

Cybersecurity

Authentication Methods



Authentication

- Authentication
 - Proving you are who you say you are
- Directory services
 - Provide information about certain things:
 - Systems
 - Users
 - Other organizational information
 - Example: LDAP



Federated Logins

- Provide network access to others
 - Not just employees
 - Partners, suppliers, customers, etc.
- Third-parties can establish a federated network
 - Authenticate and authorize between the two organizations
 - Login with your Facebook credentials
- The third-parties must establish a trust relationship
 - And the degree of trust



Attestation

- Software proves identity
 - Prove to a remote party that your OS and application software are trustworthy
- Remote Attestation
 - Centralized reporting function so your systems can analyze changes in their systems over time
 - A remote device runs an inventory of hardware and software, then encrypts and digitally signs the info using the TPM that is in the device



Authentication Technologies

- Time-Based One-Time Password (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



Authentication Technologies

- 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.



Authentication Technologies

- Phone Call:
 - A user may receive a phone call if they access a system.
- Smart Card:
 - Can be plugged in or contactless
 - Multi-factored
 - Must have a pin or biometric with the card

