NIST Update: Multi-Factor Authentication and SP 800-63 Digital Identity Guidelines

Federal Cybersecurity and Privacy Forum

February 15, 2022

David Temoshok

Discussions for Today

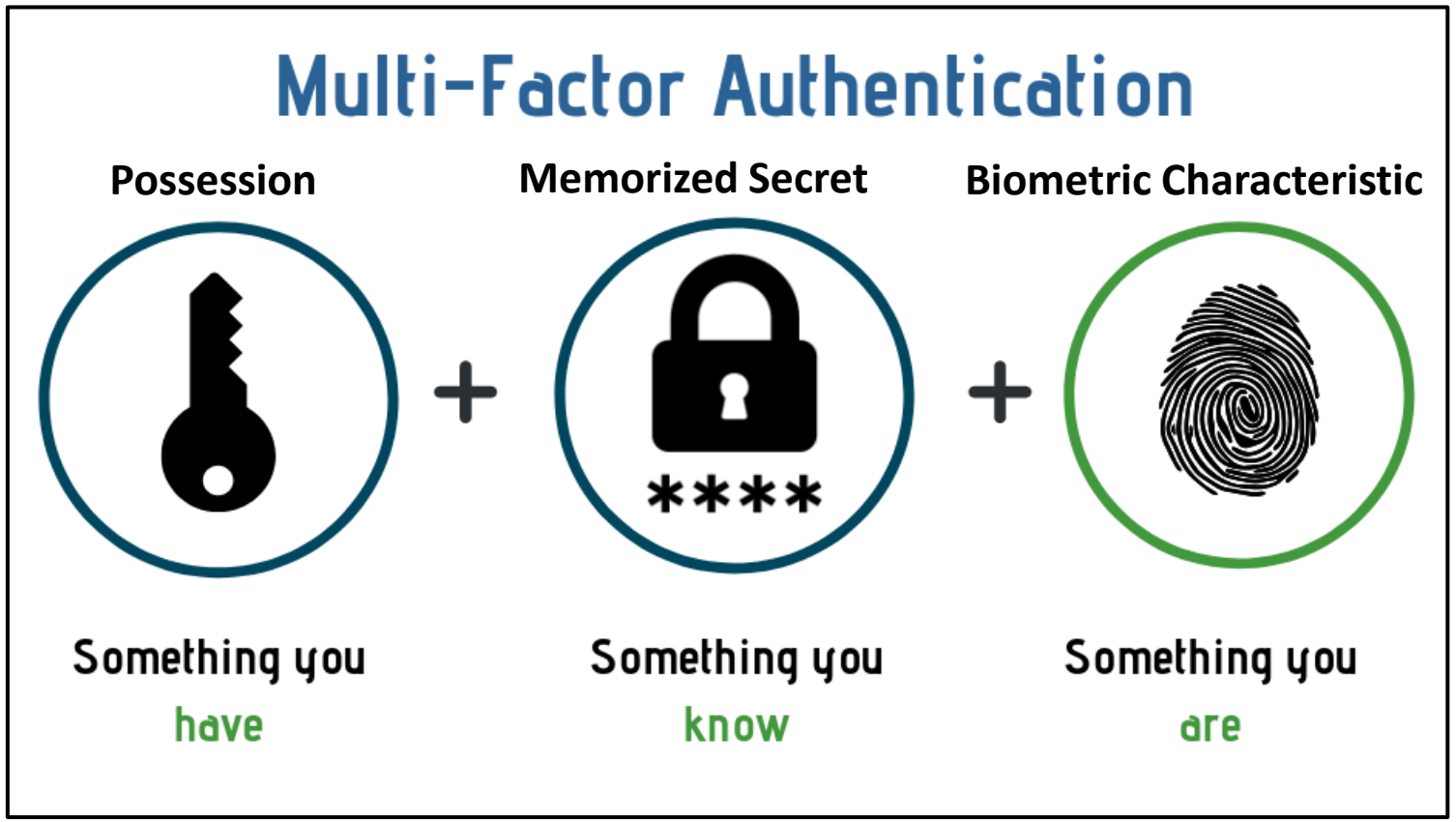
- Multi-factor Authentication Directives
- MFA Background
- Is all MFA Secure
- Phishing Attacks
- Phishing-Resistant MFA
- Phishing-Resistant MFA Example
- Biometric Authentication Factor
- Update and Considerations for SP 800-63-4

MFA Directives

- 10/14 **EO 13681** ***Improving the Security of Consumer Financial Transactions*** MFA required for access to digital applications containing personal information.
- 6/17 **NIST SP 800-63-3** ***Digital Identity Guidelines*****:** MFA required for AAL2/3 and access to any personal information. AAL2 recommends and AAL3 requires MFA to support verifier impersonation (phishing) resistance.
- 5/21 **EO 14028 Improving the Nation's Cybersecurity**: All US government agencies required to implement MFA.
- 1/22 **OMB M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles**: MFA required throughout the federal enterprise. Enterprise access must support phishing-resistant MFA, public access must offer phishing-resistant MFA.

