DEVELOPER AND VENDOR CHALLENGES

IDENTITY AND ACCESS MANAGEMENT

NATIONAL SECURITY AGENCY CYBERSECURITY
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA
CSCC COMMUNICATIONS SECTOR COORDINATING COUNCIL
DIB Sector Coordinating Council National Defense ISAC
INFORMATION TECHNOLOGY IT SCC SECTOR COORDINATING COUNCIL

DISCLAIMER

DISCLAIMER OF ENDORSEMENT

This document was written for general informational purposes only. It is intended to apply to a variety of factual circumstances and industry stakeholders, and the information provided herein is advisory in nature. The guidance in this document is provided "as is": Once published, the information within may not constitute the most up-to-date guidance or technical information. Accordingly, the document does not, and is not intended to, constitute compliance or legal advice. Readers should confer with their respective advisors and subject matter experts to obtain advice based on their individual circumstances. In no event shall the United States Government be liable for any damages arising in any way out of the use of or reliance on this guidance.

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes. All trademarks are the property of their respective owners.

PURPOSE

The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) developed this document in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity recommendations and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

CONTACT

Client Requirements/Inquiries: Enduring Security Framework nsaesf@cyber.nsa.gov.

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov

Contents

Executive Summary

Since the introduction of multi-user computer systems, user authentication has primarily relied on the use of usernames and passwords. To strengthen the authentication process, Multi-Factor Authentication (MFA) requires the user to present multiple elements in different categories, or "factors", as part of an authentication attempt. These factors are something you have, something you know, and something you are. Similarly, Single Sign-On (SSO) provides a risk mitigation capability by centralizing the management and control of authentication and access across multiple systems and from multiple identity providers. Implemented properly, it can raise the authentication assurance level required for initial sign on and can control and secure the authentication and authorization information passed between systems.

Following on the work the Enduring Security Framework (ESF) published on identity and access management (IAM) best practices for administrators, targeted for administrators to make the best use of existing solutions, a working panel staffed by subject matter experts from both government and industry was tasked with assessing developer and vendor challenges relating to IAM. The working panel specifically identified the adoption and secure employment of MFA and SSO technologies as a key developer and vendor challenge that has been difficult to meet with the technology that is currently available.

Introduction

Successful implementation of IAM in an organization involves both technology and processes; successful implementation of *secure* IAM capabilities depends on the vendor community to provide solutions to achieve secure outcomes. One key factor the vendor community must be cognizant of is the interoperability of IAM solutions since no single vendor can solve all IAM challenges an organization may face. Only by working together can these solutions enable successful and secure outcomes. IAM solutions must enable an organization's staff to distinguish legitimate users conducting the organization's mission from unauthorized entities attempting to access the infrastructure while also support a timely and effective response to indicators of compromise. Malicious actors are opportunistic and will attempt to impersonate, influence, or exploit legitimate entities to make this distinction harder, and they will take advantage of gaps in the ability to manage the entities and their accesses.

This document focuses on technical gaps and challenges related to adoption and secure employment of MFA and SSO technology. The expectation is to enable developers and integrators to refine their existing tools to address the gaps and, if necessary, develop new tools to address the challenges for their products and solutions. Further, this paper also touches on, to some degree, key non-technical challenges such as cost, staffing, and user experience impacts of employing these technologies.

Scope

While the working group recognizes the broad scope of the challenges relating to MFA and SSO, this paper specifically addresses challenges that are informed by an understanding of threats in the IAM space that are actively being exploited by adversaries. This paper is targeted at the challenges facing sophisticated organizations with substantial resources and high-end adversaries, though it also touches on some challenges (e.g., cost or ease of implementation) that inhibit less sophisticated organizations defending against more rudimentary adversaries.

Key Challenges

Multi-Factor Authentication

MFA is widely recognized as one, if not the most, important preventative security controls available today. It provides a strong defense against various adversarial attack techniques such as password spraying[1], compromised password reuse[2], and—in some instances—phishing[3]. However, a key challenge is that it is notoriously difficult to deploy and many organizations, small and large, still have not done so even if they recognize the value. In this section, we will focus on three types of challenges related to MFA implementation: definitional and policy challenges in the vendor community, deployment and adoption related challenges, and sustainment and governance related challenges.

