you missed the live session, watch it now to learn about these types of infrastructure compromise attacks, plus password and post-authentication attacks. I also share more information on our advancements in identity protections in the session, including the automatic roll-out of Microsoft-managed Conditional Access policies, automated key management, and Hardware Security Modules (HSM) for fortified key storage—crucial innovations to mitigate human errors and bolster defenses against sophisticated aggressors.

Series: Unpacking the Secure Future Initiative

As we think about the current cyber threats our customers face, as well as the unique responsibility we have to continually and continuously improve the built-in security of our products and platforms, we want to continue this conversation over the coming months. To that end, this post will be the first in a series where we'll return to unpack and share more detail about the following concepts and commitments:

- Secure by default
- Common libraries & help for developers
- Innovations in how identity systems work (TB, SSE, CAE)
- Innovations in detection and monitoring
- Innovations in key management automation
- Innovations in secure key storage
- Innovations in secure key usage

Visit our built-in security website to learn more about our security approach. And stay tuned for more posts in the future as we work together to build a secure future for our customers, ourselves, and our community.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (@MSFTSecurity) for the latest news and updates on cybersecurity.

Co-Authors

Alex Weinert

Version history

Last update: Dec 12 2023 11:49 AM
Updated by: Trevor_Rusher

Labels

Share

What's new

Surface Pro 9

Surface Laptop 5

Surface Studio 2+

Surface Laptop Go 2

Surface Laptop Studio

Surface Duo 2

Microsoft 365

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Virtual workshops and training

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

Education consultation appointment

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft Industry

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

Your Privacy Choices