PRESENTED BY: EUMIR ARCEO & PRINCETON BROOKE


AGENDA
What is Multi-Factor Authentication (MFA)
Types of MFA Methods
Advantages and Disadvantages of MFA
MFA and the Reference Monitor (RM)

WHAT IS MULTI-FACTOR AUTHENTICATION (MFA)

- MFA is a cybersecurity best practice authentication method that requires a user to provide two or more pieces of evidence or authentication factors to confirm his/her identity before access is granted by a system or application.

- The goal of MFA is to minimize the risk of an adversary to successfully compromise a system's authentication process, and in turn gain unauthorized access into the system and its data.

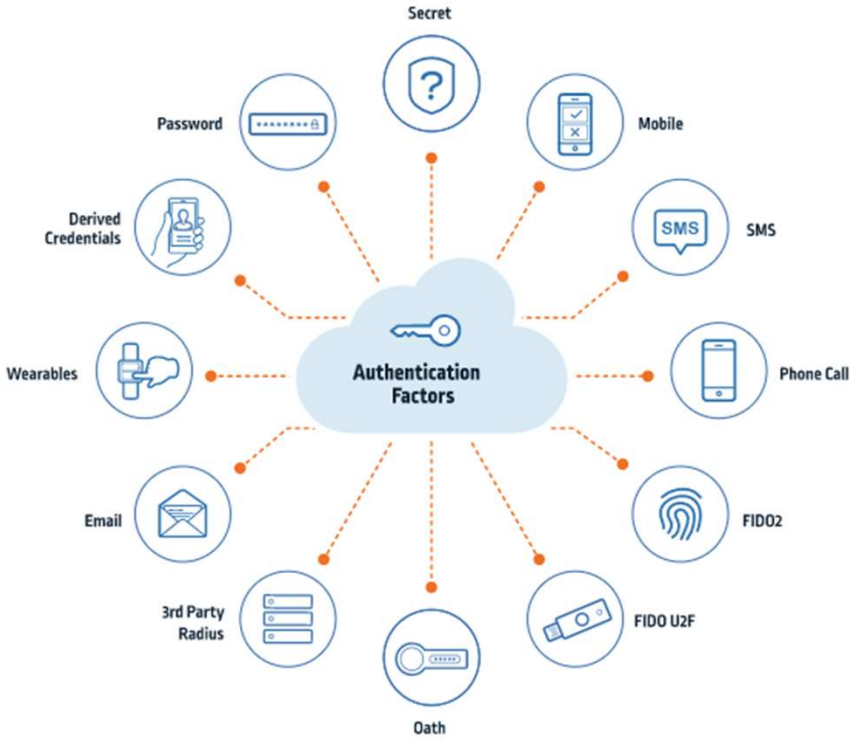
TYPES OF MFA METHODS

3 MOST COMMON MFA METHODS

1) **Something You Know:** Information only the user knows, such as username and password, a PIN or answer to a security question

1) **Something You Have:** Physical object the user has, such as a PKI card, security token, or a smartphone

1) **Something You Are:** Physical characteristics of a user (biometrics), such as a fingerprint, retina/iris scan, facial recognition, or voice authentication



ADVANTAGES AND DISADVANTAGES OF MFA

ADVANTAGES

- Adds an extra layer of security when authenticating in to a system
- Per NSA, MFA reduces security breaches by up to 90%
- Flexible implementation options to accommodate on-prem work, remote or hybrid
- Scalable, from low cost/simple to expensive/highly sophisticated MFA solutions to meet your business needs

