Multi-factor Authentication

By Dean H. Saxe (Amazon) and Khaled Zaky (Amazon)

Table of Contents

Abstract

Multi-factor authentication (MFA) is critical in securing account access and guarding against account takeover. In this article, we explain the core concepts that define MFA, explore the characteristics of different MFA types, and discuss the various threats mitigated by using MFA.

Introduction

This article describes multi-factor authentication (MFA), a key component in securing account access and guarding against account takeover. Organizations and individuals typically have multiple types of MFA and several strategies for implementing its use. Not all MFA offers the same level of security, and some types of MFA are generally not recommended.

Terminology

Many of these terms have been sourced from "Terminology in the IDPro Body of Knowledge." [i]

Term	Definition
Authentication	Authentication is the process of proving that the user with a digital identity who is requesting access is the rightful owner of that identity. Depending on the use case, an 'identity' may represent a human or a non-human entity; may be either individual or organizational; and may be verified in the real world to varying degrees, including not at all.
Authorization	Determining a user's rights to access functionality with a computer application and the level at which that access should be granted. In most cases, an 'authority' defines and grants access, but in some cases, access is granted because of inherent rights (like patient access to their own medical data). Authorization is evaluating what access or rights an identity should have in an environment.
Identity and Access Management	Identity and Access Management (IAM) is the discipline used to ensure the correct access is defined for the correct users to the correct resources for the correct reasons.
Identity Provider	An Identity Provider (IdP) performs a service that sends information about a user to an application. This information is typically held in a user store, so an identity provider will often take that information and transform it to be able to be passed to the service providers, AKA apps. The OASIS organization, responsible for the SAML specifications, defines an IdP as "A kind of SP that creates, maintains, and manages identity information for principals and provides principal authentication to other SPs within a federation, such as with web browser profiles."
Multi-Factor Authentication (MFA)	An approach whereby a user's identity is validated to the trust level required according to a security policy for a resource being accessed using more than one factor (something you know (e.g., password), something you have (e.g., smartphone), something you are (e.g., fingerprint).
MFA Prompt Bombing	Also known as MFA fatigue, MFA prompt bombing is a cyber-attack technique that describes when an attacker bombards a user with mobile-based push notifications, which sometimes leads to the user to

	approve the request out of annoyance which might lead to an account takeover.

What is Multi-factor Authentication?

MFA is an authentication mechanism that requires a user logging into an application or an online account to present two or more factors to sign in and complete their authentication flow. Traditionally this would have been just a username and a password combination or another form of single-factor authentication, such as fingerprint biometrics. Adding multiple factors reduces the likelihood of bad actors gaining unauthorized access in case any of the factors are compromised. For example, single factors, such as passwords (which are subject to reuse and compromise), are one of the most common ways malicious actors can gain unauthorized access to your accounts, data, and online assets. Adding additional factors reduces the risk of account compromise and raises authentication assurance. Check out the NIST 800-63-B, which provides recommendations on types of authentication processes, authenticator types, and various assurance levels.[ii]

There are three types of MFA factors:

- The knowledge factor is something you know. This factor could be something like a password or a PIN code.
- The possession factor is something you have. This factor could be something like a USB key, a smartphone, or an access card.
- The inherence factor is something you are. This factor could be a biometric, like facial recognition, fingerprint, or voice recognition.

What is the Difference between MFA and 2FA?

Two-factor authentication, or 2FA, is an identity and access management authentication method that requires exactly two factors of identification to gain access. It is worth mentioning that 2FA is sometimes referred to as two-step verification or 2SV in some online services. 2FA is usually used interchangeably with MFA. However, in the case of MFA, more than two factors can be required, such as a combination of password + one-time

password (OTP) + on a device with mobile device management (MDM). Therefore, 2FA is a subset of MFA.