MFA Definitional and Policy Challenges

MFA deployment is notoriously difficult for many organizations. One reason is due to confusing definitions and unclear policy around different variations of MFA. Indeed, organizations often turn to forms of MFA believed to be easy to deploy, such as those based on short messaging service (SMS), without careful evaluation of the relative security differences between MFA options. There is a need for clarity, interoperability, and standardization amongst MFA variations to allow organizations to make value comparisons and to integrate these solutions into their environment. This starts with basic steps such as using common terminology; terms like “2-step verification”, “two-factor authentication”, and “multi-factor authentication” are all widely used to describe similar capabilities. Although in some cases there are subtle technical differences between various market terms, the confusion on terminology across the vendor community makes it difficult to articulate best practices for organizations to follow. Furthermore, organizations with a desire, or mandate, for MFA often don’t know what types of authentication mechanisms are available in a particular identity solution, if the MFA solution is compatible with their existing systems, or if potential new IAM solutions are compatible with the MFA they already have. It is incumbent upon the IAM vendor community to work together to agree on terminology standardization when discussing MFA to avoid confusion amongst

[1] https://www.splunk.com/en_us/blog/learn/password-spraying.html.
[2] https://www.keepersecurity.com/blog/2023/05/08/2fa-vs-mfa-whats-the-difference/.
[3] https://www.crowdstrike.com/cybersecurity-101/phishing/.

organizations making the decision to implement MFA within their respective. An architectures' related problem is that generic vendor terminology such as 'push notification' does not map cleanly to technical security properties such as those articulated by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63,[4] *Digital Identity Guidelines*. In the context of government systems, self-validation instructions are being developed by federal Identity, Credential, and Access Management (ICAM) groups.[5] However, vendors have not yet consistently documented the mapping of their products to NIST requirements and organizations have little evidence on which to evaluate the mappings that vendors do produce.

A second problem impeding adoption of MFA is the lack of clarity regarding the security properties that certain implementations provide. In SP 800-63, NIST articulates a set of "Authenticator Assurance Levels" (AALs) as one way of classifying the relative strength of authenticators based on the security properties that they provide.[6] According to NIST, MFA is required at "AAL2" and "AAL3". At its core, MFA seeks to address two classes of threat: those related to password reuse and compromise, and those related to adversarial use of phishing.

All forms of MFA provide some protection against password reuse and compromise, though with differing levels of security. For example, SMS-based MFA is vulnerable to a variety of attacks that may expose the one-time code to threat actors and is considered among the least secure MFA options. Other forms of MFA, using separate hardware storage (whether on a physically separate device or a separated embedded hardware module), are highly resistant to the extraction of the secret key. In addition to attacks related to password reuse and compromise, some forms of MFA are resistant to phishing attacks. For example, the more sophisticated phishing attacks, are capable of intercepting one-time codes in real time and relaying them to the system to which the user is attempting to authenticate. However, some types of MFA, such as those based on public key infrastructure (PKI) or FIDO2,[7] are resistant to such phishing attacks through the cryptographic binding of authentication to either the session with or identity of the system verifying the credential. Vendors have a real opportunity to lead the industry and build trust with product consumers with additional investments to bring such phishing-resistant authenticators to more use cases, as well as simplifying and further standardizing their adoption, including in form factors embedded into operating systems, would greatly enhance the market.

MFA Adoption Challenges

In addition to areas where vendors could aid in defining and articulating MFA security properties, vendors could also help advance other MFA deployment issues within large and

[4] https://pages.nist.gov/800-63-3/.
[5] https://www.cisa.gov/safecom/icam.
[6] The current version of SP 800-63 is Revision 3, although a draft of Revision 4 is out for public comment. A copy of Revision 4 can be found here: https://pages.nist.gov/800-63-4/.
[77] https://fidoalliance.org/fido2/.

complex organizations. One such issue is support for the strongest forms of MFA, such as those based on PKI and FIDO2 standards, in vendor products. Most IAM vendors offering SSO products support both PKI and FIDO2 authentication, but some do not. And even where such support exists, it is often incomplete. For example, PKI may not be treated as a "multifactor" authenticator within authentication policy because it is an authenticator that provides multiple "factors" due to the way its cryptographic keys are unlocked. Similarly, restrictions may exist on the types of FIDO2 authenticators that can be registered (e.g. those with exportable keys, those embedded in platforms, those using server side key storage) and the ability to define policy based on attestation may be lacking. Such enterprise features are critical to adoption. In the case of both FIDO2 and PKI, support on client platforms is also inconsistent. For example, iOS and Android phones/operating systems both support FIDO2 and PKI (enrolled through Mobile Device Management), but may not support all required security or protocol versions (e.g. device bound FIDO2 keys, key storage in embedded hardware modules, or external tokens). Additional vendor investment in supporting high assurance MFA implementations for enterprise use on both mobile and desktop platforms in a maximally user-friendly flow would substantially aid in MFA adoption by organizations of all sizes.

