Identity and Access Management: Developer and Vendor Challenges

October 4, 2023

Summary:

On October 4, 2023, the Cybersecurity & Infrastructure Security Agency (CISA) and the National Security Agency (NSA) published Identity and Access Management: Developer and Vendor Challenges. This publication addresses the challenges developers and technology vendors face in identity and access management (IAM). While the publication predominately focuses on defining the challenges, CISA and the NSA provide some guidance on how to overcome these challenges.

Overview

The Memorandum for the Heads of Executive Departments and Agencies (M-22-09) required federal agencies to employ centralized identity management systems and use strong multi-factor authentication (MFA) throughout their enterprise. In addition to M-22-09, CISA has been recommending that government and critical infrastructure use MFA and single sign-on (SSO) services. Despite CISA and the White House's requests, the deployment of MFA and SSO has been challenging. This publication focuses on the technical challenges of implementing MFA and SSO, while providing recommendations on how vendors and developers can counteract the outlined challenges. One key factor the vendor community must be cognizant of is the interoperability of IAM solutions as no single vendor can solve all IAM challenges an organization may face.

Key Multi-Factor Authentication Challenges

MFA is difficult to deploy for both large and small organizations. The guidance focuses on three challenges to MFA implementation: definitional and policy challenges in the vendor community, deployment and adoption related challenges, and sustainment and governance related challenges.

- Definitional and policy challenges include unclear and confusing policies and definitions around different variations of MFA and a lack of clarity regarding the security properties that certain implementations provide.
- Deployment and adoption challenges include support for the strongest forms of MFA, such as those based on PKI and FIDO2 standards, in vendor products.
- Sustainment and governance challenges includes robust credential lifecycle management is often lacking in available MFA solutions

Multi-Factor Authentication Recommendations for Vendors

CISA and the NSA provided six recommendations related to MFA and divided them between three key challenges:

Key Challenge 1: Ambiguous MFA terminology

Recommendations

- Create standard MFA terminology that provides clear, interoperable, and standardized definitions and policies allowing organizations to make value comparisons and to integrate these solutions into their environment.
- Map products to NIST requirements such as those articulated in NIST SP 800- 63.

Key Challenge 2: Lack of clarity on security properties that certain MFA implementations provide

Recommendations

- Additional investment by the vendor community in bringing more phishing-resistant authenticators to more use cases to provide greater defense against sophisticated attacks. Further, simplify and standardize their adoption, including in the form factors embedded into operating systems would greatly enhance the market.
- Additional vendor investment in supporting high assurance MFA implementations for enterprise use on both mobile and desktop platforms in a maximally user-friendly flow to promote higher MFA adoption across all sizes.

Key Challenge 3: MFA reliance on self-enrollment by the user and “one time enrollment code flow” exposes itself as a potential threat actor

Recommendations

- Develop more secure enrollment tooling to support the complex provisioning needs of large organizations.
- Develop tools for automatically discovering and purging enrollment MFA authenticators that have not been used in a particular period of time or whose usage deviates from the expected behavior of a user could be enhanced.

Key Single Sign-On Challenges

Challenges identified with SSO include complexity and usability challenges, standards improvement opportunities, and ecosystem challenges.

- Complexity and usability challenges include a significant tradeoff between functionality and complexity, tooling for understanding trust relationships and the impact to changes in the configuration could be improved, and ensuring SSO can enable secure MFA across all use cases, including privileged access use cases.
- Standards improvement opportunities include current standards such as RFC 8176 do not cover all use cases and are not adopted by all vendors, the standardization of federation configurations themselves, and the strength of identity federation assertions themselves.
- Ecosystem challenges include architectures designed for leveraging open standard based SSO together with legacy applications not always being widely understood, in numerous RP applications SSO capabilities are bundled with other high end “enterprise” features in such a way to make them inaccessible to small and medium organizations, and identity lifecycle management through open standards (e.g. SCIM) is still not viewed as a core part of the development of business software.

Multi-Factor Authentication Recommendations for Vendors

CISA and the NSA provided five recommendations related to SSO and divided them between four key challenges:

Key Challenge 1: The significant tradeoff between SSO functionality and complexity

Recommendations

- Research into the development of a secure-by-default, easy to use, SSO system to address these gaps in the market. For example: Relying Party vendors could provide security configuration recommendations and their impact. Additionally, management of lifetime tokens such as ID token, Access Token, and Refresh Token should come with a reasonable secure default value which prevents abuse scenarios.
- IAM Vendors can aid in the detection of insecure implementations of identity federation protocols and work with the ecosystem to build awareness around these issues as well as improve the adoption of more secure uses of standards.

Key Challenge 2: Need to improve the currently deployed open standards throughout the identity ecosystem.

Recommendation

- Implement broader support for and development of identity standards in the enterprise ecosystem. This will enable a variety of security use cases, ranging from limiting access to managed devices to quickly revoking access when accounts are compromised.

Key Challenge 3: Architectures for leveraging open standard based SSO together with legacy applications are not always widely understood.

Recommendation

- Create a shared, open-source repository of open standards-based modules and patterns to solve these integration challenges to aid in adoption.

Key challenge 4: SSO capabilities are bundled with other high end enterprise features in such a way that makes them inaccessible to small and medium organizations.

Recommendation

- Include organizational SSOs in any pricing plan that are targeted at business customers, regardless of size.