History of Multi-factor Authentication

How did the industry come to embrace MFA? Although the original ideas and patents are up for debate, we can say that the concept of MFA was first commonly used with automated teller machines (ATMs, cash machines). First introduced in Europe in 1967, ATMs required a physical card containing information encoded on the magnetic stripe as the possession factor (something I have) and a PIN (something I know) to conduct bank transactions.[iii]

> *The breakthrough in security was the idea that a public number (PAN) was to be combined with a private identification number (PIN). The PAN was printed in punched holes on the card and of course, could be forged. It would be secured through the use of a PIN that would correspond to the PAN through a complex coding system. The key was that such system should be of sufficient strength to prevent anyone getting to the PIN from the PAN. Chubb tested the system by printing off 1001 cards and attempting to break this system. They failed and Goodfellow's system became the basis of the security system in the 'Chubb MD2' cash dispenser. Goodfellow's patent was filed on May 2, 1966 (GB1197183).*[iv]

In 1987, RSA introduced the first hardware key fob, enabling the use of one-time passwords (OTPs) as an authentication factor. These hardware key fobs are still in use today and sold by numerous vendors using both Time-based One Time Passwords (TOTP, see RFC6238)[v] and HMAC-Based One Time Passwords (HOTP, see RFC4226).[vi]

By the early 2000s, MFA solutions began to see a broad rollout in enterprise, government, and consumer use cases. In 2004 the United States Homeland Security Program Directive 12 (HSPD-12) was signed by President George W. Bush.

> *"US policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification."* [vii]

In response to HSPD-12, the US Federal Government, through the National Institute of Standards and Technology (NIST), released FIPS-201-1, specifying the requirements for Personal Identity Verification (PIV) for US Federal Government employees and contractors.[viii] NIST Special Publication 800-73-1[xi], released in March 2006, "specifies the

PIV data model, Application Programming Interface (API), and card interface requirements necessary [...] for interoperability across deployments or agencies. Interoperability is defined as the use of PIV identity credentials such that client-application programs, compliant card applications, and compliant integrated circuit cards (ICC) can be used interchangeably by all information processing systems across Federal agencies." [ix]

In December 2004, the US Federal Deposit Insurance Corporation (FDIC) released the paper "Putting an End to Account-Hijacking Identity Theft," which concluded with the recommendation for "upgrading existing password-based single-factor customer authentication systems to two-factor authentication."[x] Shortly after that, in 2005, the Federal Financial Institutions Examination Council released guidance for the US banking industry entitled "Authentication in an Internet Banking Environment," which stated, "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services."[xi] The requirements were not compulsory. In 2011, the RAND Corporation noted:

> *The financial sector is potentially the most varied in its implementation practices. Despite regulations (more like "guidelines") that require financial institutions to protect certain data to a certain minimum level and indicate that MFA meets these criteria, organizations in this sector make network access decisions internally.*[xii]

These changes did not arrive without debates about their value and consumer concerns about using MFA.[xiii] First deployed in Nigeria in 2005 by Neticash, SMS OTP was broadly adopted in the 2010s. At the same time, consumer use of OTPs became more common with readily available authenticator apps, such as Google Authenticator, becoming available for various smartphone devices.

The FIDO Alliance was founded in 2012 to develop a password-less authentication protocol and later, an open, second-factor protocol.[xiv] The World Wide Web Consortium (W3C) released the first WebAuthn specification in conjunction with FIDO Alliance Client to Authenticator Protocol (CTAP) in March 2019, enabling FIDO2 as a phishing-resistant authentication protocol across platforms, browsers, and devices.[xv] With the public release of passkeys by the FIDO Alliance, W3C, and commercial partners in 2022, the tools for strong, highly phishing-resistant authentication already exist in many consumer and enterprise devices such as laptops, tablets, and phones.[xvi]

Bruce Schneier wrote in 2005, "Two-factor authentication isn't our savior. It won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions. It solves the security problems we had ten years ago, not the security problems we have today."[xvii] Schneier's blog post was prescient. Even

after the broad rollout of MFA mechanisms starting in 2005, we are still fighting against phishing, fraud, and identity theft in the 2020s. As the industry has adapted to these ills, malicious actors have also adapted their mechanisms. As we close the front door with better technology, what new paths will actors take to achieve their nefarious goals?

Why Choose Multi-factor Authentication?

