Module 7

IMPLEMENTING AUTHENTICATION CONTROLS
Topic 7A

SUMMARIZE AUTHENTICATION DESIGN CONCEPTS
2.4 Summarize authentication and authorization design concepts
IDENTITY AND ACCESS MANAGEMENT

Subjects
   Users or software that request access

Objects
   Resources such as networks, servers, and data

Identification
   Associating a valid subject with a computer/network account

Authentication
   Challenge to the subject to supply a credential to operate the account

Authorization
   Rights, permissions, or privileges assigned to the account

Accounting
   Auditing use of the account
AUTHENTICATION FACTORS

Something you know
  Knowledge factor
  Password
  Personal identification number (PIN)
  Swipe pattern
  Challenge questions/password reset

Something you have
  Ownership factor
  Hardware tokens and fobs

Something you are/do
  Biometric factor
AUTHENTICATION DESIGN

Meet requirements for confidentiality, integrity, and availability

Confidentiality
   Keep credentials secure

Integrity
   Threat actors cannot bypass or subvert the authentication mechanism

Availability
   The mechanism does not cause undue delay or support issues
Strong authentication requires two (or three) types:

- Knowledge factor only is weak in terms of confidentiality

Multifactor authentication (MFA)

Two-factor authentication (2FA)

- Something you KNOW and something you HAVE
- Something you KNOW and something you ARE
- NOT something you KNOW and something else you KNOW
AUTHENTICATION ATTRIBUTES

Somewhere you are
   Geolocation via location services
   IP location (logical versus geolocation)
   Switch port, virtual LAN (VLAN), or wireless network name

Something you can do
   Performing an action in a way that can be captured as a unique pattern

Something you exhibit
   A behavior or personality trait that can be captured as a unique pattern

Someone you know
   Web of trust
Topic 7B

IMPLEMENT KNOWLEDGE-BASED AUTHENTICATION
1.2 Given a scenario, analyze potential indicators to determine the type of attack
3.8 Given a scenario, implement authentication and authorization solutions
4.1 Given a scenario, use the appropriate tool to assess organizational security (Password crackers only)
LOCAL, NETWORK, AND REMOTE AUTHENTICATION

Authentication providers
  Passwords versus password hashes

Windows authentication
  Local sign-in
  Network sign-in (Kerberos and NTLM)
  Remote sign-in

Linux authentication
  /etc/passwd and /etc/shadow
  Pluggable authentication modules (PAMs)

Single sign-on (SSO)
Single sign-on authentication and authorization provider

Clients

Application servers

Key Distribution Center (KDC)
  - Authentication Service – Ticket Granting Ticket
  - Ticket Granting Service – Service Ticket
**Kerberos Authorization**

1. **Service Request**
   - User: user1
   - Pass: ************
   - Timestamp: 2020-03-01

2. **Presents Service Ticket**
   - User: user1
   - Pass: ************
   - Timestamp: 2020-03-01

3. **Mutual Authentication (optional)**

4. **Data Transfer**

---

Images 123rf.com.
Password authentication designed to work with remote access protocols (Point-to-Point Protocol)

Password Authentication Protocol (PAP)
- Completely unsecure

Challenge Handshake Authentication Protocol (CHAP)
- Challenge/Response similar to NTLM
- Challenge is repeated during the session to prevent replay
- Various implementations (Cisco, MS-CHAPv2)
- Not secure enough to use without an encrypted tunnel
PASSWORD ATTACKS

Plaintext/unencrypted
  Sniffing passwords from unsecure protocols
  Locating passwords in documents/code repositories

Online password attack
  Adversary interacts with authentication service
  Restrict logon rates
  Shun suspect hosts

Horizontal brute force/password spraying

Offline attacks
  Password database
  Hash transmitted directly
  Hash used as key to sign an HMAC
BRUTE FORCE AND DICTIONARY ATTACKS

Exploit weak user password selection or weak cryptographic mechanisms

Brute force attack
- Generate every possible combination to match a hash
- Large output space and sufficiently long input password increase time required

Dictionary attack and rainbow tables
- Use a dictionary to test common words or phrases first
- Rainbow tables assist dictionary attacks against Windows password databases by precomputing hash chains
- Using salt means hash chains cannot be pre-computed

Hybrid attack
- Dictionary and brute force
- Fuzzing of dictionary terms (james1, james2, tom1, tom2,...)
PASSWORD CRACKERS

Cain and L0phtcrack

Hashcat

Hash type

Dictionary/word lists

Brute force

Masked

Screenshot hashcat (hashcat.net/hashcat.)
Hardware and software solutions for storing and submitting multiple user passwords

