

Lesson 7

Implementing Authentication Controls

Topic 7A

Summarize Authentication Design Concepts

Syllabus Objectives Covered

- 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



Screenshot used with permission from Microsoft.

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

Multifactor Authentication

- 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

Authentication Design Concepts



Review Activity

Topic 7B

Implement Knowledge-based Authentication

Syllabus Objectives Covered

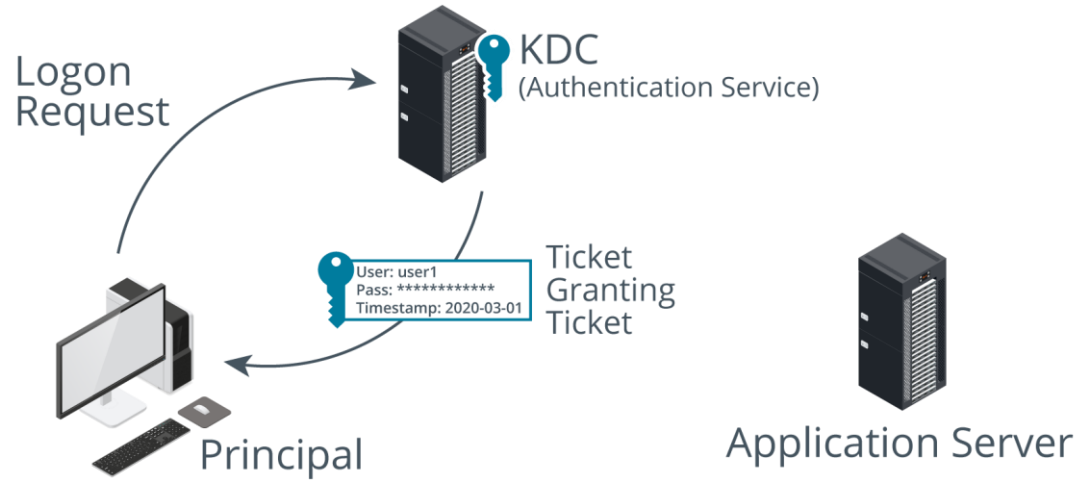
- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 3.8 Given a scenario, implement authentication and authorization solutions
- 4.1 Given a scenario, use the appropriate tool to assess organizational security (Password crackers only)

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)

