2022

Class #8 – Domain 5

Ron Woerner

Cyber-AAA Founder & CEO & vCISO
Bellevue University CyberSecurity Studies Professor

WELCOME BACK!

- How ya doing?
- By now, you should have made (at least) your first pass through chapters 1-4.
- If you have questions about any of the content so far, check out the Slack study group or reach out!

Only 138 slides tonight, and we'll finish Chapter / Domain 6, all in one night!

CISSP® MENTOR PROGRAM – SESSION FOUR

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's pr[illegible] Tube is for constructive, respectful[illegible] nt) discussion **ONLY**.
- At **NO TIME** is the online chat[illegible] ctful, offensive, obscene, indecent,
- Please do not comment abou[illegible] e **NO DISCUSSION OF POLITICS OR**
- Failure to abide by the rules r[illegible]
- **DO NOT share or post copywritten materials. (pdf of book)**

CISSP® MENTOR PROGRAM – SESSION TWO & FOUR

WHOAMI

Ron Woerner, CISSP, CISM

- Chief Security Officer, Cyber-AAA
- Cybersecurity Professor, Bellevue University

https://linktr.ee/cyberron

https://www.linkedin.com/in/ronwoerner/

@ronw123

Hackers Wanted
TEDx Omaha

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Slack Channels
- Exercise or get fresh air in between study sessions

Let's get going!

INTRODUCTION

Before we get too deep into this. Start with a "dad joke"

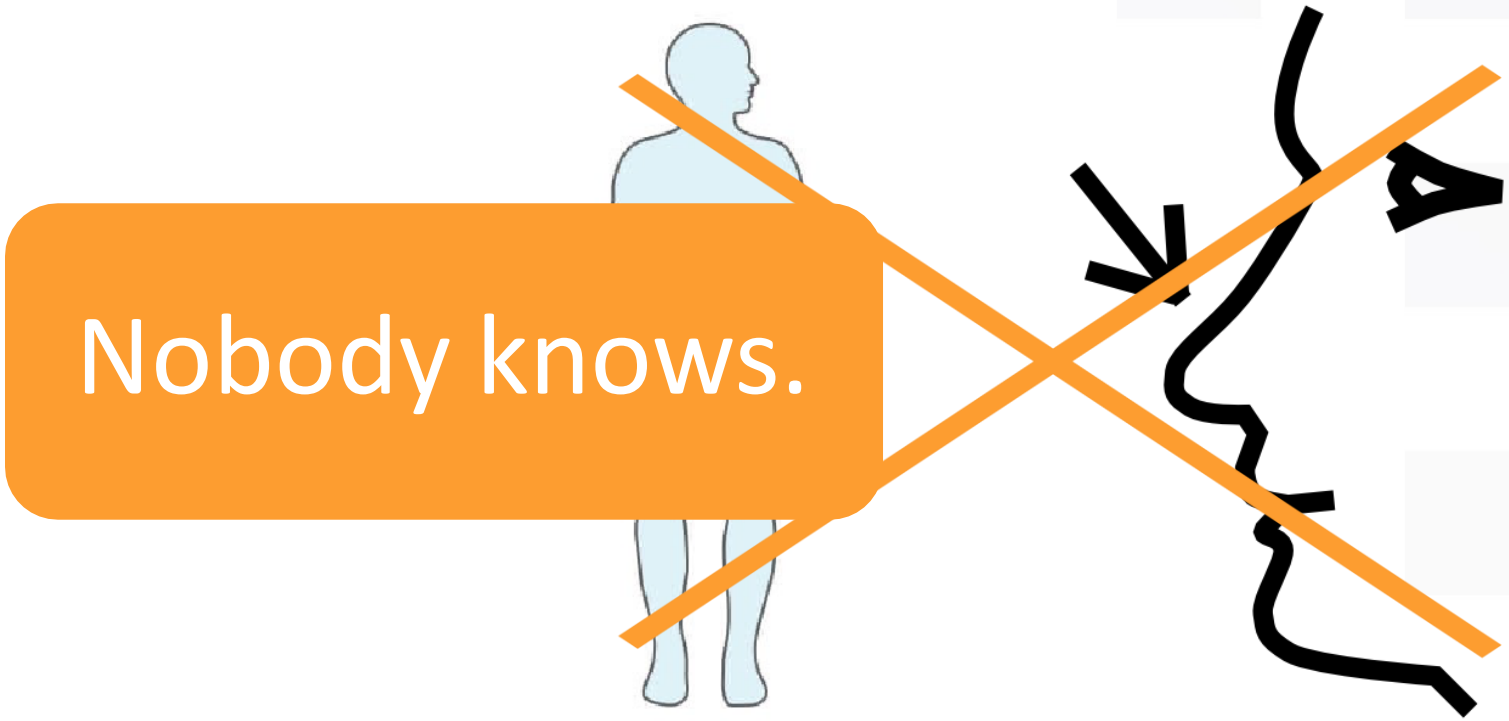
What do you call someone with no body and no nose?

CISSP® MENTOR PROGRAM – SESSION EIGHT

INTRODUCTION

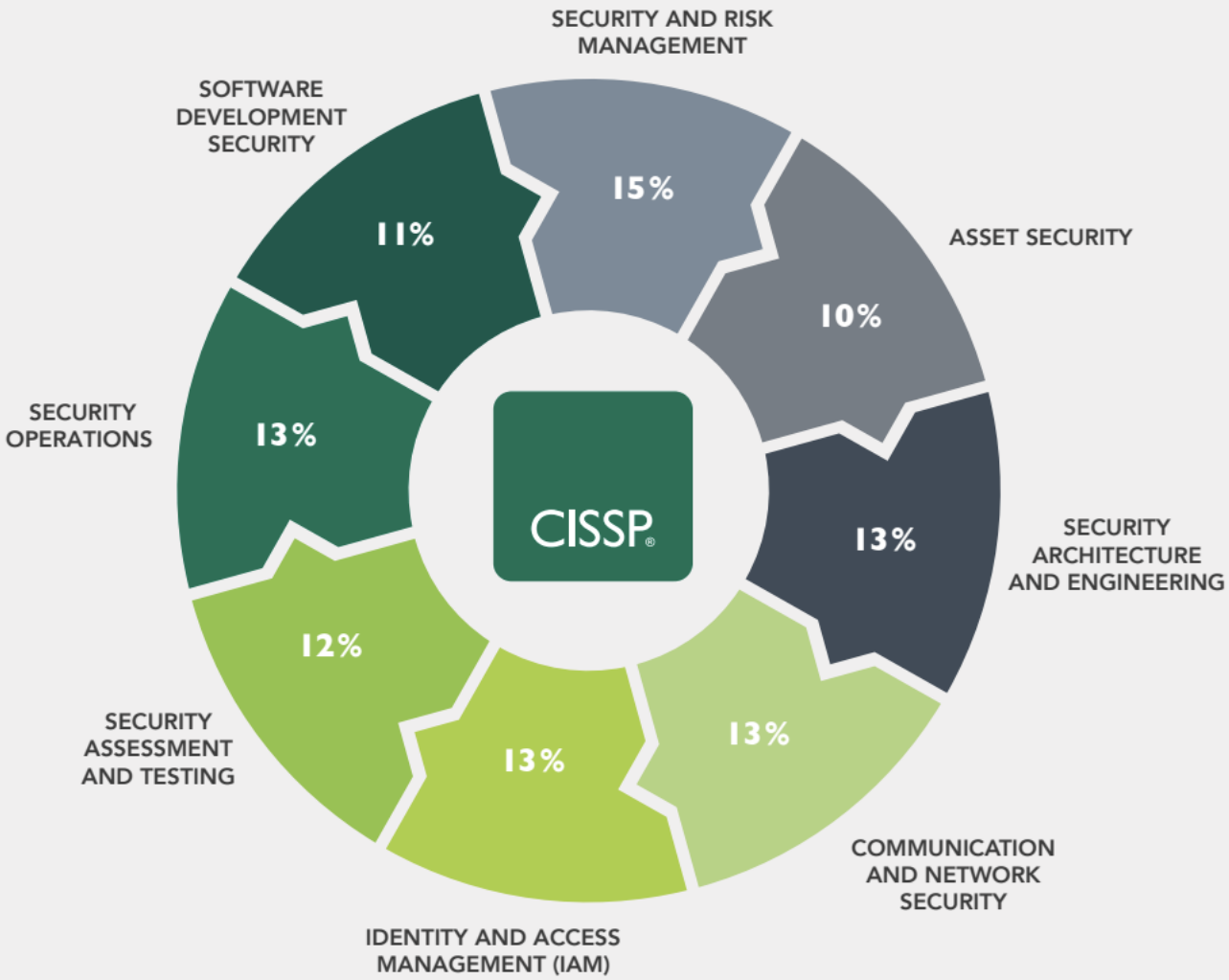
Before we get too deep into this. It's been too long since we did a "dad joke" Is that possible?

What do you call someone with no body and no nose?



CISSP **Exam Overview**

The CISSP exam evaluates expertise across eight security domains. (Think of domains as topics you need to master based on your professional experience and education.) Passing the exam proves you have the advanced knowledge and technical skills to effectively design, implement and manage a best-in-class cybersecurity program.



CISSP® MENTOR PROGRAM – SESSION ONE

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE

Domain 4: Communication and Network Security

4.1 Assess and implement secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)
- Secure protocols
- Implications of multilayer protocols
- Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))
- Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
- Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)
- Cellular networks (e.g., 4G, 5G)
- Content Distribution Networks (CDN)

4.2 Secure network components

- Operation of hardware (e.g., redundant power, warranty, support)
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security

Quick Review

Class 6: May 2nd
Instructor: Chris

Class 7: May 9th
Instructor: Evan

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE

Monday Review
(In 1 slide)

Smarter

Dumber

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	D M
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT	Process
Session (5) Allows session establishment between processes running on different stations.	**S** …gical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with … losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement •		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**	

Application-level firewall.

Circuit-level firewall.

PACKET FILTERING

Static packet filtering firewall.

Stateful inspection firewall.

GATEWAY

Can be used on all layers

Land Based Layers

Repeater and Hub

QUIZ…

Will the real test be this easy too?!

1. What is the most secure type of firewall?
   A. Packet Filter
   B. Stateful Firewall
   C. Circuit-level Proxy Firewall
   D. Application-layer Proxy Firewall

QUIZ…

Will the real test be this easy too?!

1. What is the most secure type of firewall?

   A. Packet Filter

   B. Stateful Firewall

   C. Circuit-level Proxy Firewall

   D. Application-layer Proxy Firewall

Why?

QUIZ…

Will the real test be this easy too?!

2. What WAN Protocol has no error recovery, relying on higher-level protocols to provide reliability?

   A. ATM

   B. Frame Relay

   C. SMDS

   D. X.25

QUIZ…

Will the real test be this easy too?!

2. What WAN Protocol has no error recovery, relying on higher-level protocols to provide reliability?

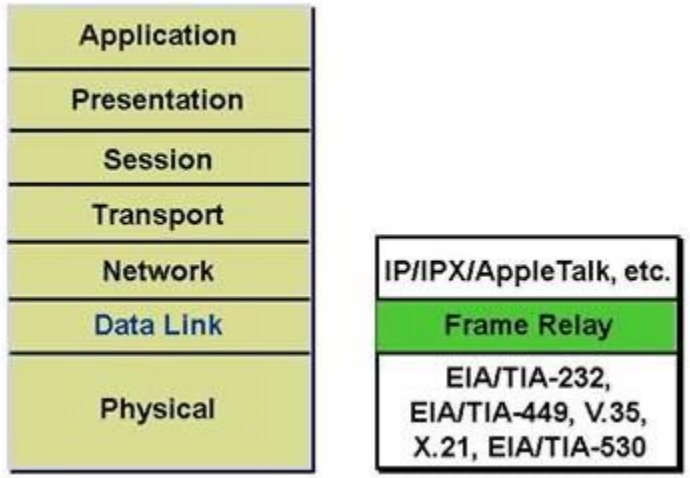
   A. ATM

   B. Frame Relay

   C. SMDS

   D. X.25

What OSI model layer does frame relay operate?



QUIZ…

Will the real test be this easy too?!