The key benefit of adopting MFA is that it improves individuals' and enterprises' security posture and delivers a higher level of assurance to guard against unauthorized account access. With MFA enforced, users are required to authenticate by presenting multiple factors, for example, a username, password, and fingerprint from their device. These additional factors reduce the risk of unauthorized access when one of the authentication factors is compromised, such as a leaked password through a third-party data breach or a phishing attack. You can think of every factor added as an additional lock as an access security layer to prevent unauthorized users from breaking in.

The Problem with Single-Factor Authentication

Single-factor authentication is when access is provided when a user presents one factor. This presentation could be in the form of a password, access card, or fingerprint biometric. The most common single-factor authentication mechanism is the password. Password-less mechanisms, such as passkeys, designed to replace passwords as an authentication factor, are expected to see broad consumer rollout after their introduction in 2022.

However, passwords are still the most widely used mechanism to authenticate to various online services. Passwords are vulnerable to various attack techniques commonly used by attackers to gain access to online accounts. Here are some examples of those techniques:

- **Identity Theft:** This is when an attacker illegally acquires personal information such as date of birth, credit card details, or even answers to security questions that could be used for password guessing or resets.
- **Phishing:** This is when an attacker falsely presents themselves as a trusted party through fraudulent emails, websites, or pop-ups, hoping that they collect someone's personal information, such as username/password.
- **Brute force:** This involves an attacker guessing username and password combinations in hopes that they would eventually gain unauthorized access to an account
- **Credential Stuffing:** This is when an attacker uses a list of known compromised passwords to take over someone's account.
- **Key-logging:** This requires an attacker to compromise the end-point like a public computer where they would have installed a key-logger to monitor and record

actual keystrokes for personal information such as login information and credit cards.
- **Man in the middle:** An attacker could use URLs that closely resemble the intended website. This deceptive URL is then used to direct the user to a reverse proxy server used by the attacker to intercept the communication between the user and the intended website in order to steal sensitive data, such as a user's password.

The introduction of passkeys presents an interesting dilemma: Are passkeys an MFA mechanism when they are syncable across cloud services? What about when they are resident on a single device? If passkeys are primarily designed as a single authentication factor to replace passwords, will we see passkeys deployed with additional factors? With varying security models depending on where the passkeys are generated and how they are stored, synced, and shared, we believe it is likely that some passkey implementations will require additional authentication factors. For additional passkey considerations, see the FIDO section below.

Multi-factor Authentication Mechanisms

Grid Cards & Grid-Based Mechanism

Possession Factor: Card
Knowledge Factor: Password
Inherence Factor: None
Phishing Resistance: None

A form of a challenge-response protocol, a unique grid with named columns and rows is printed on card stock, a plastic card (e.g., student ID), etc.[xviii] At each set of coordinates is a cell containing an alphanumeric value. Upon first factor authentication with a password, the user is presented with a dynamic challenge requiring entry of the values at multiple coordinates on the grid as a second factor.

Credential Calculators Hardware Token

Possession Factor: Credential Calculator
Knowledge Factor: Password
Inherence Factor: None
Phishing Resistance: None

In another form of challenge-response protocol, users authenticate to a service with a password and receive a numeric challenge. This challenge is entered into the device using

a keyboard, and the response is calculated. The user enters the output into the service to complete the authentication process.

One-Time Passwords - HOTP

Possession Factor: HOTP Generator
Knowledge Factor: PIN or Password
Inherence Factor: None
Phishing Resistance: None

Described by RFC 4226 as "An HMAC-based One Time Password Algorithm," HOTP is a commonly used second factor. Successive HOTP values are generated through the application of the HMAC-SHA1 algorithm, whose inputs are a static seed value, unique per device and shared with the server, and the counter, a numeric value that increments on each iteration. The output is truncated to a set of human-readable numbers, often 4-8 bytes in length.

Generally found on hardware devices with small display screens showing a set of numbers after pressing a button, the HOTP output is entered into a form field by the user to complete authentication. Of note with HOTP generation is that the codes are generated dynamically in response to a user action, such as a button press. This can lead to devices becoming out of sync with the server state when multiple HOTPs are generated by the client and unused. Desynchronization must be addressed through a re-synchronization process that is undefined by RFC.

