Cybersecurity

Architecture and Design

2.4.1 Authentication Methods

What tools and technologies are used to guarantee the user is who they claim to be?

Overview
The student will summarize authentication and authorization design concepts.

Grade Level(s)
10, 11, 12

Cyber Connections

- **Threats & Vulnerabilities**
- **Networks & Internet**
- **Hardware & Software**

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).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 2.4

- Summarize authentication and authorization design concepts.
    - Authentication methods
        - Directory services
        - Federation
        - Attestation
        - Technologies
            - Time-based one-time password (TOTP)
            - HMAC-based one-time password (HOTP)
            - Short message service (SMS)
            - Token key
            - Static codes
            - Authentication applications
            - Push notifications
            - Phone call
        - Smart card authentication

Authentication Methods

Click Here to Prove You're Not a Robot

If someone wants to claim an identity, they need to prove said identity. This requires the process of authentication. Authentication protocols, servers, and standards are technologies used to guarantee the user is who they claim to be.

Directory Services

Directory services provide information about systems, users, and other information regarding an organization. Directory services, such as the Lightweight Directory Access Protocol (LDAP), are frequently deployed as part of an identity management infrastructure. These also offer hierarchically organized information about the organization.

Federated Logins

There may be services on an organization's network made available for as many people as possible, but rather than create separate usernames and

Teacher Notes:

passwords for each individual user on each service, the organization may opt for a ***single sign on*** (SSO) authentication scheme. This is accomplished using a ***federated network*** where the user authenticates with one organization and is granted authorized access to various other organizations. This is increasingly common with normal Internet browsing. Rather than create a new account for media outlets such as the Washington Post, users can opt to log in with their Amazon, Facebook, or Gmail account info. These rely on a formal trust process between these organizations. Typically, the password and account info is not shared between these organizations. Instead the third party validates the authentication and provides acknowledgement about the user back to the original, requesting source.

Attestation

Attestation is a mechanism for software to prove its identity. The goal is to prove to a remote party that your OS and application software are trustworthy. The verifier trusts that attestation data is accurate because it has been signed by a TPM, whose key is certified by the certificate authority. Remote attestation provides a centralized reporting function so that your systems can analyze changes in their systems over time. This works by having a remote device run an inventory of hardware and software then encrypt and digitally sign the info using the TPM that is in the device. Upon boot, the same check is performed to allow or deny the boot.

21st Century Technologies

For the Security+ exam, you'll need to be familiar with a handful of authentication and authorization technologies, both past and present. The list of technologies includes

- Time-Based One-Time Password (TOTP): As the name suggests, a TOTP requires that a password be used within a short period of time to provide identification once.
- HMAC-Based One-Time Password (HOTP): Similar to a TOTP, an HOTP can only be used once; however, there is no time limit requirement for using the password.
- Short Message Service (SMS): The user can be authenticated by entering a code sent via SMS message to the user's cell phone.
- Token Key: Tokens can be used like a TOTP, providing a one-time password with a short time limit

Teacher Notes:

- Static Codes: These are codes that change after a specific amount of time
- Authentication Applications: Applications like Kerberos can provide a "ticket" that can be exchanged for access to applications.
- Push Notifications: If access has been granted by an unknown device, an email is sent to the user.
- Phone Call: A user may receive a phone call if they access a system.

Smart Cards

A ***smart card*** is a plastic card with a built-in microprocessor, typically used for electronic processes. Smart cards can be used in a contact mode or as a contactless card. You should be familiar with a smart card if you have a credit card or debit card (the chip card), but smart cards can also be used to gain access to a computer for example. Usually, the physical card must be with you to use. The act of sliding it into a device provides authentication as well as a digital certificate. Smart cards could include an additional authentication factor like having to enter a PIN. Smart cards are a great way to physically identify the individual is who they claim to be (assuming they're the ones in possession of the smart card).