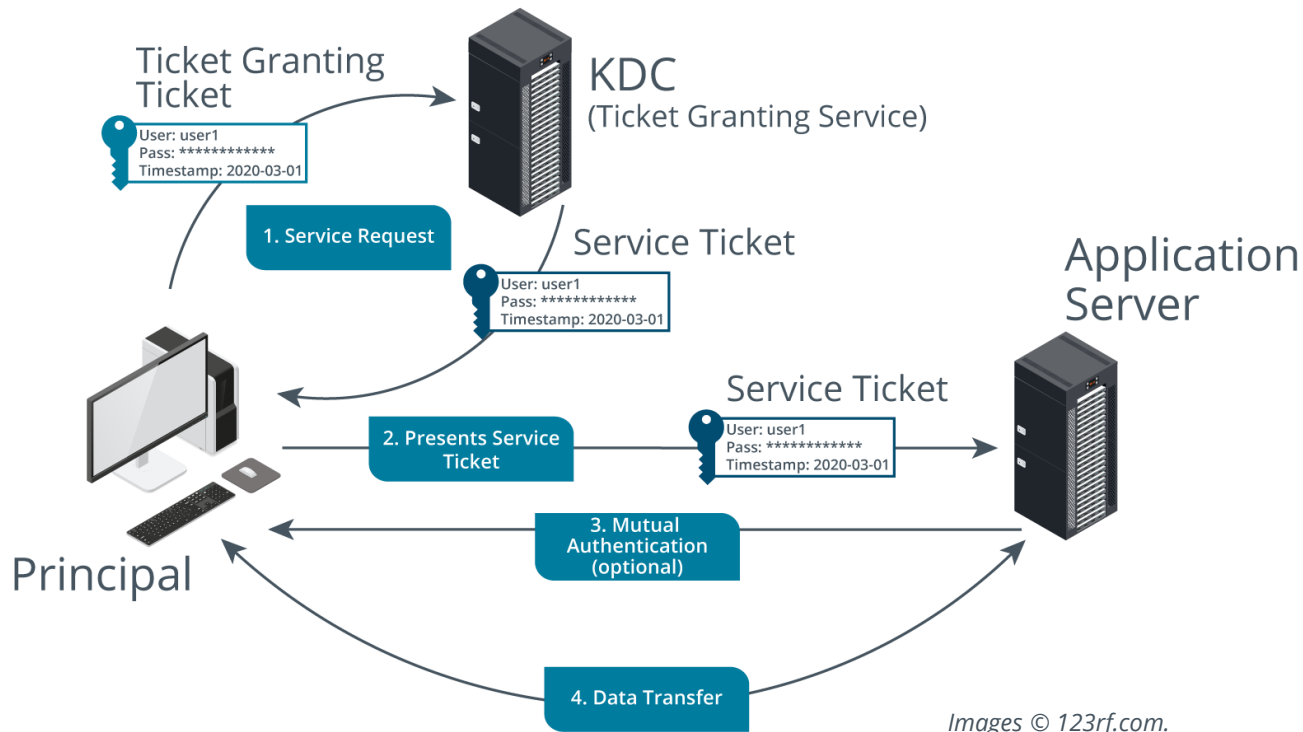
Kerberos Authentication

- Single sign-on authentication and authorization provider
- Clients
- Application servers
- Key Distribution Center (KDC)
 - Authentication Service – Ticket Granting Ticket
 - Ticket Granting Service – Service Ticket



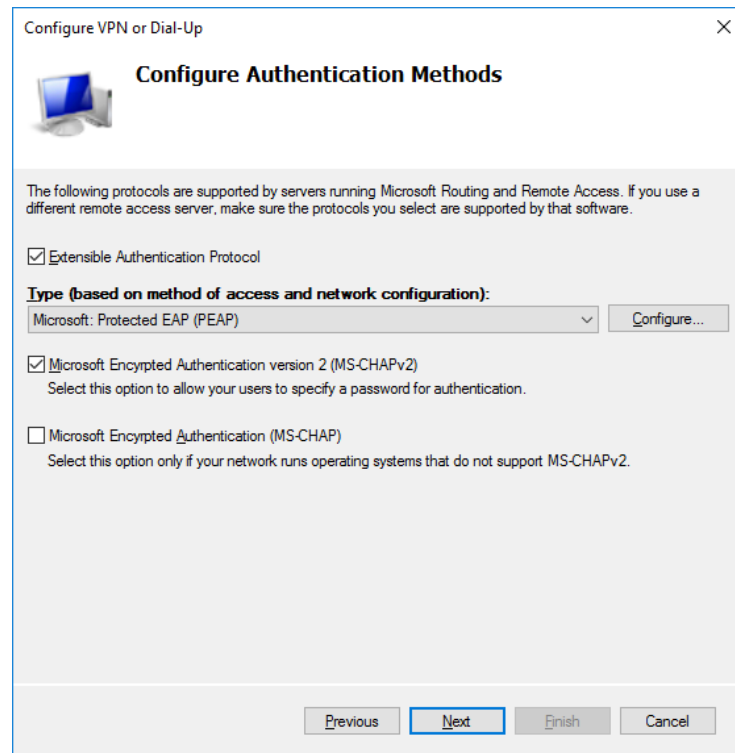
Images © 123rf.com.

Kerberos Authorization



PAP, CHAP, and MS-CHAP Authentication

- 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



Screenshot used with permission from Microsoft.