One-Time Passwords - TOTP

Possession Factor: TOTP Generator
Knowledge Factor: PIN or Password
Inherence Factor: None

Similar to a HOTP, a TOTP is defined by RFC 6238 as a time-based one-time password algorithm. The RFC describes TOTPs as a "variant of the HOTP algorithm [that] specifies the calculation of a one-time password value, based on a representation of the counter as a time factor." Since the successive values are not generated in response to a user action, desynchronization is less of an issue with TOTPs vs. HOTPs, assuming the services are not subject to excessive clock-skew.

Similar to HOTP, TOTP is often implemented in hardware devices with a small display screen that is constantly refreshed over time, displaying 4 to 8 digits. Additionally, TOTPs are often implemented by software such as password managers, Authy, etc., as a convenient mechanism for users with smartphones to carry multiple TOTP generators for

different services on a device they already possess. In this case, the user will scan a QR code with their TOTP software application, instantiating the TOTP in the software. The user then enters the current TOTP into the relying party's service to validate the TOTP has been instantiated correctly. These TOTPs may exist on multiple devices, either through a cloud-based sync or re-scanning the QR code on multiple devices as a backup of the TOTP generator.

TOTP, like HOTP, was developed by the Initiative for Open Authentication, an industry group that developed the open specifications, which later became IETF RFCs. The standards developed by OATH enabled the creation of an ecosystem of hardware devices and software implementations, eliminating the need for context-specific second factors.

One-Time Passwords - SMS (Short Messaging Service)

Possession Factor: Access to SMS on a mobile device
Knowledge Factor: PIN or Password
Inherence Factor: None

SMS OTP allows a user to authenticate using a one-time password sent over to the user's mobile number using SMS. The user configures their phone number with a relying party to receive OTPs during authentication. As noted above, NIST-800-63rev3 identifies SMS OTP as a "restricted" authenticator.

> *"The use of a RESTRICTED authenticator requires that the implementing organization assess, understand, and accept the risks associated with that RESTRICTED authenticator and acknowledge that risk will likely increase over time. It is the responsibility of the organization to determine the level of acceptable risk for their system(s) and associated data and to define any methods for mitigating excessive risks. If at any time the organization determines that the risk to any party is unacceptable, then that authenticator SHALL NOT be used.*[xix]

> *Verifiers SHOULD consider risk indicators such as device swap, SIM change, number porting, or other abnormal behavior before using the PSTN to deliver an out-of-band authentication secret."*[xx]

One-Time Passwords - Email

Possession Factor: Email address (no physical possession)
Knowledge Factor: PIN or Password
Inherence Factor: None

Email OTP allows a user to user to authenticate using a one-time password sent over to a registered email address registered to the user's account. The user must provide the OTP value during the authentication ceremony. The security of email OTP is dependent upon the security of the user's email service.

One-Time Passwords – Magic Links

Possession Factor: Indeterminate
Knowledge Factor: Indeterminate
Inherence Factor: Indeterminate

Magic links provide a fast and easy sign-in user experience. Users are authenticated by providing their email address only; they are then sent an email with a link for the user to click and complete their sign-in. This link is an embedded token that can only be used once. This provides a password-less login experience, which has many user experience advantages. However, it is worth mentioning that magic links are only as secure as a user's email address. For example, if someone gets access to a user's inbox, they can now access the magic links as they get sent to the user, which might lead to an authorized access event. Therefore, we classify the possession, knowledge, and inherence factors are indeterminate – the security is dependent upon the authentication credentials to the email service and any devices which have persistent access to the same.

FIDO U2F / FIDO2

Possession Factor: *Devices such as a phone, tablet, laptop, or a FIDO hardware security key*
Knowledge Factor: PIN code (optional, may be used in place of an inherence factor)
Inherence Factor: *fingerprint, iris, or faceprint (optional, may be used in place of a PIN code)*

The FIDO protocols (U2F/CTAP1, CTAP2.x) and WebAuthn use asymmetric cryptography to authenticate users on external hardware devices (e.g., security keys) and platform authenticators built into laptops, tablets, and phones. Authentication credentials are scoped to origins controlled by the relying party; relying parties cannot discover credentials for unrelated origins to protect privacy.[xxi] The credentials may be bound to a single device, as with hardware keys and some platform authenticators, or synchronized across a cloud fabric, ensuring availability across the user's devices. FIDO credentials are considered to be highly phishing resistant.