DISADVANTAGES

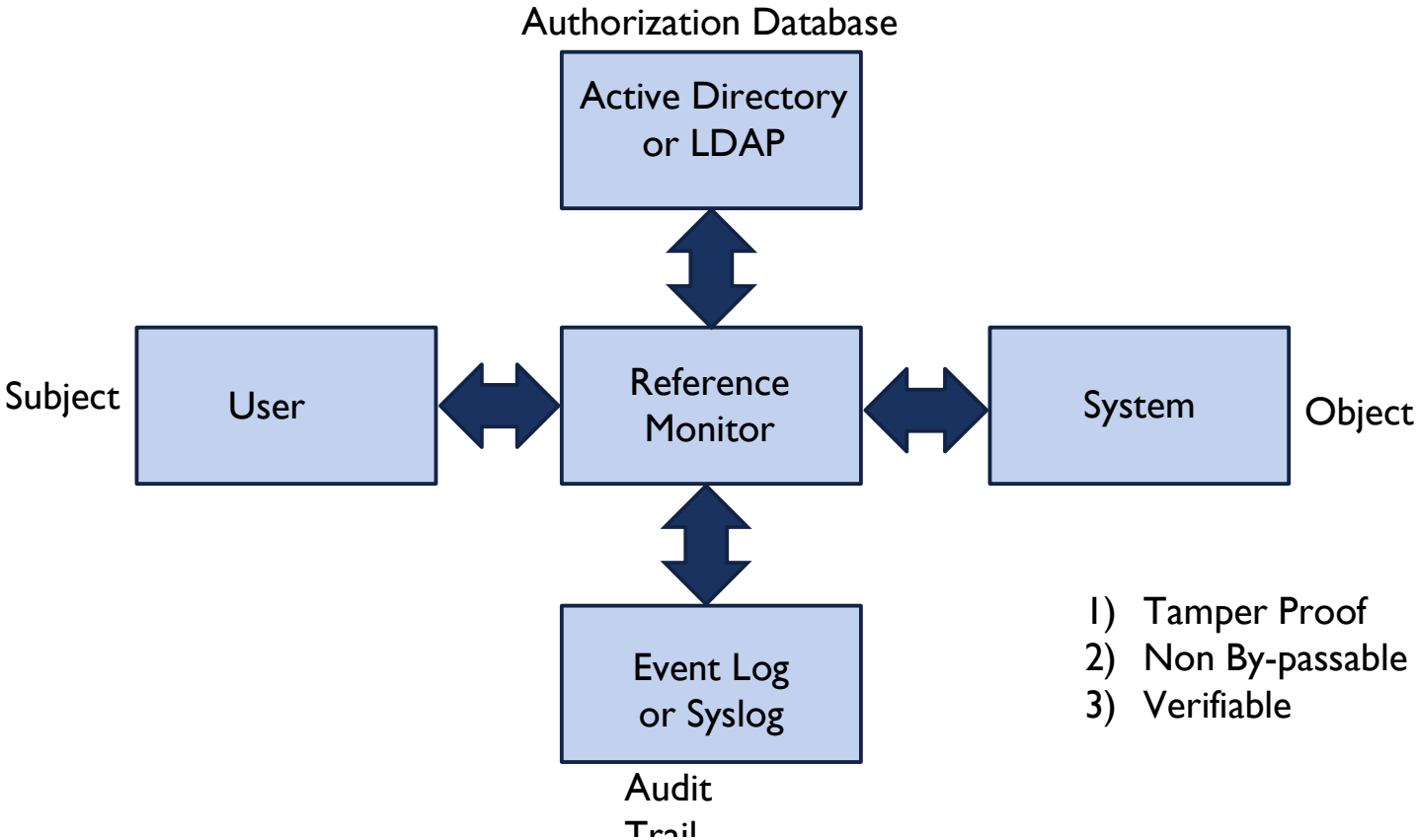
- Authentication devices (i.e., PKI card, USB token, cellphone) can get lost, misplaced or forgotten
- MFA can get burdensome for users
- MFA verification can fail due to other technology dependencies (e.g., cellphone outage, demagnetized cards, etc.)
- MFA techniques must constantly be upgraded to protect against evolving threats

ADVANTAGES AND DISADVANTAGES OF MFA – CONT.

THINGS TO CONSIDER BEFORE IMPLEMENTING MFA

- Create an MFA Policy that make sense for your company and that meets required compliance
- Educate/Train your users before/after MFA deployment
- Provide flexibility or alternative means to authenticate in case of lost/forgotten/defective authentication method
- Phase and monitor your deployment, and use audit tools to measure success/failure…make changes if needed

MFA AND THE REFERENCE MONITOR (RM)



MFA AND THE REFERENCE MONITOR (RM) – CONT.