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

```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s
```

```
Session.....: hashcat
Status.....: Running
Hash.Type.....: NetNTLMv2
Hash.Target.....: ADMINISTRATOR::515support:2f8cbd19fd1bfac9:881c5503...000000
Time.Started.....: Mon Jan  6 11:25:16 2020 (1 min, 38 secs)
Time.Estimated...: Sat Jan 11 07:49:57 2020 (4 days, 20 hours)
Guess.Mask.....: ?1?1?1?1?1?1?1?1 [8]
Guess.Charset....: -1 pPaAsSwWoOrRdD0123456789$, -2 Undefined, -3 Undefined, -4
Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....:   364.1 kH/s (11.09ms) @ Accel:128 Loops:32 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 34233472/152587890625 (0.02%)
Rejected.....: 0/34233472 (0.00%)
Restore.Point....: 2176/9765625 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:1824-1856 Iteration:0-32
Candidates.#1...: $87r8678 -> dSDoRS12
Screenshot hashcat (hashcat.net/hashcat.)
```

- Cain and L0phtcrack
- Hashcat
 - Hash type
 - Attack mode
 - Dictionary/word lists
 - Brute force
 - Masked

Authentication Management

- 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)

Knowledge-Based Authentication



Review Activity

Assisted Lab

- Auditing Passwords with a Password Cracking Utility



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



Image © 123RF.com.

- Kerberos-based smart card logon
- Card readers
- Card stores user's private key and certificate
- Use of card is protected by a PIN

Key Management Devices

- 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

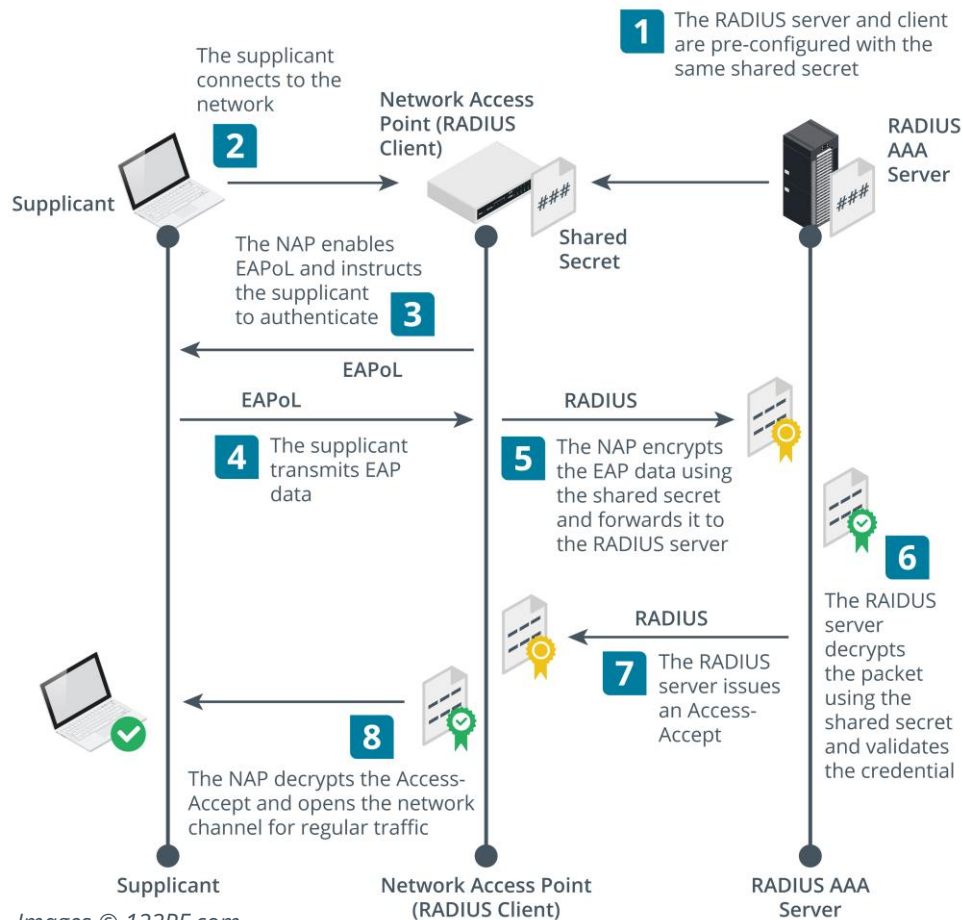


Images © 123RF.com.