Some FIDO credentials are attestable. At registration, the authenticator emits a signed attestation statement identifying the provenance of the authenticator. Relying parties can validate the signature on the attestation and collect additional authenticator metadata through the FIDO Metadata Service (MDS).[xxii] This data may include information about the authenticator's certification level and conformance to standards such as FIPS140-1.[xxiii]

Implementers should note that not all FIDO credentials are created equally. FIDO credentials may be created and managed entirely in software, within TPMs, Secure Enclaves, or other hardware embedded in general-purpose computers, phones, and tablets, or on hardware security keys. While all of these credentials use the same cryptographic primitives and protocols, relying parties should have an understanding of the differences between FIDO authentication mechanisms to help them make effective choices when implementing FIDO solutions.

- Passkeys are discoverable credentials that reside on the system that created them.
- Passkeys may be used as a highly phishing-resistant, single-factor credential, replacing passwords.
- The number of passkeys that can be configured on a single hardware security key is limited by the properties of the hardware and credentials.
- Passkeys created on hardware security keys do not leave the device.
- Passkeys may be synchronized across a fabric provided by platforms (Apple, Google, Microsoft) or password managers (1Password, Dashlane). Synchronization fabrics are provider-specific. Synchronized keys are sometimes called “multi-device credentials”. Non-synchronized keys are “single-device credentials”.
- Passkeys cannot be synchronized across providers.
- Synchronized credentials create an alternative credential recovery pathway. Credential recovery mechanisms are provider-specific.
- Passkeys may be shared by exporting them to nearby contacts through the AirDrop protocol on Apple platform devices.
- Passkeys, like all FIDO credentials, may not carry an attestation during registration. Relying parties may request attestation during credential registration. Authenticators and browsers may restrict whether an attestation is returned.
- In the event that a credential does not meet the relying party’s requirements, the RP must reject credential registration after the credential is created on the authenticator.
- Relying parties cannot be assured of the origin or security properties of unattested credentials. High-assurance use cases should require and validate all attestations.

The breadth of the FIDO2/WebAuthn ecosystem is too broad for this article. Look for a future BoK article on the FIDO protocols to address these protocols in more depth.

Push-Based Authentication

Possession Factor: *Access to the mobile device where the push notification is sent*
Knowledge Factor: PIN or Password (optional)
Inherence Factor: *Biometric on the device (optional)*

Push-based authentication is primarily a mobile-based experience. At authentication time, the service sends a push notification to the user's registered device(s) or applications. The user receives the notification and may approve or decline the request. As with most technologies, this has been abused by malicious actors who use social engineering or prompt bombing attacks to obtain the user's help to complete the authentication process.[xxiv] These attacks can be mitigated by providing additional context data to the user, such as the location of the authentication session or device identity, or requiring the user to copy a number from the push notification to the device attempting authentication.[xxv]

Smart Cards

Possession Factor: Smart Card
Knowledge Factor: PIN (optional, may use inherence factors)
Inherence Factor: Fingerprint (optional, may use PIN)

Smart Cards are physical devices of varying sizes (e.g., nano-SIM, SIM, credit card form factors) used to store a credential, often in the form of a cryptographic certificate, which can be unlocked by the user presenting a PIN or inherence factor to facilitate authentication. The card may be presented by insertion into a physical reader or via a contactless protocol, such as NFC.

Smart cards exist in a wide variety of formats with different use cases depending on the industry in which they are used. A common deployment is the use of a Common Access Card (CAC) by the US Federal Government. After identity proofing, the federal government issues a CAC to an individual as both a physical identity document used to access government property, as well as a multi-factor authenticator. Upon inserting the CAC into a reader, the user enters a PIN to unlock the device. Once unlocked, the CAC authenticates the user against a directory service via the public key certificate embedded in the hardware.

Threat Mitigation by MFA Mechanism

The NIST Special Publication 800-63B is a recommended read as it provides an informative section on the various threat and security considerations and how to mitigate them. In this section, we highlight a subset of threats against MFA mechanisms and whether the mechanism is susceptible to the threat (❌), partially mitigates the threat (~), or completely mitigates the threat (✅).