Multi-factor Authentication

- Multi-factor authentication requires 2 or more authentication factors of different types for verification.
- Memorized secret or biometric + possession-based verification factor.



Authentication Factors

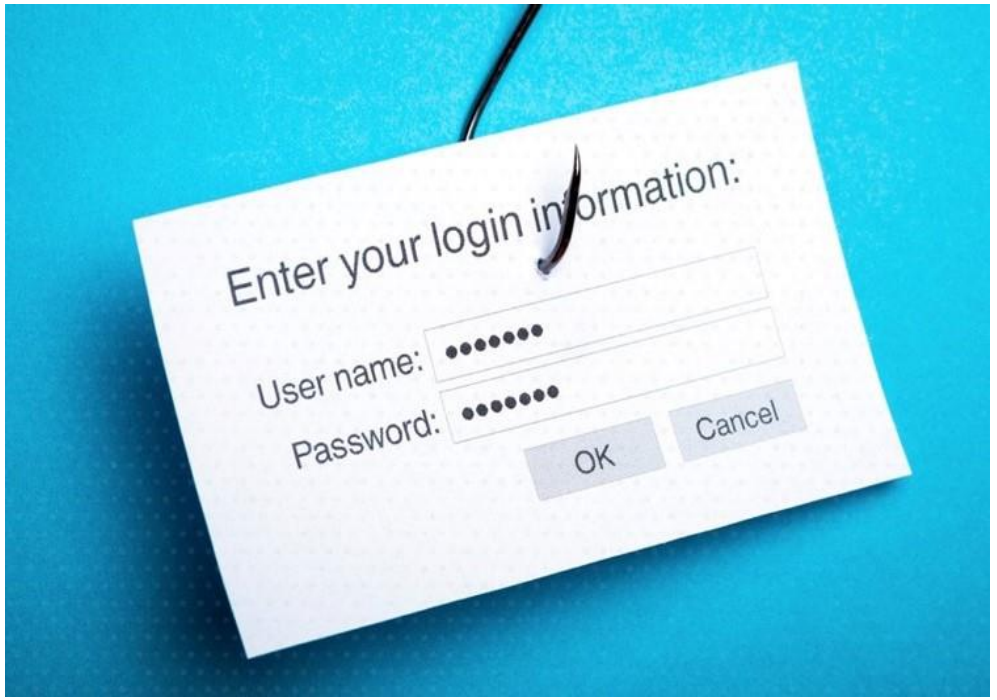
Is all MFA Secure

- All MFA is MUCH MORE SECURE than single-factor user ID + memorized secret.
- However, MFA using (unencrypted) SMS/PSTN is recognized to be vulnerable to attacks.
  - SP 800-63-3 cites these vulnerabilities and has RESTRICTED the use of SMS/PSTN.
- All MFA processes using shared secrets are vulnerable to phishing attacks.
  - Shared Secret authenticators: memorized secrets, look-up secrets, out-of-band authentication (SMS/PSTN) including push notification, one-time-passwords (OTP).
  - Shared secrets don't stay secret: Any MFA based on shared secrets can be phished.
- Strong MFA uses asymmetric key cryptography for protection from phishing attacks.
  - SP 800-63-3 calls these cryptographic authenticators: PIV/CAC cards, FIDO U2F authenticators, FIDO2/WebAuthN.

Basic MFA: Memorized secret (PW) + SMS/PSTN message, phone call
Better MFA: Memorized secret (PW) + push notification (app) or OTP SW/device
Best MFA: PW or Biometric + asymmetric key cryptographic authentication

Phishing Attacks

- The majority of all cyberattacks occur through stolen login credentials typically obtained through various forms of phishing attacks.
- Phishing attacks are often disguised as trusted senders of email or SMS messages or legitimate websites to trick the victim into entering sensitive information, present login credentials or to click on an attachment or URL to send the victim to a malicious imposter site.
- Stolen login and sensitive information are used by cybercriminals to take over the victim's accounts to impersonate the victim for financial and other fraudulent activities.
- Phishing attacks are becoming more sophisticated making it more difficult to distinguish from valid communications.



Phishing-Resistant MFA

- **OMB M-22-09:** Agencies must use strong MFA throughout their enterprise.
  - For agency staff, contractors, and partners, phishing-resistant MFA is required.
  - For public users, phishing-resistant MFA must be an option.
- **OMB M-22-09:** *"phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.*
- SP 800-63-3 uses the term "verifier impersonation resistance", term "phishing resistance" is planned for SP 800-63-4.
  - Verifier impersonation resistance is required for AAL3 and recommended for AAL2.
- Phishing resistant authentication requires PW or biometric + asymmetric key cryptographic processes (PIV, CAC, FIDO2).