These same ease of use challenges also apply to configuring systems such as SSO providers to consume MFA. An often-bewildering list of options is available to be combined in complicated ways to support diverse requirements. Vendors could offer a set of pre-defined default configurations, that are pre-validated end to end for defined use cases. For example, a flow designed around the use of PKI and FIDO2 for maximum security or a flow defined around the use of mobile push applications with number matching for supporting business to business use cases from unknown platforms where stronger forms of MFA are not currently possible. Diverse requirements do require the ability to tweak detailed configuration options but offering safe and secure default paths that are well validated end to end is also critical.

MFA Sustainment and Governance Challenges

The final category of MFA related challenges addressed in this paper is governance and sustainment of MFA over time as employees join and leave the organization. All types of authentication credentials – including passwords – must be directly associated to user identities and their directory accounts. Robust management of this process, which is often called "credential lifecycle management", is often lacking in available MFA solutions. PKI-based MFA has a robust ecosystem of tools developed to register and issue PKI credentials, link them to accounts in a federated manner, and manage the revocation of credentials when they are either compromised or users are unenrolled, or both. However, many other types of MFA rely on user self-enrollment and some type of "one time enrollment code" flow which is itself a potential target of threat actors. Such flows often require the development of custom tools by organizations to align them with their business processes. The properties of these one-off flows vary widely and may be vulnerable to certain types of attacks that can compromise user credentials.

There is room for the IAM vendor community to develop more secure enrollment tooling to support the more complex provisioning needs of large organizations. For example, organizations may need to be able to enroll a user with an authenticator on one network while allowing them access to systems on a separate network. Along similar lines, tools for automatically discovering and purging enrolled MFA authenticators that have not been used in a particular period, or whose usage deviates from the expected behavior of a user, could be enhanced. Many of the approaches that are currently used to analyze user behavior to determine sign-on and account-level risk could be enhanced to better support governance of MFA authenticators. This is important because strong governance over MFA authenticator lifecycle enables higher trust to be placed in the use of MFA when it is employed.

For FIDO authenticators in particular, further enhancements are necessary to support attestation in the enterprise context. For example, the ability to determine that an authenticator was issued to a particular organization or person should be supported as a first-class capability in the market by IAM vendors. There is tension between FIDO's privacy preservation properties and the desire of enterprises to track and manage authenticator registration. Enterprise attestation and registration of FIDO tokens to SSO providers can provide a way to navigate this tradeoff, but further refinement of the flows and support in the ecosystem is required to reach the necessary enterprise experience.

SSO and Identity Federation

Identity Federation and SSO are critical security capabilities. By SSO, we mean a situation where an identity provider (IdP) within an organization authenticates a user and then conveys proof of that authentication to a series of applications – called relying parties (RPs) – typically without requiring the user to re-authenticate for each application. SSO is built on top of identity federation protocols such as security assertion markup language (SAML) or Open ID Connect (OIDC) that specify how authentication may be conveyed from the IdP to the RPs. These capabilities are critical for security because they make more advanced authentication, such as multi-factor authentication, or contextual authentication policies[8],a problem to be solved once within an organization rather than handled differently for each application. However, to do this, they concentrate risk into the IdP as the source of trust for authentication to a swath of applications. This trade-off is typically worth it due to the previously mentioned benefits, but vendors developing SSO technologies need to design their systems to the highest of security standards given their critical role in securing the enterprise. There are numerous challenges we have identified that could be addressed by IAM vendors as well as the vendors of RP systems. The following types of challenges will be addressed below: complexity and usability challenges, standards improvement opportunities, and ecosystem challenges.

[8] Contextual authentication policies factors in variables such as user behavior, device used, geographical location, and controls access based to determine access.