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



Terminal Access Controller Access-Control System

- 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

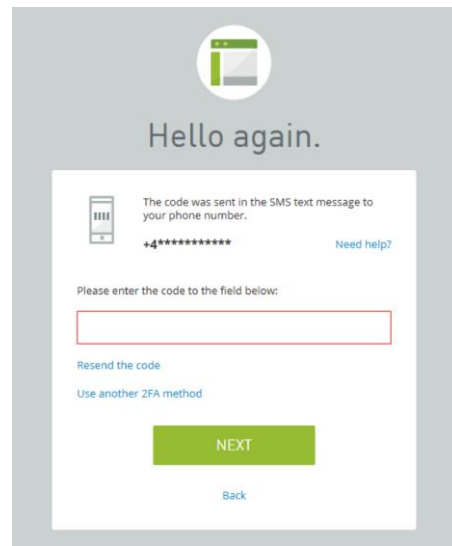
- One-time password (OTP)
 - Generated by some algorithm and used only once
 - RSA SecurID
- Static code
 - “Dumb” smart cards
- Fast Identity Online (FIDO) Universal Second Factor (U2F)



Image © 123RF.com.

Open Authentication (OATH)

- HMAC-based One-time Password Algorithm (HOTP)
- Time-based One-time Password Algorithm (TOTP)



The screenshot shows a mobile application interface for authentication. At the top, there is a circular icon with a green and white design. Below it, the text "Hello again." is displayed. The main content area is a white card with a light gray border. Inside the card, there is a small icon of a smartphone on the left. To its right, the text reads: "The code was sent in the SMS text message to your phone number." Below this text is a phone number starting with "+4" followed by asterisks. To the right of the phone number is a link that says "Need help?". Below the phone number, the text "Please enter the code to the field below:" is displayed. Underneath this text is a red-outlined rectangular input field. Below the input field are two links: "Resend the code" and "Use another 2FA method". At the bottom of the card is a large green button with the text "NEXT" in white. Below the card, there is a "Back" link.

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

Authentication Technologies



Review Activity

Assisted Lab

- Managing Centralized Authentication



Topic 7D

Summarize Biometrics Authentication Concepts

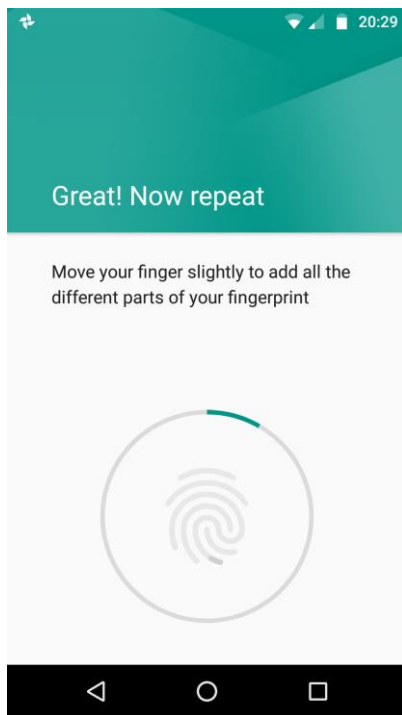
Syllabus Objectives Covered

- 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 Enroll 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

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

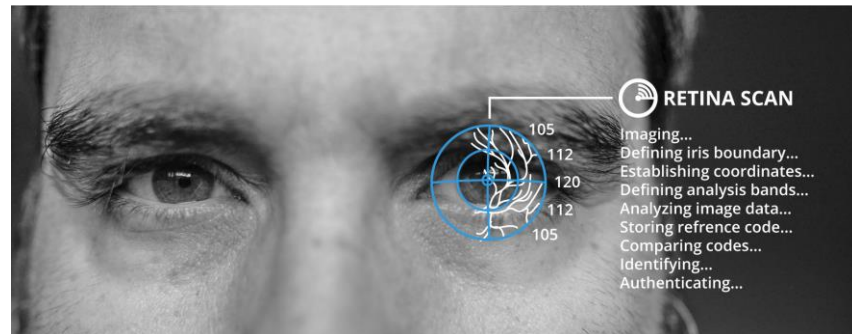


Photo by Ghost Presenter on Unsplash.

Behavioral Technologies

- Something you do
 - Voice recognition
 - Gait analysis
 - Signature recognition
 - Typing
- Other uses than authentication
 - Identification/alerting
 - Continuous authentication/account locking

Biometrics Authentication Concepts



Lesson 7

Summary