Phishing-Resistant MFA Example

- Phishing-resistant MFA uses asymmetric key cryptographic authentication processes.
- These processes typically use cryptographic challenge-response protocols.

User authenticates locally to their device/API by PIN/PW or biometric

User/device authenticates to server through cryptographic authentication process

LOCAL

ONLINE

AUTHENTICATOR

SERVER

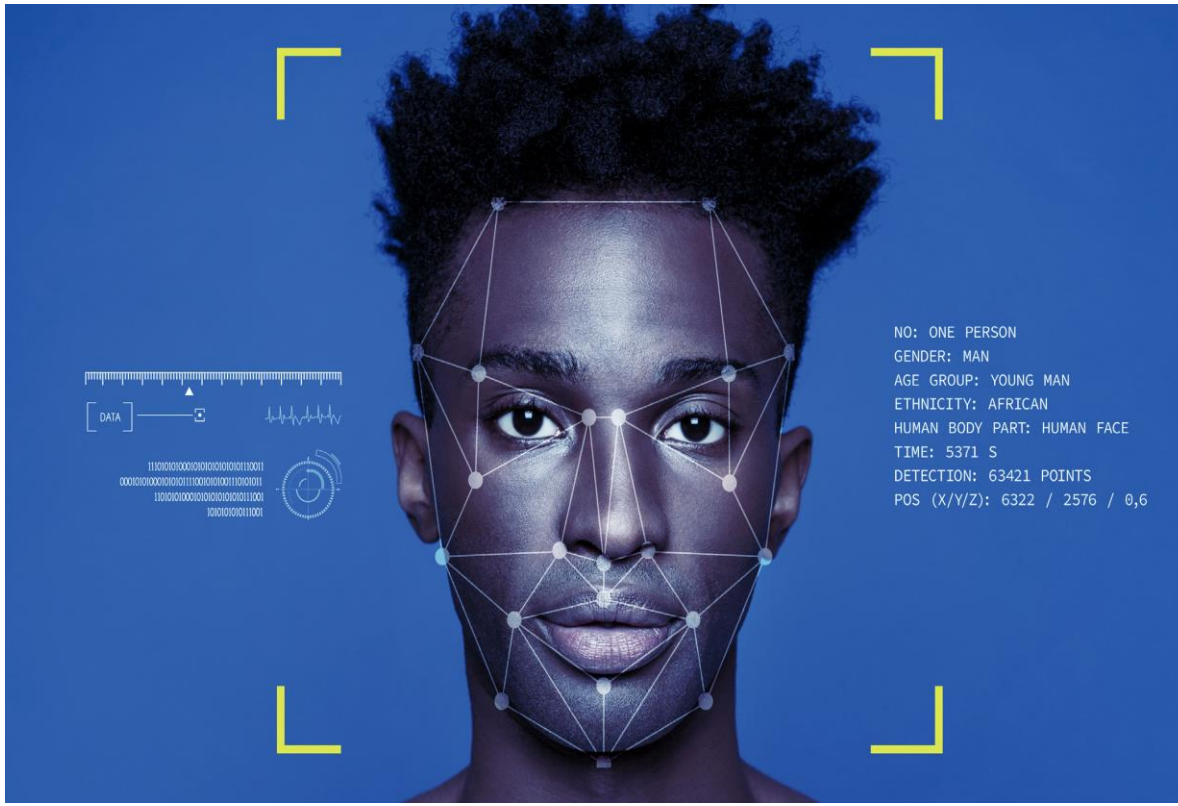
PIN/PW, Biometric

Device, Platform

Cryptographic Authentication Process

Biometric Factor for MFA

- Biometric characteristic comparison is a convenient and effective authentication factor for MFA.
- Biometric characteristics – something you are AND something you do (behavioral, voice pattern, gait).
- Biometric limitations: not a secret and cannot be used for SFA, cannot be revoked, biometric verification is probabilistic, biometric comparison algorithms vary in performance.
- Biometric facial image authentication in SP 800-63-3 is 1:1, not 1: N.



SP 800-63 rev. 4 Key Update Considerations

- 63: Update and simplification of assurance level selection decision trees.
- 63A: Identity Assurance Level 1 (IAL1) step up to provide identity proofing requirements for low-risk applications.
- 63A: Guidance for the strength characteristics, validation, and verification of digital identity evidence, such as mDL.
- 63A: Revision to sources for identity evidence validation to permit credible sources.
- 63B: AAL2 differentiation of non-phishing resistant MFA and strong (phishing resistant) MFA.
- 63C: Restructure of presentation of federation trust and federation registration and information connection models and update for FAL requirements and protections.

Look for draft SP 800-63 rev. 4 in the near future.

Questions/Comments?

David Temoshok

Senior Advisor

Applied Cybersecurity

NIST IT Laboratory

dig-comments@nist.gov