3. Which endpoint security technique is the most likely to prevent a previously unknown attack from being successful?

    A. Signature-based antivirus

    B. Host Intrusion Detection Systems (HIDS)

    C. Application Whitelisting

    D. Perimeter firewall

QUIZ…

Will the real test be this easy too?!

3. Which endpoint security technique is the most likely to prevent a previously unknown attack from being successful?

   A. Signature-based antivirus

   B. Host Intrusion Detection Systems (HIDS)

   C. Application Whitelisting

   D. Perimeter firewall

QUIZ…

Will the real test be this easy too?!

4. Restricting Bluetooth device discovery relies on the secrecy of what?

    A. MAC Address

    B. Symmetric key

    C. Private Key

    D. Public Key

QUIZ…

Will the real test be this easy too?!

4. Restricting Bluetooth device discovery relies on the secrecy of what?

   A. MAC Address

   B. Symmetric key

   C. Private Key

   D. Public Key

CISSP® MENTOR PROGRAM – SESSION EIGHT

CISSP CERTIFICATION EXAM OUTLINE & CLASS SCHEDULE

Domain 5: Identity and Access Management (IAM)

New Topic!

5.1 Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities
- Applications

5.2 Manage identification and authentication of people, devices, and services

- Identity Management (IdM) implementation
- Single/Multi-Factor Authentication (MFA)
- Accountability
- Session management
- Registration, proofing, and establishment of identity
- Federated Identity Management (FIM)
- Credential management systems
- Single Sign On (SSO)
- Just-In-Time (JIT)

5.3 Federated identity with a third-party service

- On-premise
- Cloud
- Hybrid

New Topic!

DOMAIN 5
Identity and Access Management

IDENTITY AND ACCESS MANAGEMENT (IAM or IDAM) is fundamental to information security. Controlling access to resources requires the ability to identify and validate the entities requesting access and to hold them accountable for the actions they take. Entities can be users, systems, applications, or processes, and IAM consists of four foundational elements: identification, authentication, authorization, and accountability (IAAA).

Book pp. 377 – 418 (or 514-581 pdf)

DOMAIN 5

April 2018 – April 2021	Effective May 1, 2021
Domain 5: Identity and Access Management (IAM)	**Domain 5:** **Identity and Access Management (IAM)**
• Control physical and logical access to assets • Manage identification and authentication of people, devices, and services • Integrate identity as a third-party service • Implement and manage authorization mechanisms • Manage the identity and access provisioning lifecycle	• Control physical and logical access to assets • Manage identification and authentication of people, devices, and services • Federated identity with a third-party service • Implement and manage authorization mechanisms • Manage the identity and access provisioning lifecycle • Implement authentication systems
Exam Weight: 13%	**Exam Weight: 13%**

DAM)
ess
e the
le for

CISSP® MENTOR PROGRAM – SESSION EIGHT

WHAT ARE WE GOING TO COVER?

Agenda – Domain 5: Identity and Access Management

- Authentication Methods
- Access Control Technologies
- Access Control Models

Identity & Access Management (IAM or IdAM)

Starting on page 377 this evening

Not a challenging domain, but don't let your guard down.

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

pp. 377 – 418 (or 514-581 pdf)

Topics:

- CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS
- MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES
- FEDERATED IDENTITY WITH A THIRD-PARTY SERVICE
- IMPLEMENT AND MANAGE AUTHORIZATION MECHANISMS
- MANAGE THE IDENTITY AND ACCESS PROVISIONING LIFECYCLE
- IMPLEMENT AUTHENTICATION SYSTEMS

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Definitions

- Objects are assets that require access control.
  - Files, datasets, resources, networks
  - Facilities, paper
- Subjects are an active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state. (NIST)
  - Human or non-human
- Access is anything a subject is permitted to do with or to an object.

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

DOMAIN 5: IAM
CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Definitions

- Centralized IAM uses a dedicated access control function or system, to manage all access control.
  - Easier management
  - Single point of failure
- Decentralized IAM assigns access control decisions to system or information owners. (Greater freedom)

- Provisioning = Granting access
- Deprovisioning = Removing access

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Access Control Layers

- Data / Information
- Application
- System
- Device
- Network

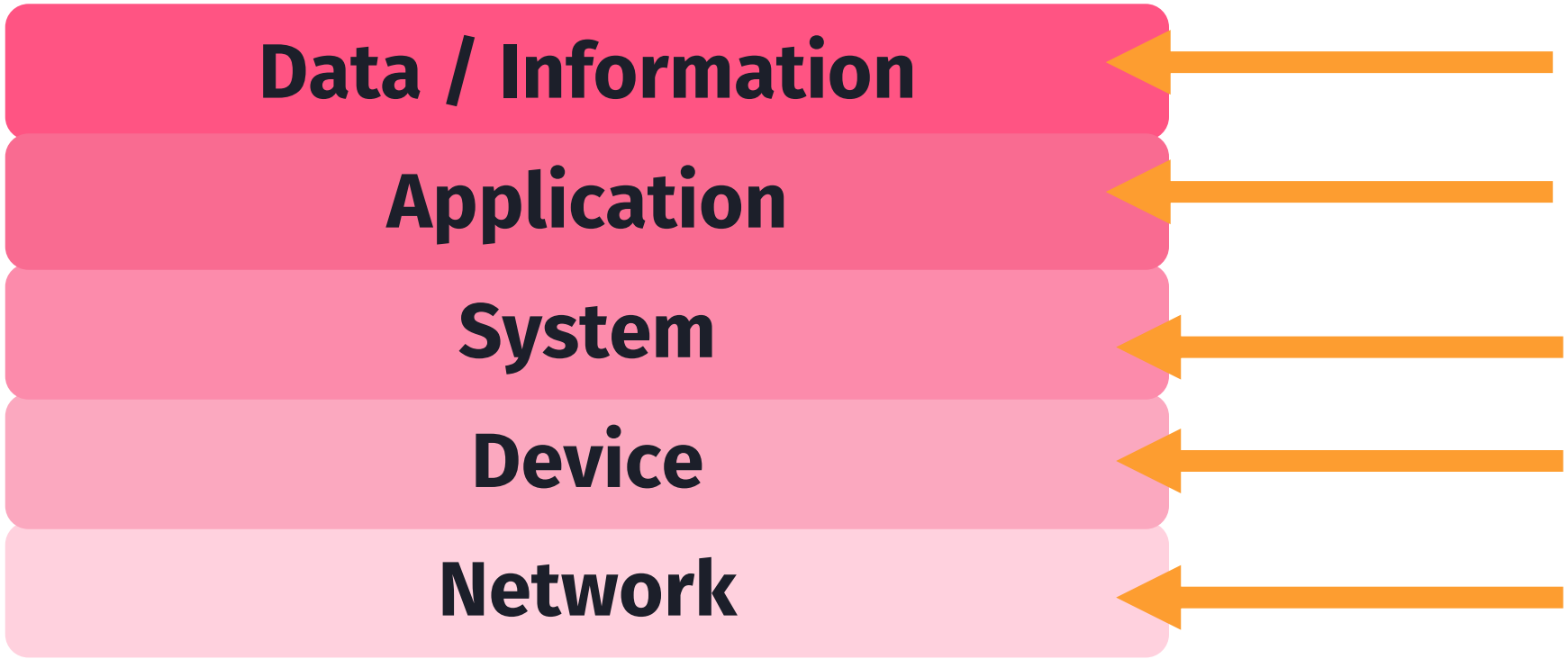
Identifying the needs for information access control is a fundamental requirement for the security practitioner.

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Access Control Layers



DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Devices

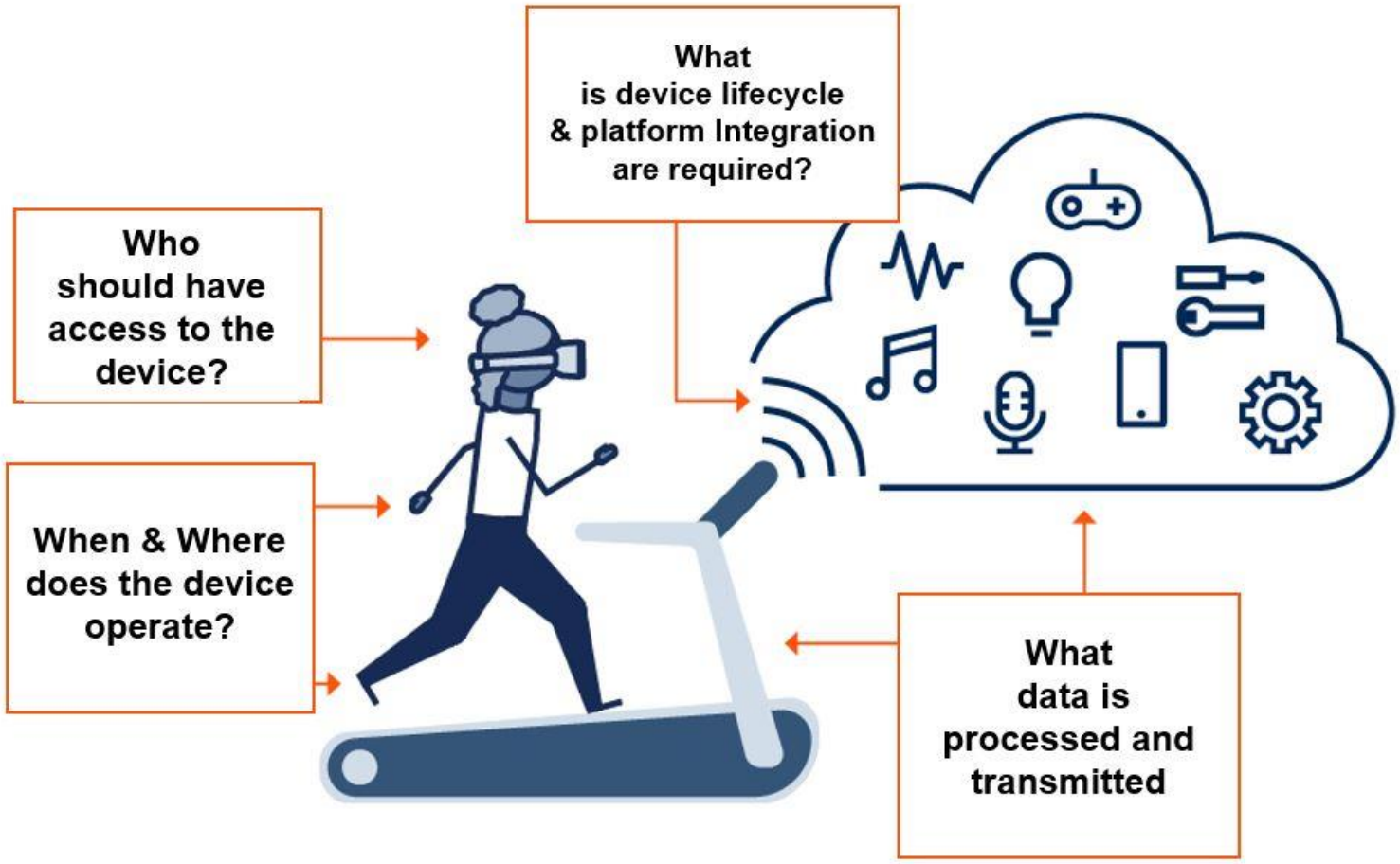
- Anything with an IP Address
- Devices can be both objects and subjects in an access control model
- Endpoint detection and response(EDR)
- Mobile device management (MDM)