Complexity and Usability Challenges

First, there is still a significant tradeoff between functionality and complexity. Organizations can choose streamlined IdPs with simplified configurations that aren't able to support all the use cases that they may face, or they may deploy sophisticated tooling that requires significant numbers of highly skilled personnel to operate in a secure way. For many organizations, this is a difficult tradeoff that results in the deployment of SSO technology that is impossible to securely manage, undermining the security benefits of SSO. For example, it is critical to maintain the security of the key material used in identity federation protocols. Doing so may require the deployment of dedicated hardware security modules (HSM) and robust operational practices as well as significant amounts of skilled personnel to successfully integrate and sustain such systems. Choosing instead to store keys less securely (i.e. on disk) opens the door to adversaries compromising the keys and thus gaining access to systems across the enterprise. The growth of cloud-based identity tools delivered as software-as-a-service (SaaS) has eased the burden of deploying SSO significantly for organizations of various sizes, but such tools are not available to all market segments (e.g., operational technology (OT)) or OT networks in critical infrastructure. There is room for the development of a secure-by-default, easy to use, SSO system to address these gaps in the market. RP vendors could provide security configuration recommendations and their impacts. For example, the management of lifetime tokens such as ID tokens, Access Tokens, and Refresh Tokens should come with a reasonable secure default value which prevents wider abuse scenarios. It would allow the business to reduce the risk while providing a seamless user experience to restricted resources.

Second, tooling for understanding trust relationships and the impact to changes in the configuration could be improved. Changes to identity configurations often have organization-wide impact and thus need to be carefully controlled and managed. For example, a known threat vector for exploiting identity federation leverages compromising an on-premises IdP and pivoting to administrative accounts in the cloud that trust the on-premises IdP. Such identity federations are often set up unintentionally and could be automatically detected by IAM vendors by correlating data between the RP and the IdP. Similarly, identity federation protocols, such as SAML, support a variety of different configuration profiles. Some uses of SAML are known to be less secure than others. IAM vendors could aid in the detection of insecure implementations of these protocols and work with the ecosystem to build awareness around these issues as well as improve the adoption of the more secure uses of the standards.

Finally, there is the issue of ensuring SSO can enable secure MFA across all use cases, including privileged access use cases. As discussed above, the best path to MFA is through support in an SSO platform. Most SSO platforms in use today, both on-premises and in the cloud, support a variety of MFA options. However, there are often accounts that are not federated through SSO. For example, this is frequently true of high-level admin accounts as these accounts need to configure the setup of SSO itself in relying parties. Such accounts are attractive targets for threat actors and need to be protected with MFA. Some RPs support

the ability to configure the privileged roles for these high-level admins so that they trust separate, dedicated IdPs for "privileged access management" (PAM), however this capability is not particularly widespread in RPs. Other RPs natively support some level of MFA for administrative users, but the types of MFA options available varies and is rarely as complete as a dedicated SSO platform.

In the cloud context, key software as a service (SaaS) vendors should either organically support a spectrum of MFA options, including phishing resistant MFA options, for their administrative roles or should provide the ability to segregate trust (e.g. a separate federation configuration) for administrative roles. Furthermore, for any break glass accounts that are required to configure such trusts or not protected by MFA, RPs should ensure that these accounts can be protected with best practices, such as being vaulted and configured to alert on all usage.

Today, a commonly used pattern is to employ PAM tooling that effectively functions as a password vault (often with one-time use passwords) and a session monitoring tool. Users authenticate to such a tool via SSO and the tool mediates administrative access to platforms. Such solutions ultimately frequently rely on secrets shared between the PAM tools and the RP system, including long-lived secrets used to reset the passwords of administrative accounts. There is an opportunity for more robust privileged authentication flows that leverage modern federation protocols in a way avoids the need to maintain per-user passwords for administrative users. Wider support in the industry for such approaches would reduce the risk of privileged account compromise.

Standards Improvement Opportunities

Open standards are a critical part of the identity ecosystem, however, there is room for improvement. This paper focuses on several identity standards topics, but it is not meant to be a comprehensive list of such issues.

One example is that there is not yet a universally adopted standard for communicating the strength of MFA between IdPs and RPs. Current standards such as RFC 8176[9] do not cover all use cases and are not adopted by all vendors. Competing standards based on NIST SP 800-63 are also in use, as are proprietary implementations of these concepts. Standardization of these MFA types would aid in driving adoption of MFA in enterprise environments, especially in complicated use cases requiring different types of MFA strength for different user populations. Improvements in the terminology and understanding of the security properties of MFA, as discussed in the previous section, would aid in providing a basis for this type of standard.

[9] RFC 8176 - Authentication Method Reference Values RFC 8176 - Authentication Method Reference Values (ietf.org).