1) Tamper Proof
   - Depending on what MFA technologies being implemented
   - Newer implementation of Biometrics combined with Dynamic Linking

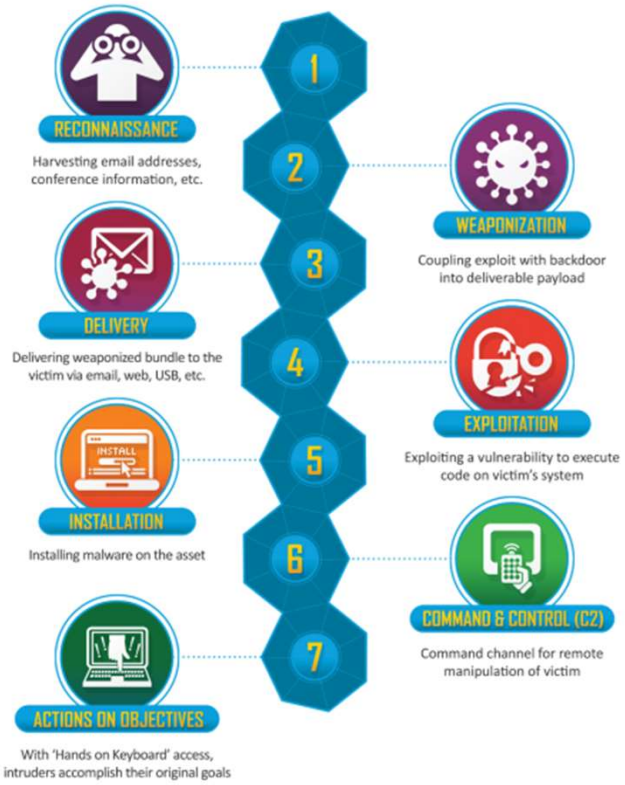
1) Non By-passable
   - Depending on what MFA technologies being implemented
   - OWASP Top 10 - SQL Injection

1) Verifiable
   - Depending on what MFA technologies being implemented
   - Fingerprint Technology - False Acceptance Rate (FAR)

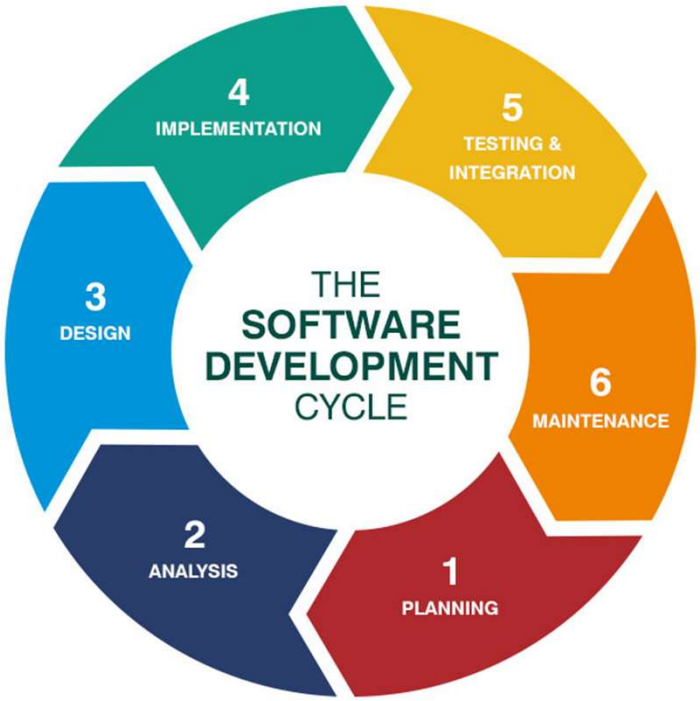
ANATOMY OF MFA ATTACK

Threats:

- Phishing.
- Push bombing, Push notification fatigue.
- Signal System 7 (SS7) vulnerabilities.
- Carrier SIM Swap.



MFA Implementations



MFA Forms of Implementation:

- COTS.
- Public key infrastructure PKI.
- One-time password OTP or Token.
- Push notification.
- Push notification number matching.
- SMS or Voice.

REFERENCES

1. https://www.nist.gov/back-basics-multi-factor-authentication
2. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA
3. https://www.microsoft.com/security/blog/2020/03/05/it-executives-prioritize-multi-factor-authentication-2020/
4. https://www.marshmma.com/us/insights/details/eight-things-to-consider-before-enabling-multi-factor-authentication-mfa.html
5. https://www.cyberark.com/products/multi-factor-authentication/
6. https://csrc.nist.gov/glossary/term/reference_monitor
7. https://www.cisa.gov/uscert/ncas/current-activity/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching

THANK YOU