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Device Security



Source: Gartner

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

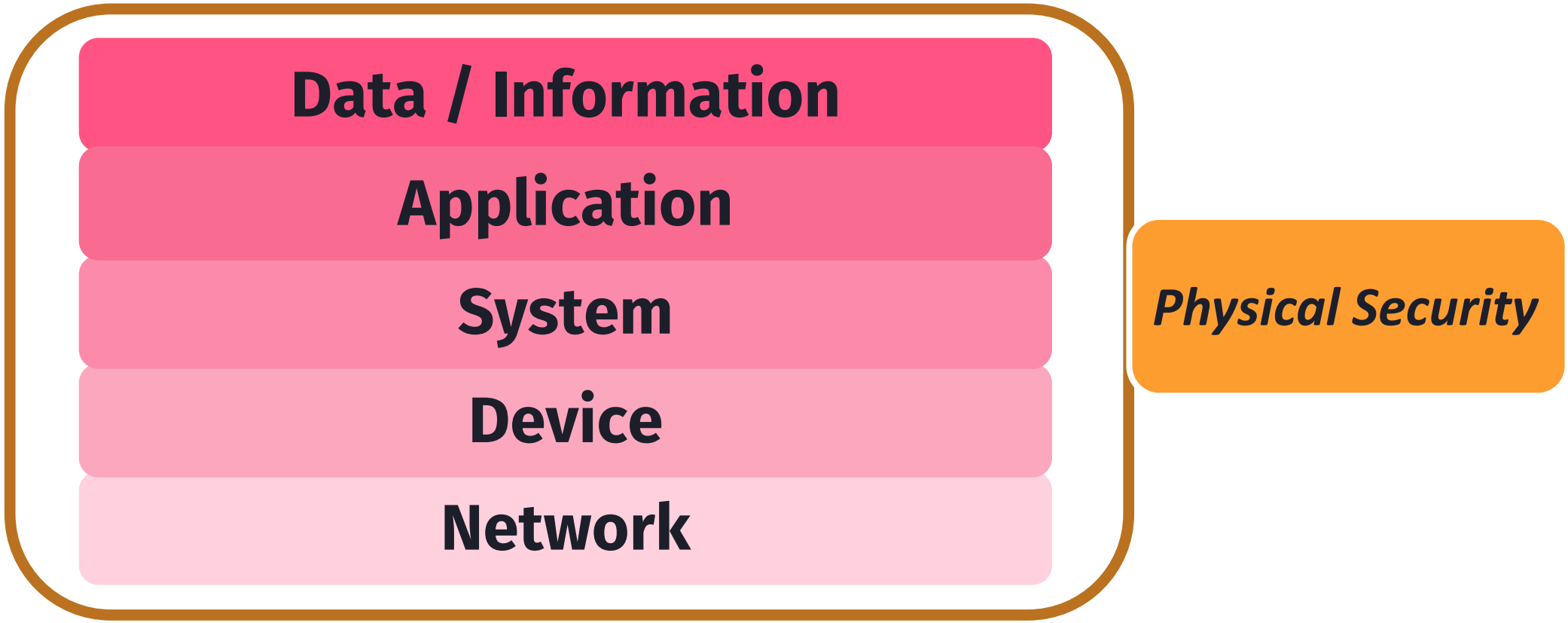
Device Security

- Device Protection - enforces security policies on each device, including password complexity, software updates, and restricting apps
- Device Restrictions - identifies hardware that is not supported or systems that have been **jailbroken**
- Remote lock or wipe - allows the organization to prevent unauthorized users from gaining access
- Containerization - BYOD

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM
CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Access Control Layers



CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Physical Access Control Systems (PACS)

- Traditional Physical Security – 3 G's – Guards, Guns & Gates
- Access Controls – Badges, Keys, Visitor management

- Answer: Who, where, when, why, how
- The complexity of the controls chosen must reflect the value of the assets being protected.

See Chapter 7

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Physical Access Control Systems (PACS)

- User Identification –
  - ID, Badge, Sticker
  - RFID, QR code, Barcode
- Device identification – Non-human assets

See Chapter 7

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Physical Access Control

- Fences & gates
  Delay, Deter, Deny
- Secured doors
- Locks & keys

See Chapter 7

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Physical Access Control

- Guards
- Turnstile / Mantrap
- Intrusion Detection Sensors
  Detect
- CCTV Surveillance

See Chapter 7

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Homework

Sentry AI – Smart Surveillance System
https://www.youtube.com/watch?v=k_Y6I4igjIY

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 2 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Homework

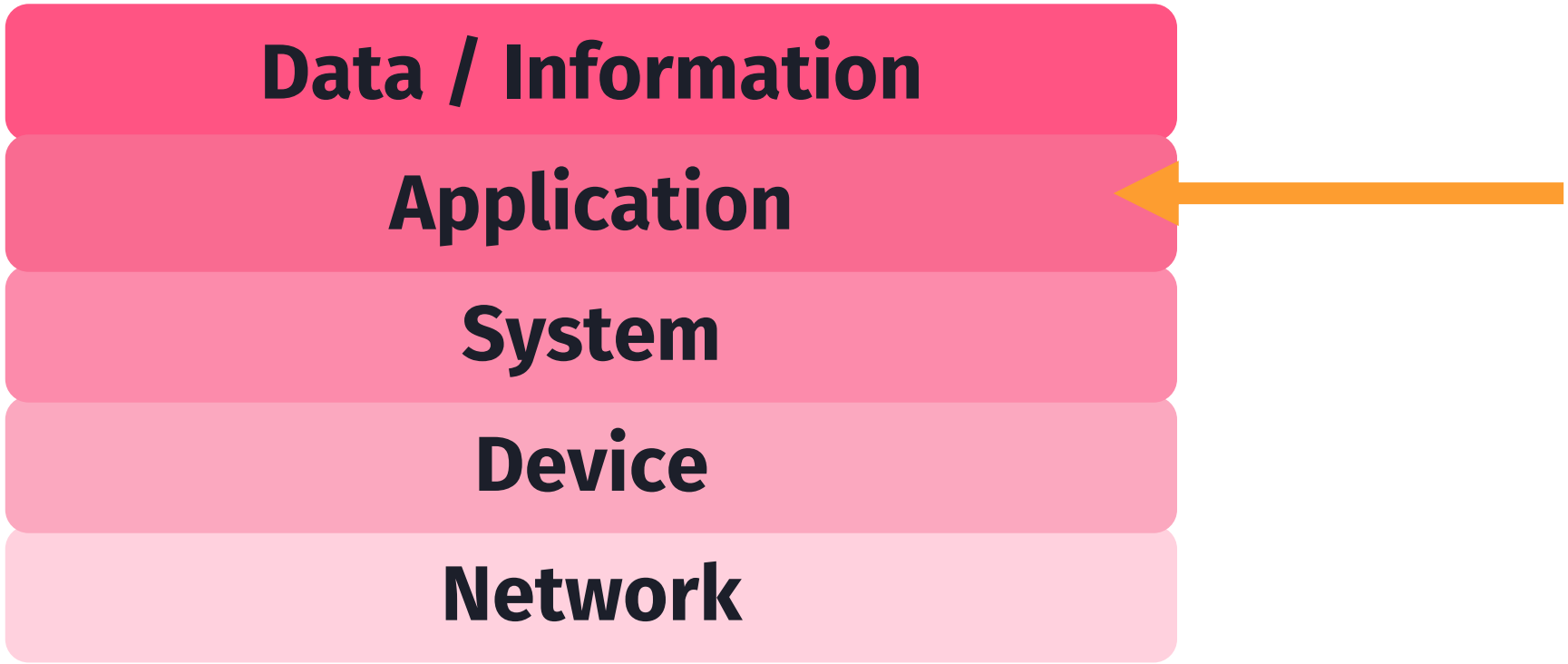
Google Data Center Security: 6 Layers Deep,
https://www.youtube.com/watch?v=kd33UVZhnAA

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Access Control Layers



DOMAIN 5: IAM

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Application Access (objects)

- Access to applications
  Role-based access control (RBAC) — More on this later
- Access to data in applications
  - Data flows between applications — Data Maps
  - BYOD & MDM – isolating / containerizing apps
- Access within applications
  - *Multiple levels* – General vs admin
  - *Granularity* – Controlling access based on level

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IDENTITY & ACCESS MANAGEMENT

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

New Topic!

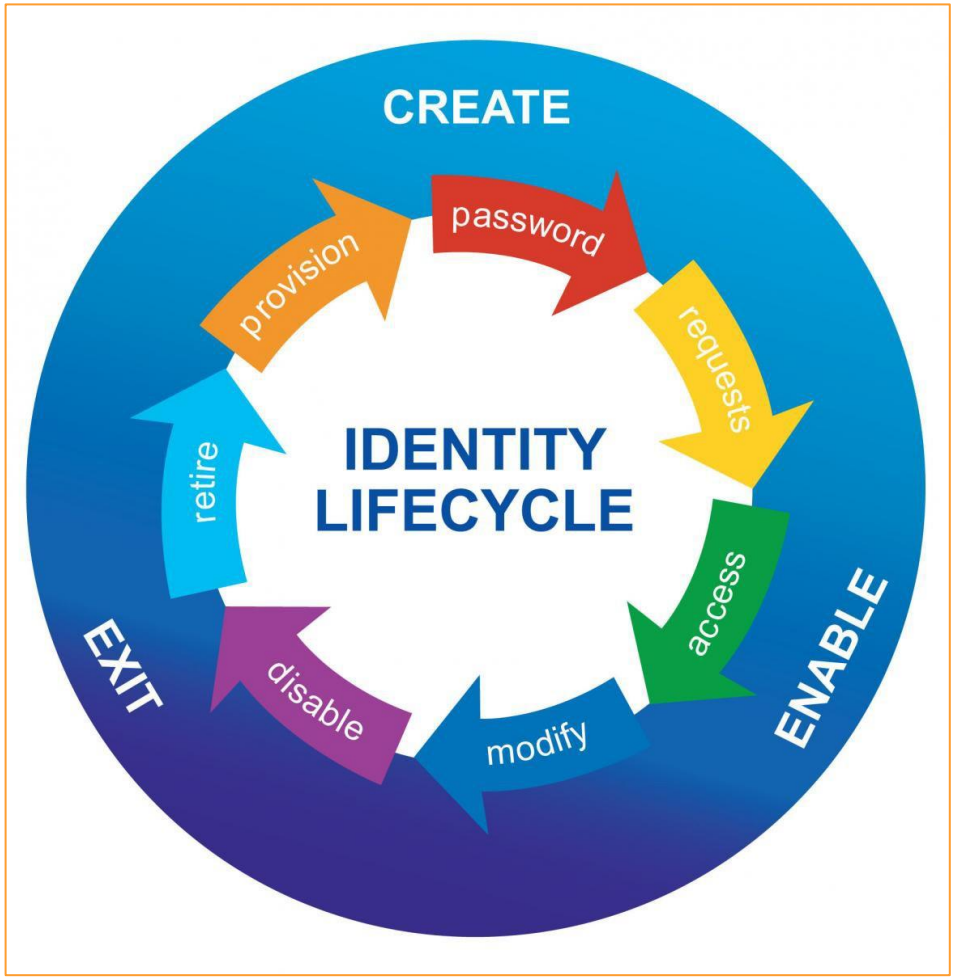
Identification, Authentication, Authorization, Auditing (IAAA)

- *Identification*
  - Process of a subject asserting an identity.
  - Begins before a subject attempts to access an object.
- *Authentication* - the process of proving the asserted identity.
- *Identity Management (IdM)*

Domain 5: Identity and Access Management

Identity Management Implementation

- Provisioning
  - Requesting identity creation & approval process(es)
  - Begins before a subject attempts to access an object
- Deprovisioning
  - Temporary suspension
  - Disabling
  - Deleting