The threats considered below are:

- Credential duplication - Can the credential be duplicated and used in a manner undetectable to the owner? For example, a grid card could be photographed and used illicitly if the password was known, but the attack is not scalable.
- Eavesdropping / Man in the Middle - Active or passive eavesdropping of communications can compromise flows that depend on secrets, either by sniffing the secret off the wire as they are being delivered to the recipient (e.g., attacks on mobile SMS networks or SIM swapping), or by replaying secrets obtained through phishing.
- Replay - Some MFA mechanisms are designed for one-time use. Implementations may fail to enforce one-time use of these secrets, allowing sniffed secrets to be replayed.
- Social Engineering - Manipulating a target through psychological means such as authority, intimidation, urgency, and other mechanisms to force a victim to take actions that may not be in their own best interests. In the realm of MFA, this may be seen through attacks such as prompt bombing.
- Phishing - A form of social engineering where the victim is enticed into entering their credentials into a fraudulent site designed to look like a legitimate service. Phishers will collect credentials, including passwords and second factors, and use them immediately to authenticate to the legitimate site to further their schemes. In 2020, phishing was the most frequent crime reported to the FBI Internet Crime Complaint Center (IC3), representing almost one-third of all complaints (241,343 of 791,790).[xxvi]

Threats (--->)	**Credential Duplication**	**Eavesdropping / Man in the Middle / Replay**	**Phishing**	**Social Engineering**
Mechanisms (down)				
Grid Cards & Grid-Based Mechanism	✗	~	✗	✗
Credential Calculators Hardware Token	✗	~	✗	✗
One-Time Passwords - HOTP	~	~	✗	✗
One-Time Passwords - TOTP	✗	~	✗	✗

One-Time Passwords - SMS	N/A	~	✗	✗
One-Time Passwords - Email	N/A	~	✗	✗
FIDO U2F / FIDO2	~	✓	✓	✓
Push-Based Authentication	N/A	✓	✓	~
Smart Cards	✓	✓	✓	✓

Conclusion

Using MFA is now considered an essential security best practice. It protects against many cyber threats, and the user experience has significantly improved since the early days of heavy hardware tokens. There is more to learn when it comes to deploying MFA in an environment; we suggest further exploring this space by reading Nishant Kaushik's "Designing MFA for Humans".[xxvii]

References

[i] "Terminology in the IDPro Body of Knowledge," IDPro Body of Knowledge, updated 30 September 2021, https://bok.idpro.org/article/id/41/.

[ii] Grassi, Paul A., James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, and Justin P. Richer, "NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology, U.S. Department of Commerce, updated 2 March 2022, https://doi.org/10.6028/NIST.SP.800-63b.

[iii] Bátiz-Lazo, Bernardo, "A Brief History of the ATM: How automation changed retail banking, an Object Lesson," The Atlantic, 26 March 2015, https://www.theatlantic.com/technology/archive/2015/03/a-brief-history-of-the-atm/388547/ (accessed 14 December 2022).

[iv] Batiz-Lazo, Bernardo and Reid, Robert J. K., "Evidence from the Patent Record on the Development of Cash Dispensing Technology," MPRA: Munich Personal RePEc Archive, University of Leicester, University of Leicester and University of Glasgow, 30 June 2008, https://mpra.ub.uni-muenchen.de/9461/1/MPRA_paper_9461.pdf (accessed 14 December 2022).

[v] M'Raihi, D., Machani, S., Pei, M., and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, DOI 10.17487/RFC6238, May 2011, <https://www.rfc-editor.org/info/rfc6238>.

[vi] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, DOI 10.17487/RFC4226, December 2005, <https://www.rfc-editor.org/info/rfc4226>.

[vii] U.S. Department of Homeland Security,"Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors," last updated 27 January

2022, https://www.dhs.gov/homeland-security-presidential-directive-12 (accessed 14 December 2022).