Password key
  USB token
  Possibly Bluetooth/NFC connectivity

Password vaults
  Software-based

Federal Information Processing standard (FIPS 140-2)
Topic 7C

IMPLEMENT AUTHENTICATION TECHNOLOGIES
SYLLABUS OBJECTIVES COVERED

2.4 Summarize authentication and authorization design concepts
3.3 Given a scenario, implement secure network designs (HSM only)
3.8 Given a scenario, implement authentication and authorization solutions
SMART CARD AUTHENTICATION

Kerberos-based smart card logon

Card readers

Card stores user’s private key and certificate

Use of card is protected by a PIN
Provision keys with risk of insider threat reduced

Smart cards and USB keys

Trusted Platform Module (TPM)
  Virtual smart cards

Hardware Security Module (HSM)
  Provision keys to devices across the network
  Key archive and escrow
  Reduced attack surface and tamper-evident
  Cryptographically secure pseudorandom number generator (CSPRNG)
  Plug-in card and network rack form factors
EXTENSIBLE AUTHENTICATION PROTOCOL/IEEE 802.1X

Authenticate user at network access devices
  - Wireless networks
  - Port authentication for switched networks
  - Remote access over a virtual private network

Extensible Authentication Protocol (EAP)
  - Supports multiple authentication implementations
  - Certificates and smart cards

IEEE 802.1X Port-based Network Access Control
  - Supplicant
  - Network access server (NAS)
  - AAA server
REMOTE AUTHENTICATION DIAL-IN USER SERVICE

1. The RADIUS server and client are pre-configured with the same shared secret.

2. The supplicant connects to the network.

3. The NAP enables EAPoL and instructs the supplicant to authenticate.

4. The supplicant transmits EAP data.

5. The NAP encrypts the EAP data using the shared secret and forwards it to the RADIUS server.

6. The RADIUS server decrypts the packet using the shared secret and validates the credential.

7. The RADIUS server issues an Access-Accept.

8. The NAP decrypts the Access-Accept and opens the network channel for regular traffic.
TACACS+
Centralizing administrative logins for network appliances
Reliable TCP transport (over port 49)
Data encryption
Discrete authentication, authorization, and accounting functions
TOKEN KEYS AND STATIC CODES

One-time password (OTP)
  Generated by some algorithm and used only once
  RSA SecurID

Static code
  “Dumb” smart cards

Fast Identity Online (FIDO) Universal Second Factor (U2F)
OPEN AUTHENTICATION (OATH)

HMAC-based One-time Password Algorithm (HOTP)

Time-based One-time Password Algorithm (TOTP)
2-STEP VERIFICATION

Transmit a code via an out-of-band channel

- Short message service (SMS)
- Phone call
- Push notification
- Email account

Possibility of interception
Topic 7D

SUMMARIZE BIOMETRICS AUTHENTICATION CONCEPTS
2.4 Summarize authentication and authorization design concepts
BIOMETRIC AUTHENTICATION

Enrollment
  Sensor and feature extraction

Efficacy rates and considerations
  False Rejection Rate (FRR) or Type I error
  False Acceptance Rate (FAR) or Type II error
  Crossover Error Rate (CER)
  Throughput (speed)
  Failure to Enrol Rate (FER)
  Cost/implementation
  Privacy concerns
  Accessibility concerns
FINGERPRINT RECOGNITION

Fingerprint sensors
- Small capacitive cells
- Easy to implement
- Relatively simple enrollment
- Quite vulnerable to spoofing

Vein matching (vascular biometrics)
- More complex scanner

Android is a trademark of Google LLC.
FACIAL RECOGNITION

Facial recognition
- Enrollment can be relatively slow
- Privacy issues
- Prone to relatively high false acceptance/rejection rates/spoofing

Retinal scan
- Pattern of blood vessels
- Scanning relatively intrusive and complex

Iris scan
- Pattern of eye surface
- Easier to scan
- More vulnerable to spoofing
BEHAVIORAL TECHNOLOGIES

Something you do
  Voice recognition
  Gait analysis
  Signature recognition
  Typing

Other uses than authentication
  Identification/alerting
  Continuous authentication/account locking
Module 7

SUMMARY

Guidelines for implementing Authentication Controls

• Assess the design requirements for CIA given the context for the solution

• Determine whether an MFA is required and which method to use
  • Smart card, OTP keys/fobs or OTP authenticator applications
  • Biometric tech such as fingerprint, face, iris, retina, voice and vein
  • 2-step verification using SMS, phone call email or push
  • Vaults and USB keys/wireless fobs and such

• Select an appropriate authentication protocol or framework
  • Kerberos for sign-in to local networks with support for smart cards
  • 802.1X/EAP/Radius for authentication at a network access device with support for smartcard authentication or secure pwd transport
  • TACAS+ for administration of network appliances

• Assess risks from password attacks, especially when using legacy protocols and where hashes are exposed