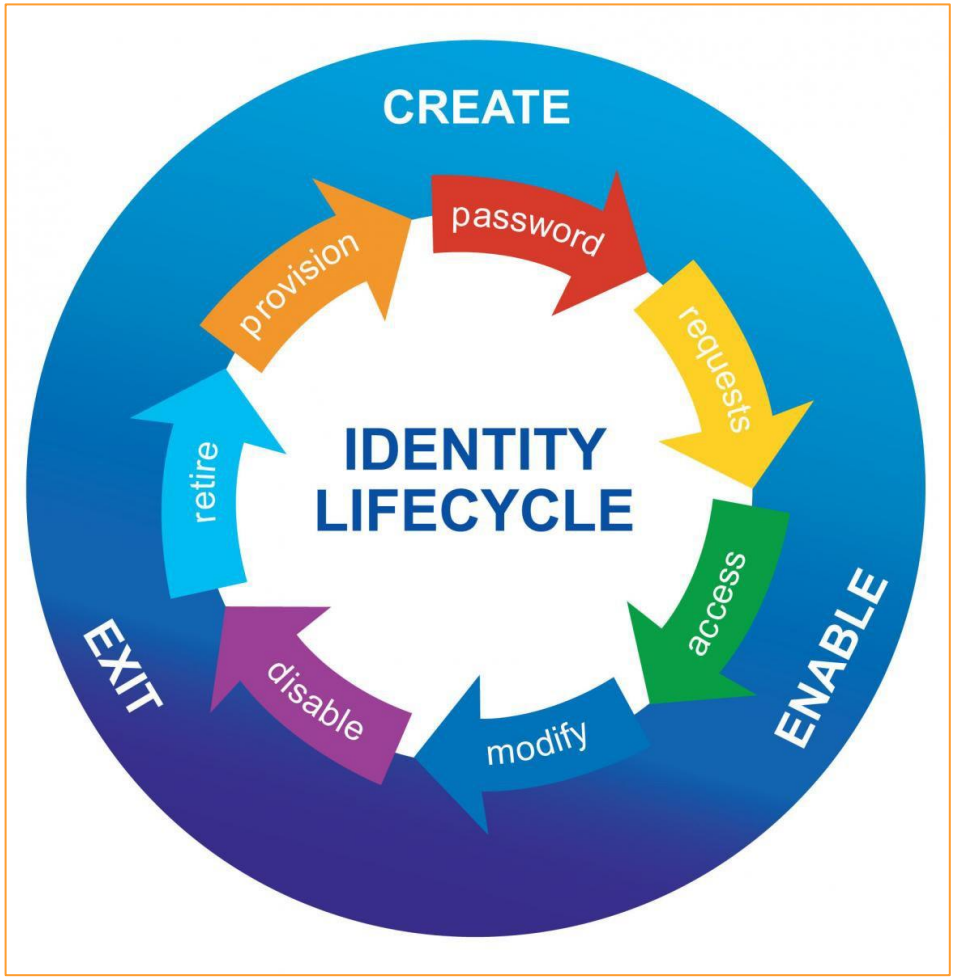


CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Identity Management Implementation

- Authorization Management
  - After identity creation
  - Sets permissions (more later)
- Identity (& Access) Review



DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT

Registration, Proofing, and Establishment of Identity

WARNING! Jumping ahead in the book

NIST SP 800-63-3, "Digital Identity Guidelines"

Credential Service Provider (CSP)

Identity Assurance Levels (IALs)

- IAL1: User self-asserts identity ("Trust me")
- IAL2: Submission of identity documentation – links user to a real-world identity
- IAL3: Reliable evidence of identity + verification

DOMAIN 5: IDENTITY AND ACCESS MANA

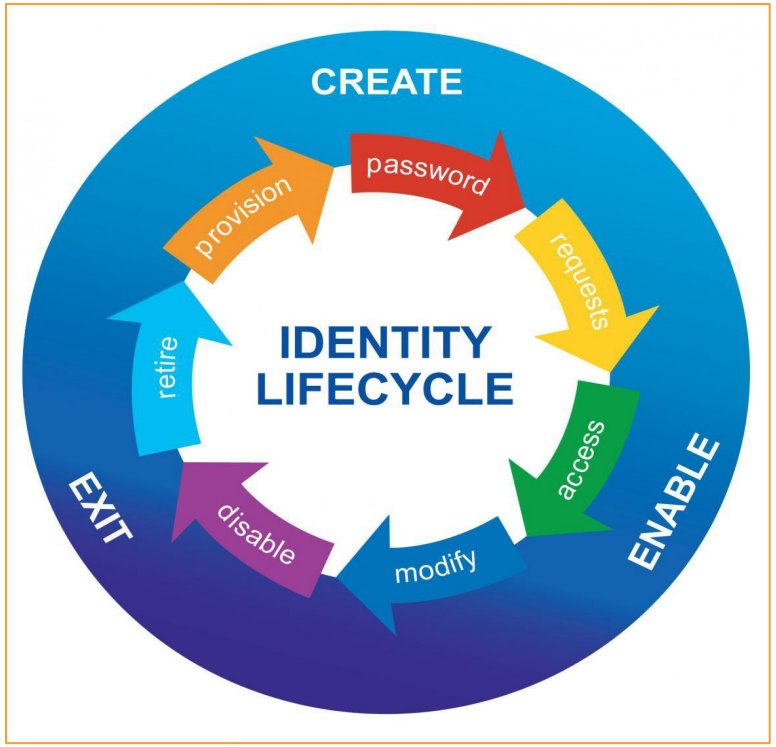
WARNING! Jumping ahead in the book

Credential Management System (CMS)

Tools to manage the identity lifecycle

Examples: Password Managers, PKI (CAs & RAs), AD/LDAP, etc.

- *Sponsorship*: Authorized entity sponsoring the subject
- *Enrollment*: Initial provisioning
- *Credential production*: By services provider
- *Issuance*: Provided to user



Domain 5: Identity and Access Management

Authentication Methods

- A **subject** first identifies his or herself; this identification cannot be trusted.
  - The subject then authenticates by providing an assurance that the claimed identity is valid
- A **credential set** is the term used for the combination of both the identification and authentication of a user
- Three basic authentication methods:
  - **Type 1** (something you know),
  - **Type 2** (something you have), and
  - **Type 3** (something you are).
  - A fourth type of authentication is some place you are (sorta).

Which is the oldest?

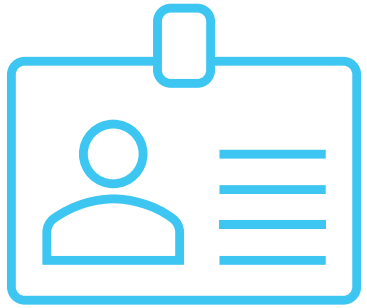
CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Authentication Methods

Something you **know**:

- Password
- Passphrase
- PIN



Something you **have:**

- Smartcard
- Token
- Device
- Application

Something you **are:**

- Fingerprints
- Face
- Eyes
- Biometrics

Where you **are:**

- Geolocation

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know – Passwords

- Memorized Secrets (Passwords, Passphrases, PINs)
  - Long static passwords, comprised of words in a phrase or sentence
  - An example of a passphrase is: “I will pass the CISSP® in 2 months!”
  - Usually have less randomness per character compared to shorter complex passwords (such as “B$%Jiu∗!”), but make up for the lack of randomness with length
- One-time passwords
  - Used for a single authentication
  - Very secure but difficult to manage
  - A one-time password is impossible to reuse and is valid for just one-time use

Long is Strong

Domain 5: Identity and Access Management

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know

Super Strong Password

Long is Strong

CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Rule 1 - Password Length <16 chars
Rule 2 - Only numbers char weight for passwords <16 chars
Rule 3 - Only lower case letters char weight for passwords <16 chars
Rule 4 - Only upper case letters char weight for passwords <16 chars
Rule 5 - Only letters char weight for passwords <16 chars
Rule 6 - Mix of letters and numbers char weight for passwords <16 chars
Rule 7 - Number times where this password is compromised in a breach
Rule 8 - The password is word that exists in dictionary
Rule 9 - The password is word that exists in dictionary with simple obfuscation
Rule 10 - 80%+ from the password is word that exists in dictionary
Rule 11 - 80%+ from the password is word that exists in dictionary with simple obfuscation
Rule 12 - 60%+ from the password is word that exists in dictionary
Rule 13 - 60%+ from the password is word that exists in dictionary with simple obfuscation
Rule 14 - The password is double word (stopstop, crabcrab)
Rule 15 - Contains common sequences from a keyboard row (qwerty, etc.)
Rule 16 - Contains numeric sequences based on well known numbers such as 911
Rule 17 - Word with numbers appended
Rule 18 - Contains anything personally related (phone, zip, birthday, email username)

Long is Strong

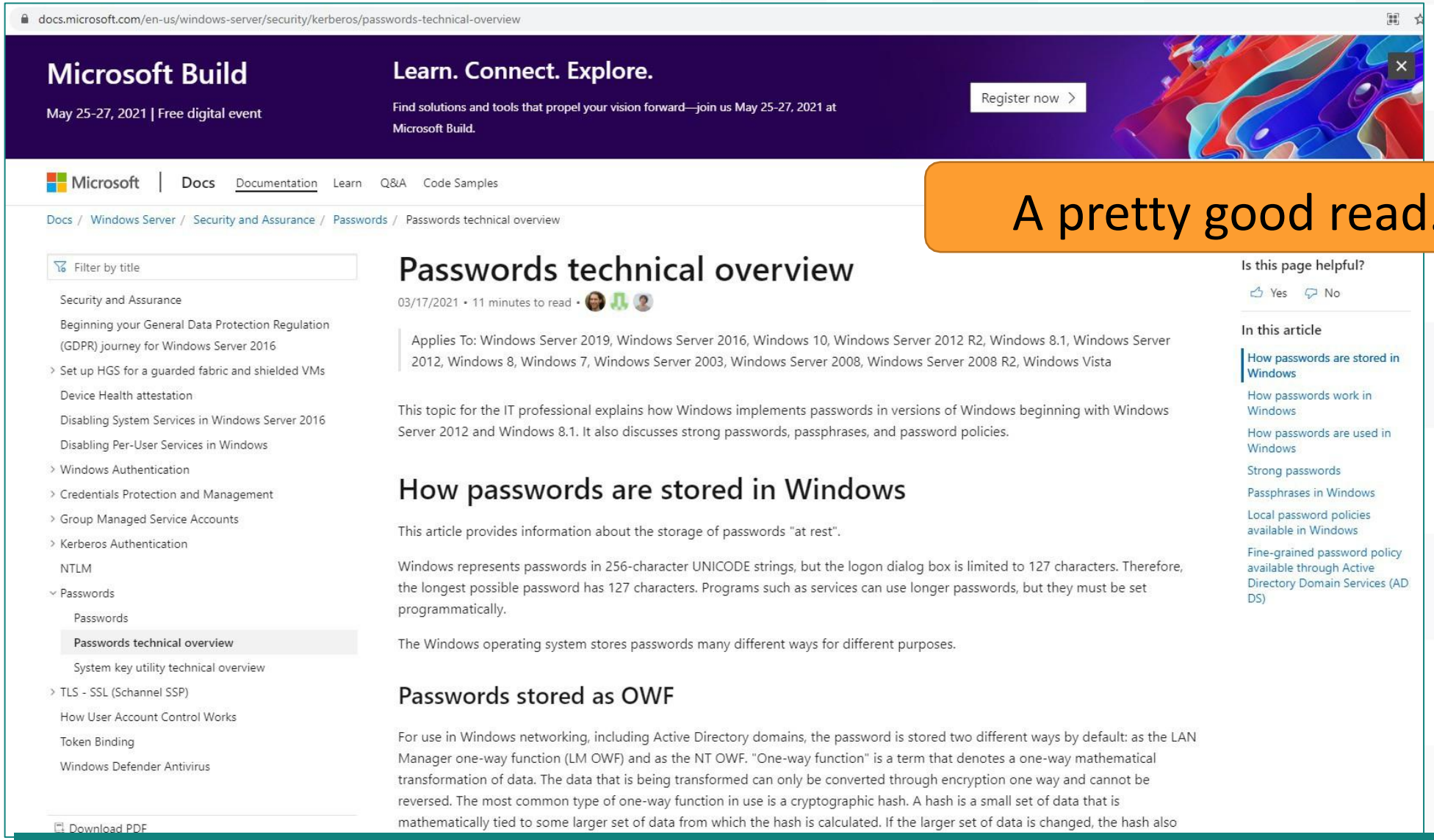
Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know – Passwords

- Dynamic passwords
  - Change at regular intervals
  - RSA Security makes a synchronous token device called SecureID that generates a new token code every 60 seconds. The user combines their static PIN with the RSA dynamic token code to create one dynamic password that changes every time it is used.
  - One drawback when using dynamic passwords is the **expense** of the tokens themselves
- Strong authentication (also called multifactor authentication) requires that the user present more than one authentication factor

Source: NIST SP800-63B

CISSP® MENTOR PROGRAM – SESSION EIGHT



A pretty good read.

https://docs.microsoft.com/en-us/windows-server/security/kerberos/passwords-technical-overview

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know - Passwords

Password Hashes and Password Cracking

- In most cases, clear text passwords are not stored within an IT system; only the hashed outputs
- Hashing is one-way encryption using an algorithm and no key
- When a user attempts to log in, the password they type is hashed, and that hash is compared against the hash stored on the system
- The hash function cannot be reversed: it is impossible to reverse the algorithm and produce a password from a hash
- An attacker may run the hash algorithm forward many times, selecting various possible passwords, and comparing the output to a desired hash, hoping to find a match (and to derive the original password). This is called password cracking.

CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know - Passwords

Password Hashes and Password Cracking

Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years

March 21, 2019 208 Comments

Hundreds of millions of **Facebook** users had their account passwords stored in plain text and searchable by thousands of Facebook employees — in some cases going back to 2012, KrebsOnSecurity has learned. Facebook says an ongoing investigation has so far found no indication that employees have abused access to this data.

- An attacker may ru rd many times, selecting various possible pa e output to a desired hash, hoping to find a match (and to derive the original password). This is called password cracking.

WHAT THE &%!$?

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know - Passwords

Password Hashes and Password Cracking

- Password hashes for modern UNIX/Linux systems are stored in/etc/shadow (which is typically readable only by root)
- Windows systems store hashes both locally and on the domain controller (DC) in a file called the security account management file or SAM file
- Password hashes may be sniffed on networks or read from memory
- The SAM file is locked while the Windows operating system is running tools such as fgdump by foofus.net (http://www.foofus.net/fizzgig/fgdump/) can dump the hashes from memory.

CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know - Passwords

Password Hashes and Password Cracking

See 2021 Slides and Video for password hacking tools

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know - Passwords

Password Managers

- A software application that can manage authentication material like passwords, passphrases, and answers to secret questions
- Support across desktop and mobile operating systems
- Can serve to offload the work of creating, remembering, and filling in passwords.

What password manager do you use?

Investopedia – Best Password Managers – https://www.investopedia.com/best-password-managers-5080381

Domain 5: Identity and Access Management

Type 1 Authentication: Something You Know - Passwords

Review Crypto / Hashing

Password Salting

- Allows one password to hash multiple ways
- Some systems (like modern UNIX/Linux systems) combine a salt with a password before hashing: “The designers of the UNIX operating system improved on this method by using a random value called a “salt.” A salt value ensures that the same password will encrypt differently when used by different users. This method offers the advantage that an attacker must encrypt the same word multiple times (once for each salt or user) in order to mount a successful password-guessing attack.”
- Makes rainbow tables far less effective (if not completely ineffective)

If two passwords are the same, their hashes will be identical.

Mon, 11 May 2020 16:18:58 -0400

NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

COMPUTER SECURITY

NIST
National Institute of

How long is a standard “good” password?

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

Mon, 11 May 2020 16:18:58 -0400

NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

A Brief Summary

Also referred to as memorized secrets, here is a brief summary of 2019 NIST password guidelines:

- 8 character minimum when a human sets it
- 6 character minimum when set by a system/service
- Support at least 64 characters maximum length
- All ASCII characters (including space) should be supported
- Truncation of the secret (password) shall not be performed when processed
- Check chosen password with known password dictionaries
- Allow at least 10 password attempts before lockout
- No complexity requirements
- No password expiration period
- No password hints
- No knowledge-based authentication (e.g. who was your best friend in high school?)
- No SMS for 2FA (use a one-time password from an app like Google Authenticator)

pdf

How long is a standard “good” password?

https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

Microsoft Password Guidance

Robyn Hicock, rhicock@microsoft.com

Microsoft Identity Protection Team

Purpose

This paper provides Microsoft's recommendations for password management based on current research and lessons from our own experience as one of the largest Identity Providers (IdPs) in the world. It covers recommendations for end users and identity administrators.

Microsoft sees over 10 million username/password pair attacks every day. This gives us a unique vantage point to understand the role of passwords in account takeover. The guidance in this paper is scoped to users of Microsoft's identity platforms (Azure Active Directory, Active Directory, and Microsoft account) though it generalizes to other platforms.

Summary of Recommendations

Advice to IT Administrators

Azure Active Directory and Active Directory allow you to support the recommendations in this paper:

1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.
6. Enforce registration for multi-factor authentication.
7. Enable risk based multi-factor authentication challenges.

Advice to Users

Domain 5: Identity and Access M

Further Confuses things... 😐

NIST SP800-63B – Authenticator Assurance Levels (AAL)

Level of Assurance	Description
AAL1	AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.
AAL2	AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.
AAL3	AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

CISSP® MENTOR PROGRAM

Domain 5: IAM

NIST SP800-63B – Authenticator Assurance Levels (AAL)

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

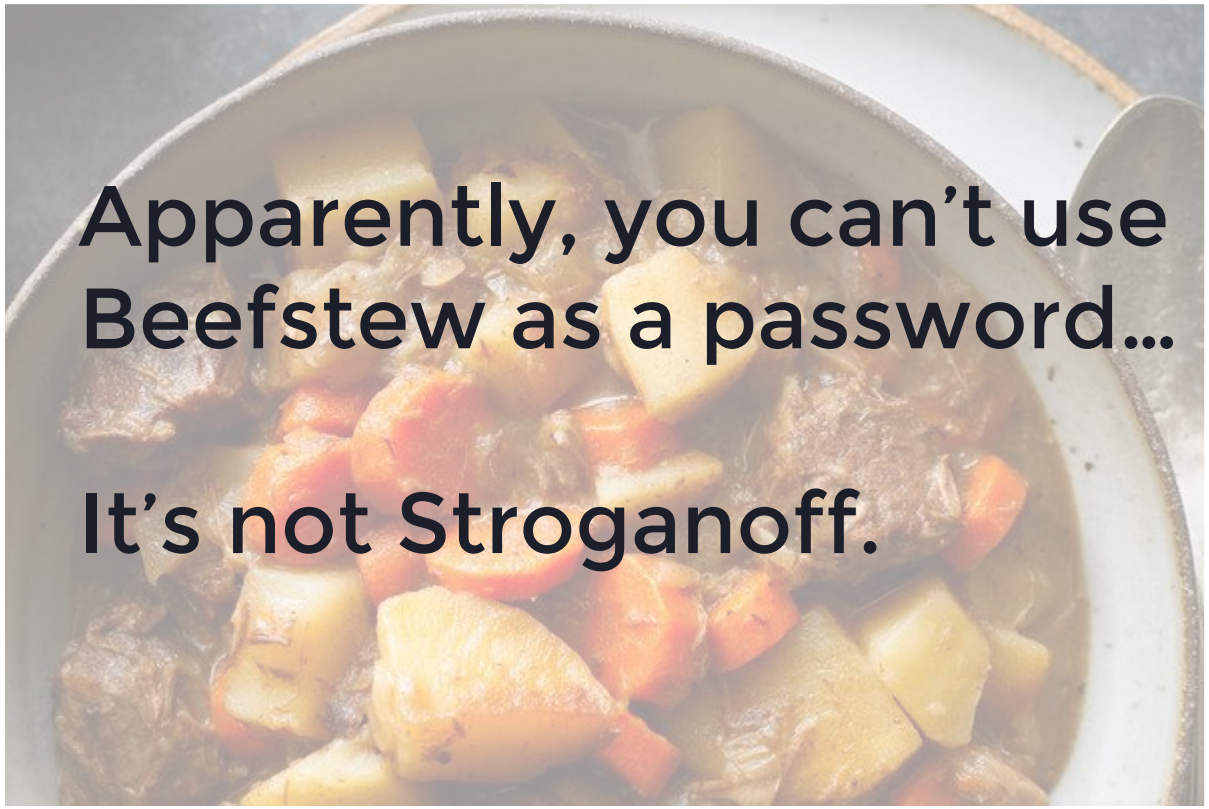
Table 4-1 AAL Summary of Requirements

Requirement	AAL1	AAL2	AAL3
Permitted authenticator types	Memorized Secret; Look-up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 validation	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Security controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)
MitM resistance	Required	Required	Required
Verifier-impersonation resistance	Not required	Not required	Required
Verifier-compromise resistance	Not required	Not required	Required
Replay resistance	Not required	Required	Required
Authentication intent	Not required	Recommended	Required
Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IDENTITY & ACCESS MANAGEMENT

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS



Domain 5: Identity and Access Management

Type 2 Authentication: Something You Have

- Something you have - requires that users possess something, which proves they are an authenticated user
- A token is an object that helps prove an identity claim
- Possessing the car keys, credit cards, bank ATM cards, smartcards, and paper documents
- Safeguarding the confidentiality and availability of the physical devices

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT

Apple, Microsoft and Google announce plans to enable passwordless authentication for billions of devices

VentureBeat

https://venturebeat.com/2022/05/05/passwordless-authentication/

Homework

Domain 5: Identity and Access Management

Type 2 Authentication: Something You Have

Synchronous Dynamic Token

- Time or counters are synchronized with an authentication server.
- Implemented in hardware (RSA SecureID) and software (Google / Microsoft Authenticator).
- The authentication server expects a certain value based on time or count, as part of the authentication scheme.

Domain 5: Identity and Access Management

Type 2 Authentication: Something You Have

Synchronous Dynamic Token

- Time or counters are synchronized with an authentic
- Implemented in hardware (RSA SecureID) and softwa ft Authenticator).
- The authentication server expects a certain value bas as part of the authentication scheme.

How many use an authenticator app?

Domain 5: Identity and Access Management

Type 2 Authentication: Something You Have

Asynchronous Dynamic Token

- Not synchronized with a central server
- Most common variety is challenge-response tokens
  - Systems produce a challenge, or input for the token device
  - The user manually enters the information into the device along with their PIN, and the device produces an output
  - Output is then sent to the system
- Combining access control types is recommended
- Using more than one type of access control is referred to as strong authentication or multifactor authentication

Doma ment

Type 2

Asynchr

- Not sy
- Most
  - Sy
  - Th with their PIN, an
  - Ou
- Comb
- Using strong authe

Domain 5: Identity and Access Management

Type 2 Authentication: Something You Have

Conditional MFA

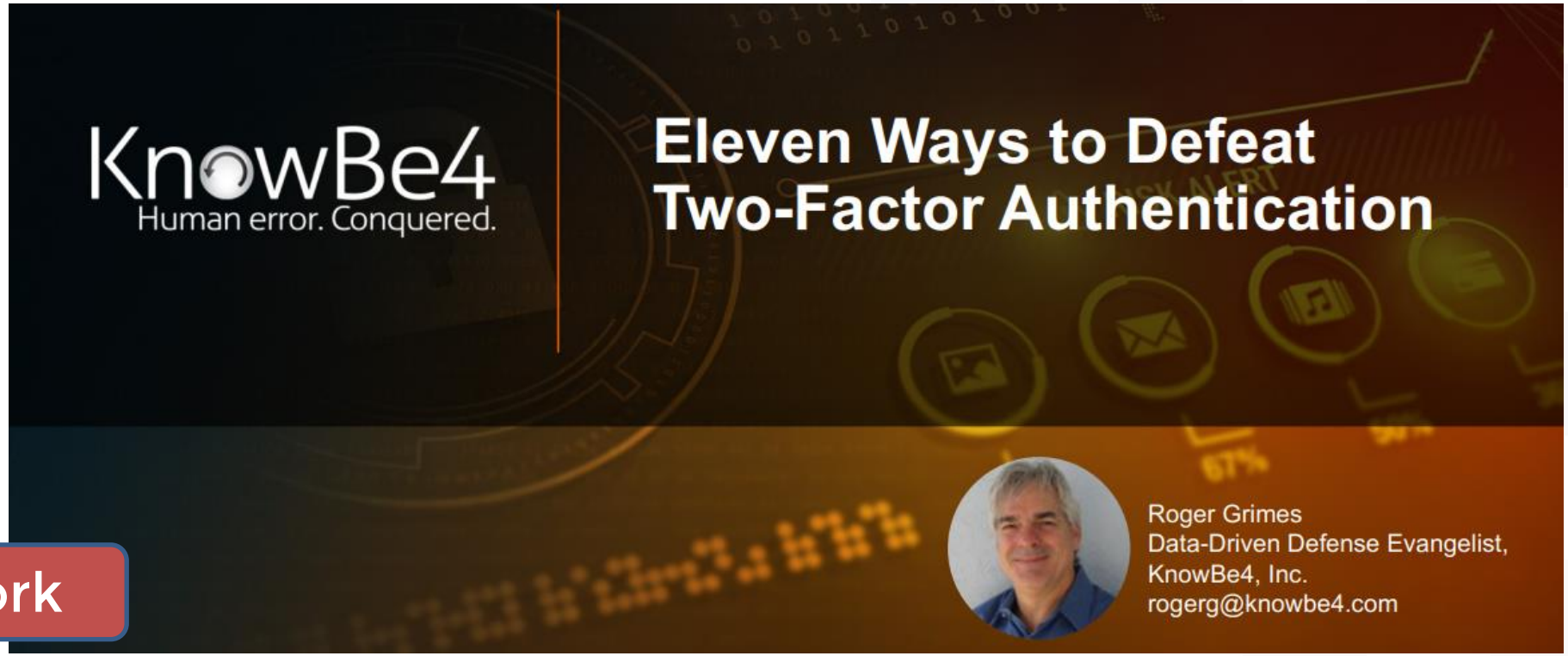
- Dynamic trusted device authentication can also be used to both increase security and provide greater usability
- A key element of *attribute-based access control* (ABAC)
- Time or location based

CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Type 2 Authentication: Something You Have

SMS Authentication - Is it safe?



