LESSON NOTES

CYBERSECURITY

Domain 4.0 - Security Operations

4.6.2 - Multifactor Authentication (MFA)

Lesson Overview:

Students will:

- Investigate common methods to manage access.

Guiding Question: What are some common implementations of multifactor authentication?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

4.6 - Given a scenario, implement and maintain identity and access management

- Multifactor authentication
  - Implementations
    - Biometrics
    - Hard/soft authentication tokens
    - Security keys
  - Factors
    - Something you know
    - Something you have
    - Something you are
    - Somewhere you are

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Multifactor Authentication (MFA)

Multifactor Authentication (MFA) is a security process that requires users to provide two or more distinct forms of identification before granting access to a system, application, or service. MFA enhances security by adding additional layers of verification beyond traditional username and password authentication.

MFA provides an additional layer of security beyond passwords, reducing the risk of unauthorized access. Even if one factor (e.g., password) is compromised, the additional factors add a layer of protection, mitigating the impact of credential theft. MFA is often required by regulatory standards and compliance frameworks to ensure robust security practices. The use of multiple factors provides a higher level of assurance that the user accessing the system is legitimate. MFA can be ***implemented*** using various factors, allowing organizations to choose the combination that best suits their security requirements and user experience.

Biometrics involves using unique physical or behavioral characteristics to verify a user's identity. Common biometric factors include fingerprints, facial recognition, iris scans, and voice recognition. Biometrics provides a highly secure and personalized form of authentication.

Authentication tokens are physical or virtual devices that generate one-time passwords (OTPs) or codes. *Hard tokens* are physical devices, while ***soft tokens*** are typically software-based applications. Tokens provide an additional layer of authentication by requiring users to possess a physical or virtual device.

Security keys are physical devices that use cryptographic processes to authenticate users. They often support protocols like FIDO (Fast Identity Online) for secure authentication. Security keys enhance security by requiring the possession of a physical device and are commonly used in web-based authentication.

Something you know involves knowledge-based information that only the user should know, such as a password, PIN, or answers to specific security questions. Traditional passwords fall into this category, but MFA goes beyond this by incorporating additional factors.

Something you have involves possession of a physical or virtual item, such as an authentication token, smart card, or mobile device. Requires users to possess a tangible item in addition to knowledge-based authentication.

Something you are involves unique physical or behavioral characteristics inherent to an individual, such as fingerprints, facial features, or voice patterns. Biometrics add a layer of authentication based on physiological or behavioral traits.

Somewhere you are involves verifying the user's location or presence at a specific place, often determined through geolocation or proximity to a predefined location. This is useful for ensuring that the user is accessing resources from an expected or authorized location.

Multifactor Authentication enhances security by requiring users to provide multiple forms of identification. Implementations include biometrics, authentication tokens, and security keys, while factors encompass knowledge-based information, possession of items, biometrics, and location-based verification. MFA is a key component of modern authentication strategies, offering stronger protection against unauthorized access.