[viii] National Institute of Standards and Technology, "Personal Identity Verification (PIV) of Federal Employees and Contractors," Federal Information Processing Standard (FIPS) 201-1, March 2006, https://csrc.nist.gov/CSRC/media/Publications/fips/201/1/archive/2006-06-23/documents/FIPS-201-1-chng1.pdf. Please note version is for historical reference only; the current version of this publication is FIPS 201-3, published January 2022 and available at https://doi.org/10.6028/NIST.FIPS.201-3.

[ix] Dray, James, Scott Guthery, and Teresa Schwarzhoff, "NIST Special Publication 800-73-1: Interfaces for Personal Identity Verification," Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, March 2006, https://csrc.nist.gov/publications/detail/sp/800-73/1/archive/2006-03-15. Please note version is for historical reference only; the current version of this publication is NIST 800-73-4, published May 2015 and available at https://doi.org/10.6028/NIST.SP.800-73-4.

[x] U.S. Department of Justice, Office of Justice Programs, "Putting an End to Account-Hijacking Identity Theft," NCJ Number: 210758, December 2004, https://www.ojp.gov/ncjrs/virtual-library/abstracts/putting-end-account-hijacking-identity-theft (accessed 14 December 2022).

[xi] Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment," 2005, https://www.ffiec.gov/pdf/authentication_guidance.pdf (accessed 14 December 2022)

[xii] Libicki, Martin C., Edward Balkovich, Brian A. Jackson, Rena Rudavsky, Katharine Watkins Webb, "Influences on the Adoption of Multifactor Authentication," technical report, RAND Homeland Security and Defense Center, 2011, https://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR937.pdf (accessed 14 December 2022).

[xiii] "Banks to Use 2-factor Authentication by End of 2006," Slashdot forum discussion, 2005, https://it.slashdot.org/comments.pl?sid=165833&cid=13832042 (accessed 14 December 2022).

[xiv] FIDO Alliance, "History of FIDO Alliance," n.d., https://fidoalliance.org/overview/history/ (accessed 14 December 2022).

[xv] "Web Authentication: An API for accessing Public Key Credentials Level 1," W3C Recommendation, 4 March 2019, and "Client to Authenticator Protocol (CTAP)," FIDO Alliance, 21 June 2022, https://fidoalliance.org/specifications/download/.

[xvi] Passkey.dev website, W3C WebAuthn Community Adoption Group and the FIDO Alliance, https://passkeys.dev/ (accessed 14 December 2022).

[xvii] Schneier, Bruce, "The Failure of Two-Factor Authentication," Schneier on Security blog, March 2005, https://www.schneier.com/blog/archives/2005/03/the_failure_of.html (accessed 14 December 2022).

[xviii] Williams, Andy, "Grid-based two-factor authentication comes to campus cards," SecureIDNews, 25 September 2006, https://www.secureidnews.com/news-item/grid-based-two-factor-authentication-comes-to-campus-cards/# (accessed 14 December 2022).

[xix] NIST 800-63B Section 5.2.10 Restricted Authenticators.

[xx] NIST 800-63B Section 5.1.3.3 Authentication using the Public Switched Telephone Network.

[xxi] "Web Authentication: An API for accessing Public Key Credentials Level 2," W3C Recommendation, 8 April 2021, section 3. Dependencies, https://www.w3.org/TR/webauthn-2/#scope.

[xxii] FIDO Alliance Metadata Service, website, https://fidoalliance.org/metadata/ (accessed 14 December 2022).

[xxiii] FIDO Alliance Certified Authenticator Levels, website, https://fidoalliance.org/certification/authenticator-certification-levels/ (accessed 14 December 2022).
[xxiv] Goodin, Dan, "A Sinister Way to Beat Multifactor Authentication Is on the Rise," Ars Technica, 30 March 2022, https://www.wired.com/story/multifactor-authentication-prompt-bombing-on-the-rise/.
[xxv] Cybersecurity & Infrastructure Security Agency, "Implementing Number Matching in MFA Applications," October 2022, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf.
[xxvi] "Internet Crime Report 2020," Internet Crime Compliant Center, Federal Bureau of Investigation, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
[xxvii] Kaushik, N., (2020) “Designing MFA for Humans”, IDPro Body of Knowledge 1(3). doi: https://doi.org/10.55621/idpro.49.