Homework

https://www.knowbe4.com/hubfs/KB4-11WaystoDefeat2FA-RogerGrimes.pdf & https://blog.knowbe4.com/author/roger-grimes

Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

- Something you are - biometrics, which uses physical characteristics as a means of identification or authentication
- Biometrics may be used to establish an identity, or to authenticate (prove an identity claim)
- Associated with the physical traits of an individual, it is more difficult for that individual to forget, misplace, or otherwise lose control of the access capability
- Care should be given to ensure appropriate accuracy and to address any privacy issues that may arise
- Should be reliable, and resistant to counterfeiting
- Data storage required to represent biometric information (called the template or the file size) should be relatively small: 1000 bytes or less is typical

Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

Biometric Fairness, Psychological Comfort, & Safety

- Biometrics should not cause undue psychological stress to subjects, and should not introduce unwarranted privacy issues
- Biometric controls must be usable by all staff, or compensating controls must exist
- Potential exchange of bodily fluid is a serious negative for any biometric control: this includes retina scans (where a user typically presses their eye against an eyecup), and even fingerprint scanning (where many subjects touch the same scanner)
- Fully passive controls, such as iris scans, may be preferable (there is no exchange of bodily fluid)

Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

Biometric Controls

- Fingerprints
- Hand Geometry
- Retina Scan
- Iris Scan
- Keyboard Dynamics
- Dynamic Signature
- Voice
- Facial Scan

Not really covered in the book.

Still know…

See last years slides

Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

Biometric Enrollment and Throughput

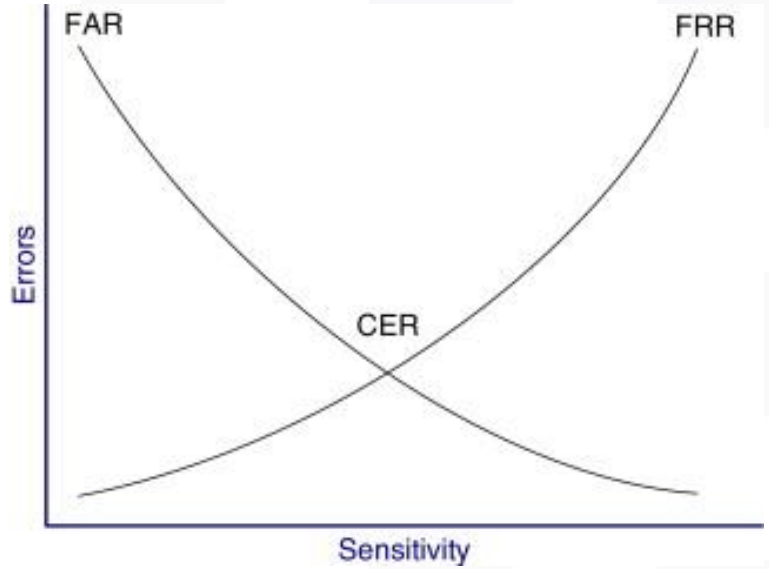
- Enrollment describes the process of registering with a biometric system: creating an account for the first time
  - Enrollment is a one-time process that should take 2 minutes or less.
  - Challenge with remote workers
- Throughput describes the process of authenticating to a biometric system
  - Also called the biometric system response time
  - A typical throughput is 6-10 seconds

Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

Biometric Accuracy

- Should be considered before implementing a biometric control program
- Three metrics are used to judge biometric accuracy:
  - False Reject Rate (FRR),
  - False Accept Rate (FAR),
  - Crossover Error Rate (CER).



Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

Biometric Accuracy / Access Control Errors

- **False Reject Rate (FRR)**
  - When an authorized subject is rejected by the biometric system as unauthorized
  - Also called a **Type I error**
  - Cause frustration of the authorized users, reduction in work due to poor access conditions, and expenditure of resources to revalidate authorized users
- **False Accept Rate (FAR)**
  - Occurs when an unauthorized subject is accepted as valid
  - Risks an unauthorized user gaining access
  - Also called a **Type II error**

Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

Biometric Accuracy / Access Control Errors

Note: A false accept is worse than a false reject: most organizations would prefer to reject authentic subjects to accepting impostors. FARs (Type II errors) are worse than FRRs (Type I errors).

Two is greater than one, which will help you remember that FAR is Type II, which are worse than Type I (FRRs).

Over 40 data points are usually collected and compared in a typical fingerprint scan. The accuracy of the system may be lowered by collecting fewer minutiae points (ten or so). This will lower the FRR, but raise the FAR. It also increases the possibility that a user's fingerprints would be easier to counterfeit.

Domain 5: Identity and Access Management

Type 3 Authentication: Something You Are

Biometric Accuracy / Access Control Errors

Crossover Error Rate (CER)

- Describes the point where the False Reject Rate (FRR) and False Accept Rate (FAR) are equal
- Also known as the **Equal Error Rate (EER)**
- The overall accuracy of a biometric system
- As the accuracy of a biometric system increases, FARs will rise and FRRs will drop
- As the accuracy is lowered, FARs will drop and FRRs will rise

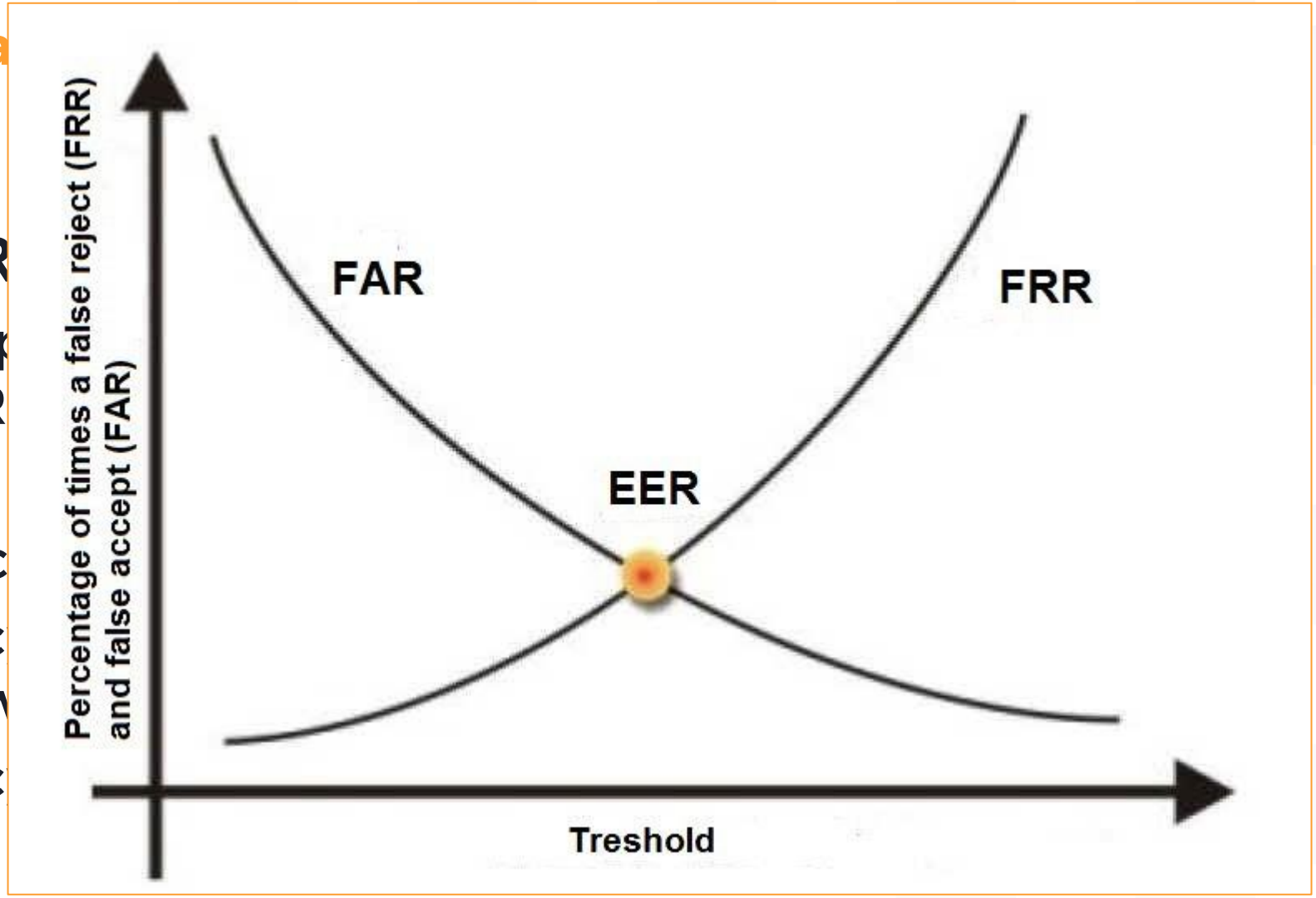
Domain 5: Identity and Access Management

Type 3 Authentica

Biometric Accuracy

Crossover Error R

- Describes the p
  False Accept R
- Also known as
- The overall acc
- As the accurac
  rise and FRRs w
- As the accurac



Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Session Management

- Session is an exchange between communicating devices, such as a client and server exchanging information
- Access is limited to the session
- Session security vulnerabilities
  - Session Hijacking - MITM
  - Session Sidejacking – same network, not direct attack
  - Session fixation – reuse session IDs

OWASP Session Management Best Practices - https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Access Control

New Topic!

And Finally…

We're on to Access Control

Review Chapter 3 – Fundamental Concepts of Security Models

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Centralized Access Control

- Concentrates access control in one logical point for a system or organization
- Can be used to provide Single Sign-On (SSO), where a subject may authenticate once, and then access multiple systems
- Can centrally provide the three "A's" of access control: Authentication, Authorization, and Accountability
  - Authentication: proving an identity claim
  - Authorization: authenticated subjects are allowed to take on a system
  - Accountability: the ability to audit a system and demonstrate the actions of subjects

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Decentralized Access Control

- Allows IT administration to occur closer to the mission and operations of the organization
- Also called distributed access control
- Provides more local power: each site has control over its data
- The U.S. military uses decentralized access control in battlefield situations

Exam Warning - Do not get confused on the CISSP exam if asked about DAC compared to decentralized access control. DAC stands for discretionary access control. Decentralized access control will always be spelled out on the exam.

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Federated Identity Management (FIdM)

Question: Is it centralized or decentralized?

Exam Warning – FIdM may also be called FIM.
Look at the context of the question.

CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Registration, Proofing, and Establishment of Identity

Covered earlier with Identity Management

Credential Management System (CMS)

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Single Sign-On (SSO)

- Allows multiple systems to use a central Authentication Server (AS)
- Allows users to authenticate once, and then access multiple, different systems
- Allows security administrators to add, change, or revoke user privileges on one central system

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Single Sign-On (SSO)

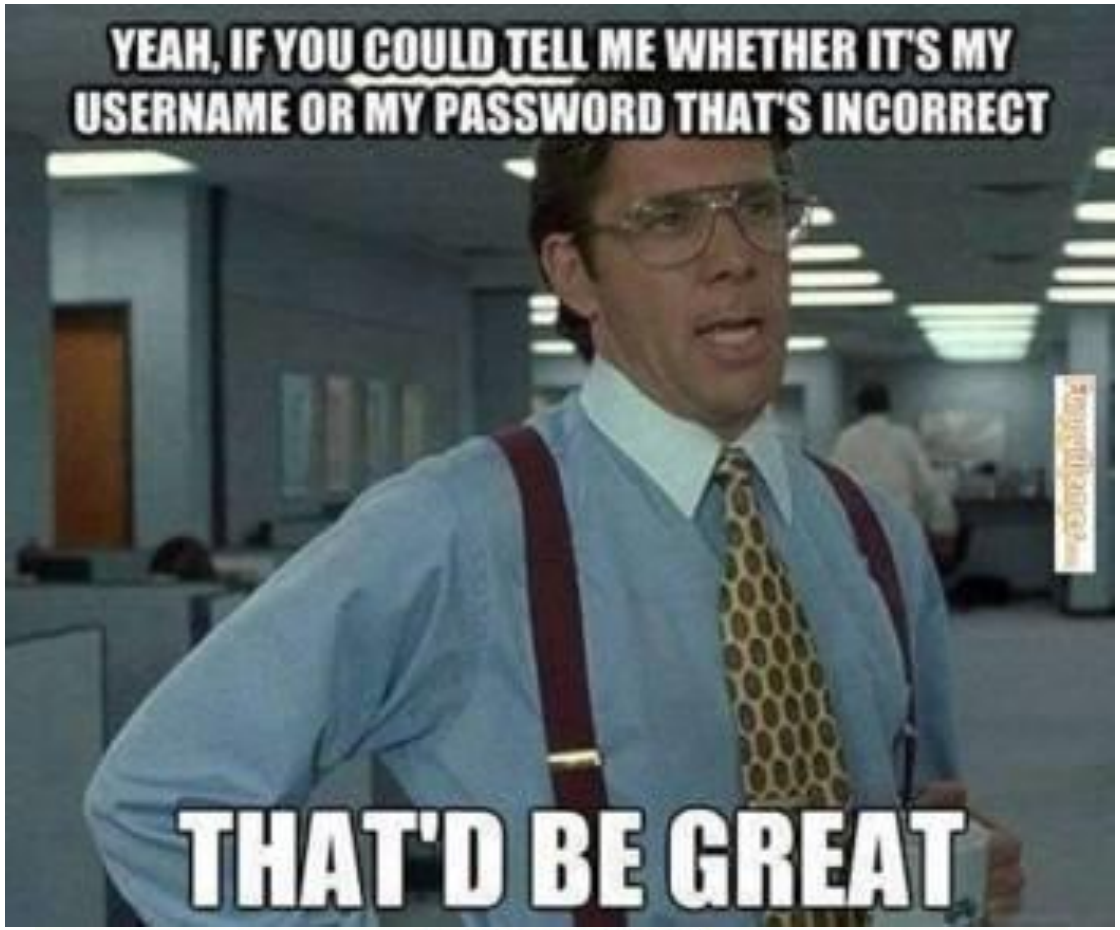
As outlined in the IBM article, "Build and Implement a Single Sign-On Solution" by Chris Dunne, September 30, 2003, SSO is an important access control and can offer the following **benefits**:

- "**Improved user productivity**. Users are no longer bogged down by multiple logins, and they are not required to remember multiple IDs and passwords. Also, support personnel answer fewer requests to reset forgotten passwords."
- "**Improved developer productivity**. SSO provides developers with a common authentication framework. In fact, if the SSO mechanism is independent, then developers do not have to worry about authentication at all. They can assume that once a request for an application is accompanied by a username, then authentication has already taken place."
- "**Simplified administration**. When applications participate in a single sign-on protocol, the administration burden of managing user accounts is simplified. The degree of simplification depends on the applications since SSO only deals with authentication. So, applications may still require user-specific attributes (such as access privileges) to be set up."

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: IDENTITY & ACCESS MANAGEMENT

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS



Domain 5: Identity and Access Management

Federated Identity with a Third-Party Service

New Topic!

Federated Identity Management (FIdM)

- A process that allows for the conveyance of identity and authentication information across a set of networked systems. (NIST Glossary)
- The establishment of a trusted relationship between separate organizations and third parties, such as application vendors or partners, allowing them to share identities and authenticate users across domains. (Ping Identity)

Domain 5: Identity and Access Management

Federated Identity with a Third-Party Service

Federated Identity Management (FIdM)

- Applies SSO on a wider scale; cross-organization/domain
- Trusted authority for digital identities across multiple organizations
- Microsoft Account, Google Account, Facebook, Twitter, etc.
- SAML, Oauth, OpenID, etc.
- SAML is an XML-based framework for exchanging security information, including authentication data. [*More later*]

FIDM and SSO are not synonymous.

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Practice Question

Which of the following statements about single sign-on (SSO) is not true?

A. A user can sign on a system once and access other systems without re-authentication

B. An SSO user account causes more serious impact then non-SSO if breached

C. Systems require federation protocols to support SSO

D. A user can create multiple user accounts across systems that support SSO

Domain 5: Identity and Access Management

Manage Identification and Authentication of People, Devices, and Services

Practice Question

Which of the following statements about single sign-on (SSO) is not true?

A. A user can sign on a system once and access other systems without re-authentication

B. An SSO user account causes more serious impact then non-SSO if breached

C. Systems require federation protocols to support SSO

D. A user can create multiple user accounts across systems that support SSO

Domain 5: Identity and Access Management

Federated Identity with a Third-Party Service

Identity as a Service (IDaaS)

- A cloud-based subscription model for IAM, where identity and access services are rendered over the internet by a third-party provider rather than deployed on-premises. (Ping Identity)
- Gartner Inc., divides IDaaS services into two categories:
  - Web access software for cloud-based applications such as software as a service (SaaS)
  - Web-architected applications; and cloud-delivered legacy identity management services.

(Reference)

Domain 5: Identity and Access Management

Federated Identity with a Third-Party Service

Identity as a Service (IDaaS)

Risks

- Single point of failure
- Loss of control

Types

- On-prem – LDAP, Microsoft AD
- Cloud (cloud-native)
  - IAM broker
  - Just in time (JIT) provisioning
- Hybrid
  - Dual IAM implementation
  - Microsoft AD & AzureAD

Domain 5: Identity and Access Management

Federated Identity with a Third-Party Service

- IdP = Identity Provider
- SP = Service Provider

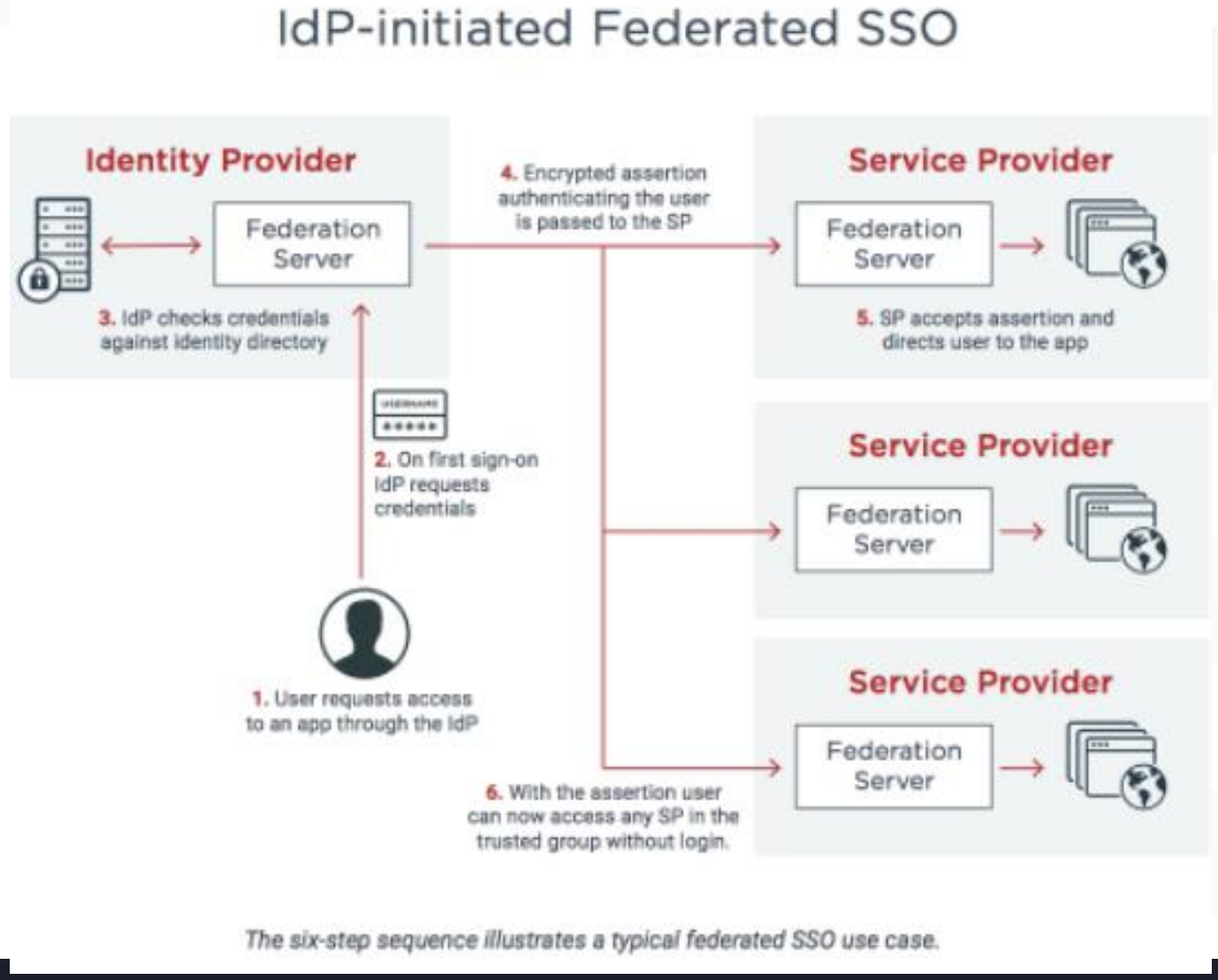


Image Source: https://www.pingidentity.com/en/resources/blog/posts/2021/sso-vs-federated-identity-management.html

New Topic!

Domain 5: Identity and Access Managem

Implement and Manage Authorization Mechanisms (aka Access Control Models)

- Role-Based Access Control (RBAC)
- Rule-Based Access Control (RuBAC)
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Attribute-Based Access Control (ABAC)
- Risk-Based Access Control

Do not think of one model being better than another.
Each model is used for a specific information security purpose.

Domain 5: Identity and Access Management

Implement and Manage Authorization Mechanisms

Role-Based Access Control (RBAC)

- Defines how information is accessed on a system based on the role of the subject
- Subjects are grouped into roles and each defined role has access permissions based upon the role, not the individual
- Keeps each role separate on the system and reduces the exposure of more sensitive accounts
- RBAC is a type of non-discretionary access control because users do not have discretion regarding the groups of objects they are allowed to access, and are unable to transfer objects to other subjects
- See NIST: http://csrc.nist.gov/rbac & https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

Domain 5: Identity and Access Management

Implement and Manage Authorization Mechanisms

Rule-Based Access Control (RuBAC)

- Based on a list of predefined rules to determine authorization
- Information systems often implement RuBAC via an access control list (ACL)
- Implement the concepts of implicit and explicit permissions
- Content and Context-Dependent Access Controls

Domain 5: Identity and Access Management

Implement and Manage Authorization Mechanisms

Mandatory Access Control (MAC)

See Chapter 3 Models

- System-enforced access control based on subject's clearance and object's labels
- Subjects and Objects have clearances and labels, respectively, such as confidential, secret, and top secret
- A subject may access an object only if the subject's clearance is equal to or greater than the object's label
- Subjects cannot share objects with other subjects who lack the proper clearance, or "write down" objects to a lower classification level such as from top secret to secret)
- Usually focused on preserving the confidentiality of data
- Expensive and difficult to implement - Clearing users is an expensive process

Domain 5: Identity and Access Management

Implement and Manage Authorization Mechanisms

Discretionary Access Control (DAC)

- Gives subjects full control of objects they have been given access to, including sharing the objects with other subjects
- Subjects are empowered and control their data
- Standard UNIX and Windows operating systems use DAC for filesystems
- If a subject makes a mistake, such as attaching the wrong file to an email sent to a public mailing list, loss of confidentiality can result
- Mistakes and malicious acts can also lead to a loss of integrity or availability of data

Domain 5: Identity and Access Management

Implement and Manage Authorization Mechanisms

Attribute-Based Access Control (ABAC)

- Policy-based access control
- Combines attributes about the subject and evaluates them against a policy to make an access control decision
- Examples: Time of day, Location
- Cyber example: Firewall rules

Domain 5: Identity and Access Management

Implement and Manage Authorization Mechanisms

Risk-Based Access Control (RBAC)

- Dynamic access control using a variety of parameters to determine authorization.
- Utilize a number of factors to dynamically define authentication requirements.
- Integrate threat intelligence data and make dynamic authentication decisions.
- Cyber example: IDS/IPS

Domain 5: Identity and Access Management

Mana
Provi

New Topic!