A second topic is around the standardization of federation configurations themselves. The OpenID foundations FastFederation (FastFed) standard specifies an approach to exchanging metadata required by identity federation protocols. Such standards are critical for simplifying and scaling the adoption of SSO technologies and should be supported broadly in the ecosystem. Their continued development and adoption is important to lower the burden to integrating SSO with applications and systems, thus enabling enhanced authentication.

Another issue around standards concerns the strength of identity federation assertions themselves. Many identity federation protocols use bearer assertions that are vulnerable to theft and replay. The validity of bearer assertions, which can be significant, can increase this risk. It is important that IAM vendors and RPs carefully consider issues such as assertion lifetime, assertion reuse, and assertion scope (e.g. issuer and audience) and provide tools for system owners to easily manage this risk. Furthermore, the use of identity federation protocols such as OAuth2 that leverage direct network "back channel" between the RP and the IdP rather than simply passing data through the user's browser (the "front channel") provides some security benefit by avoiding the exposure of a long-term credential to the user's browser. Broader support of back-channel federation protocols would thus enhance security. Similarly, efforts such as the IETF OAuth2 DPoP token binding work are important to reduce the risks associated with bearer tokens that can be stolen and be reused. Broad industry support for these efforts is important.

Finally, there are early-stage standards activities around sharing of within-session risk. These protocols (RISC and CAEP) enable identity providers and relying parties to exchange signaling around risk of particular sessions. Broad support for and development of these standards in the enterprise ecosystem will enable a variety of security use cases, ranging from limiting access to managed devices to quickly revoking access when accounts are compromised.

Ecosystem Challenges

Beyond complexity and standards, integration of SSO into the enterprise is still often difficult for a variety of reasons. For one, architectures designed for leveraging open standard based SSO together with legacy applications are not always widely understood. For example, in some organizations it is still difficult to integrate applications with an organizational IdP due to lack of talent or knowledge of architectural options (e.g. proxy, application server module, managed proxy service, etc.). Many organizations have developed robust practices for solving these challenges, but their work is not widely known outside of that organization. Community development by the IAM vendor ecosystem of a shared, open-source repository of open standards-based modules and patterns to solve these integration challenges would aid in adoption. Some vendors have created such repositories, but they are typically not widely embraced by multiple vendors and sometimes leverage proprietary integration points rather than open standards.

In addition to these capability gaps, there are several business practices in the market that merit attention. 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. This business practice deprives these organizations of the security benefits of MFA and other critical capabilities that come from adoption of SSO and is based on a flawed assumption that SSO is an "enterprise" feature. In today's market, SSO is a table stakes feature for organizations of all sizes and should be included in any pricing plans that are targeted at business customers, regardless of size. Along a similar vein, when SSO is supported, SAML is often the only supported protocol option. SAML has a number of security pitfalls and complexities that require careful configuration to avoid. For similar reasons, it is prone to implementation mistakes in RP applications. As discussed in the standards opportunities section, RP vendors should add support for OAuth2 and OIDC as an alternative federation protocol. OIDC was designed to fix several of the technical problems with SAML and broader support would aid in reducing security issues related to SAML misconfiguration or improper implementation.

Additionally, identity lifecycle management through open standards (e.g. SCIM) is still not viewed as a core part of the development of business software. Identity vendors often write custom integrations against proprietary APIs to manage the lifecycle of identities in RP systems, if such management is possible at all. Lifecycle management is a critical security capability. For example, it helps to implement the idea of least privilege and aids in detection of unexpected activity such as the creation of an account in a relying system that is not associated with a validated identity of the organization. SCIM and related standards should be adopted as table stakes by the RP ecosystem (both SaaS and on-premises software).

Conclusions

The challenges in the employment of MFA and SSO technologies in enterprise environments require further work by IAM vendors and further development of RP applications. These challenges span the spectrum from developing new product offerings to broadly adopting key ongoing standards activities. MFA and SSO are both critical security technologies that need to be adopted securely to address key threats all enterprises face, but doing so in a secure manner today is more difficult than in the past. Through public-private partnership, this situation can be improved, and the security of all organizations further enhanced.

Appendix I: Key Recommendations for Vendors

Key Challenge: 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[10].

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

Recommendation:

- 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 Challenge: The significant tradeoff between SSO functionality and complexity.

Recommendation:

- 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

[10] NIST SP 800-63: *Digital Identity Guidelines.*

Token should come with a reasonable secure default value which preventing 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: 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: 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: SSO capabilities are bundled with other high end enterprise features in such a way that makes the inaccessible to small and medium organizations.

Recommendation:

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