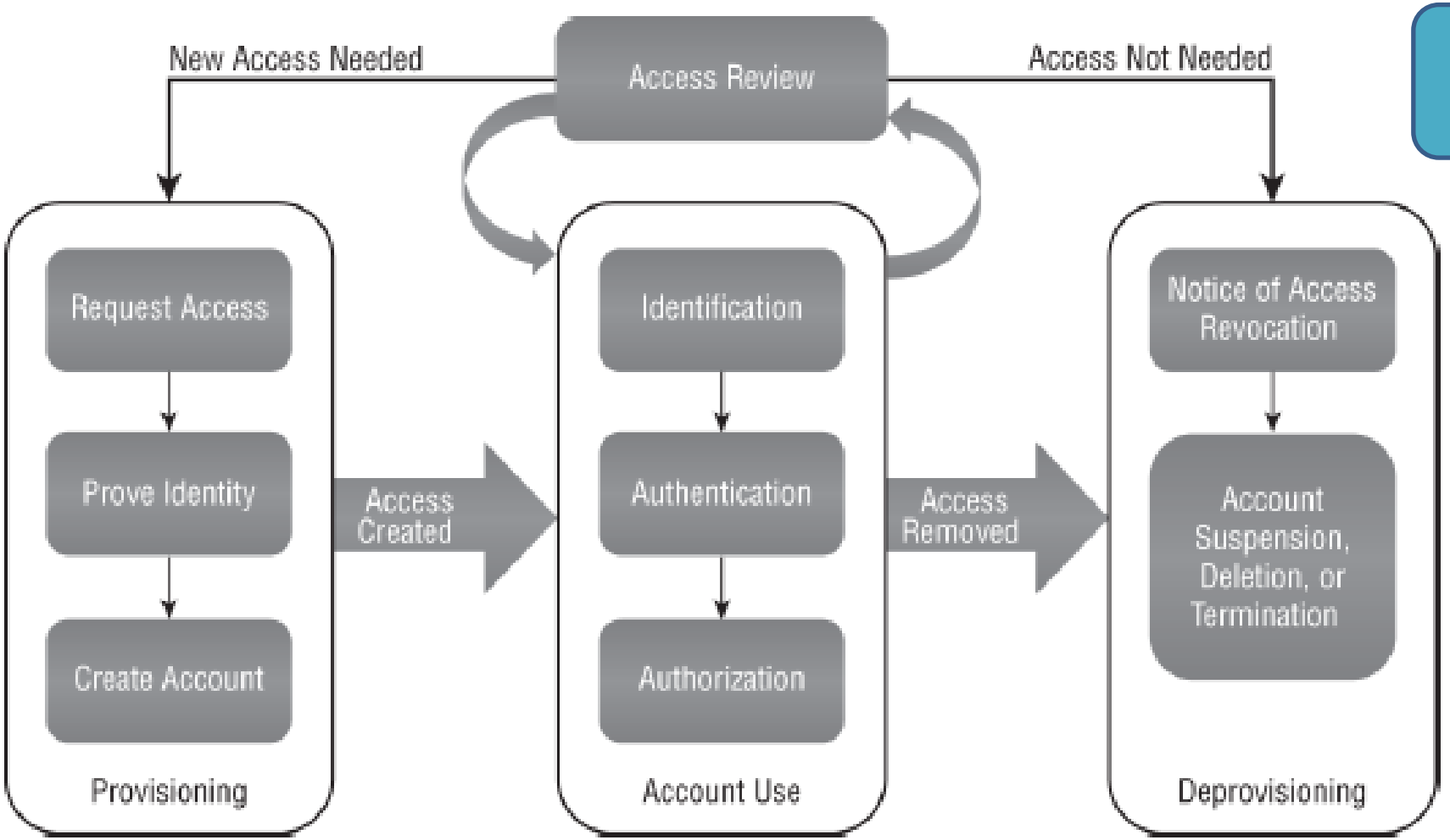


FIGURE 5.1 The access management lifecycle

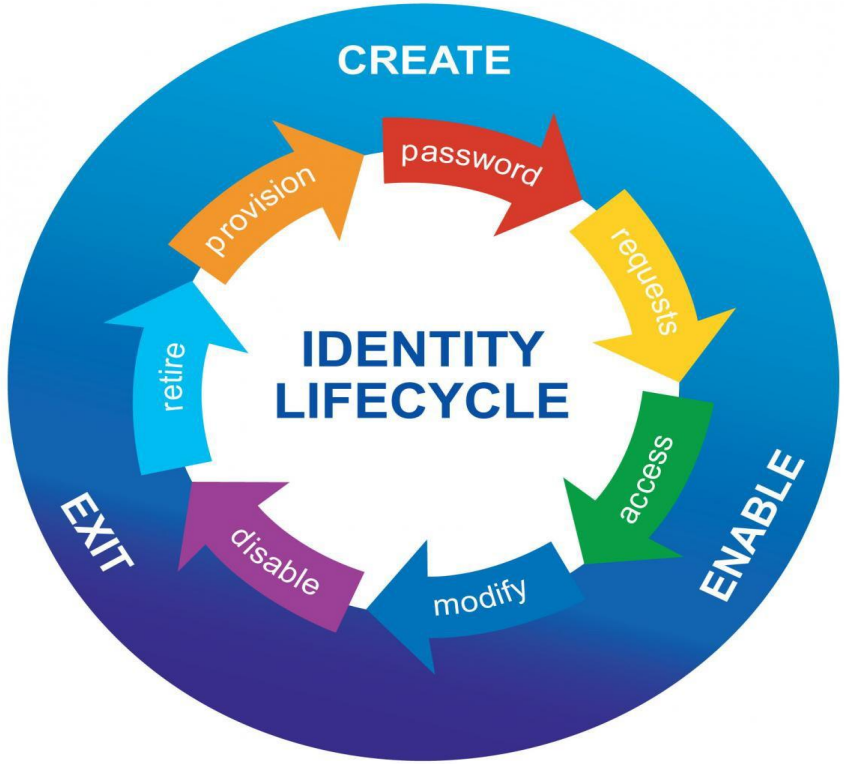
CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Identity & Access Lifecycle

Review from earlier

- Provisioning
  - Requesting identity creation & approval process(es)
  - Begins before a subject attempts to access an object
- Deprovisioning
  - Temporary suspension
  - Disabling
  - Deleting



CISSP® MENTOR PROGRAM – SESSION EIGHT

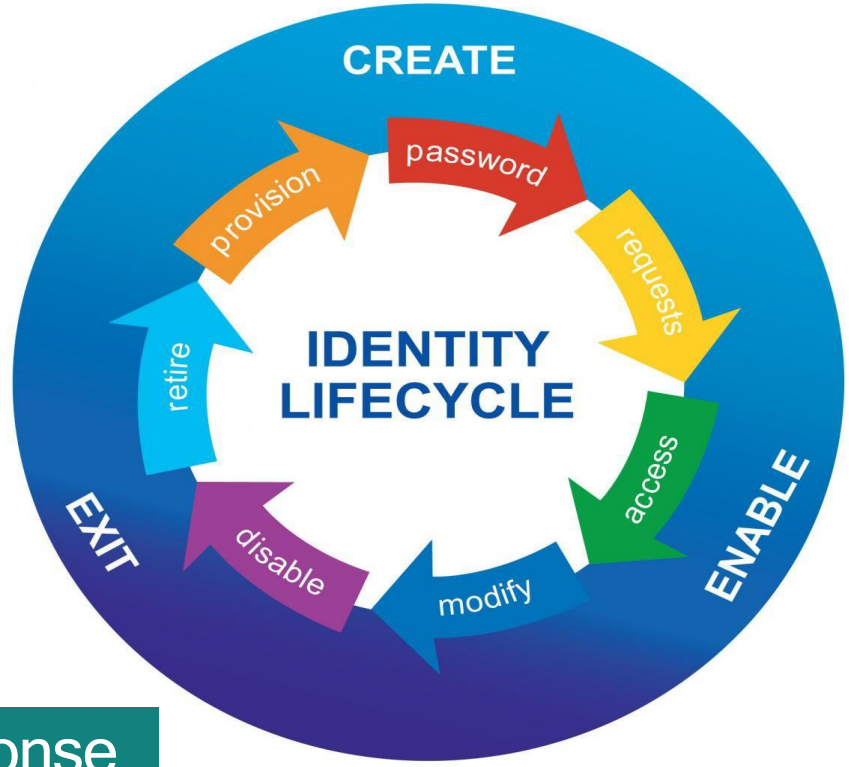
Domain 5: Identity and Access Management

Identity & Access Lifecycle

Review from earlier

Account Access Review

- Include identifying what systems, data, and permissions a user is granted
- Cadence – How often
  - General user
  - Admins
  - System accounts
- Permission Creep
- Automate! (SOAR, SIRM)



SOAR = Security Orchestration, Automation, and Response

Domain 5: Identity and Access Management

Identity & Access Lifecycle

Deprovisioning Risks

- Hostile or involuntary circumstances include a staff member being let go at the company's decision.
- Friendly or voluntary circumstances include a staff member resigning or retiring and generally carry less risk.
- Job changes are treated by some high-security organizations the same as a friendly deprovisioning as an extra precaution.

Beware of self-provisioning / deprovisioning...

Domain 5: Identity and Access Management

Identity & Access Lifecycle

Privilege Escalation

- Temporary access
- Allows end-users to install / update approved software as administrator
- Production Control - *Break-the-glass* process – Specific users given access to production systems to update or fix issues. Part of change control.
- Examples:
  - Linux/Unix: `sudo`
  - Windows: UAC

Domain 5: Identity and Access Management

Implement Authentication Systems

New Topic!

Federated Identity Management (FIdM) & Identity as a Service (IDaaS)

- Open Authorization (OAuth) / OpenID Connect
- Security Assertion Markup Language (SAML)
- Kerberos
- RADIUS / TACACS+

See 2021 Video for more information:
https://youtu.be/G5YSeFYqKB8

Domain 5: Identity and Access Management

Implement Authentication Systems

Open Authorization (Oauth)

An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications.

IETF RFC 6749 (https://datatracker.ietf.org/doc/html/rfc6749)

OAuth Community Site (https://oauth.net/)

OAuth 2.0 Simplified (https://www.oauth.com/)

Domain 5: Identity and Access Management

Implement Authentication Systems

Open Authorization (Oauth)

Four key roles that systems in an ***Oauth federation*** must implement to exchange authorization information:

- ***Resource owner***: Any entity that grants access to a protected resource, such as an information system or dataset.
- *Resource server*: Any server hosting the protected resource, which accepts and responds to access requests.
- ***Client***: Any application making requests for access to protected resources.
- ***Authorization server***: Any server issuing access tokens to clients after successful authentication; tokens are used across the federated system to gain access.

Domain 5: Identity and Access Management

Implement Authentication Systems

OpenID Connect

- Authentication functions built on top of OAuth version 2.0 and federates identity management.
- Similar to SSO
- Implemented on Web Applications – given a choice of Identity Providers (Google, Facebook, Microsoft, etc.)

Key steps of OIDC authentication (developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauthand-oidc)

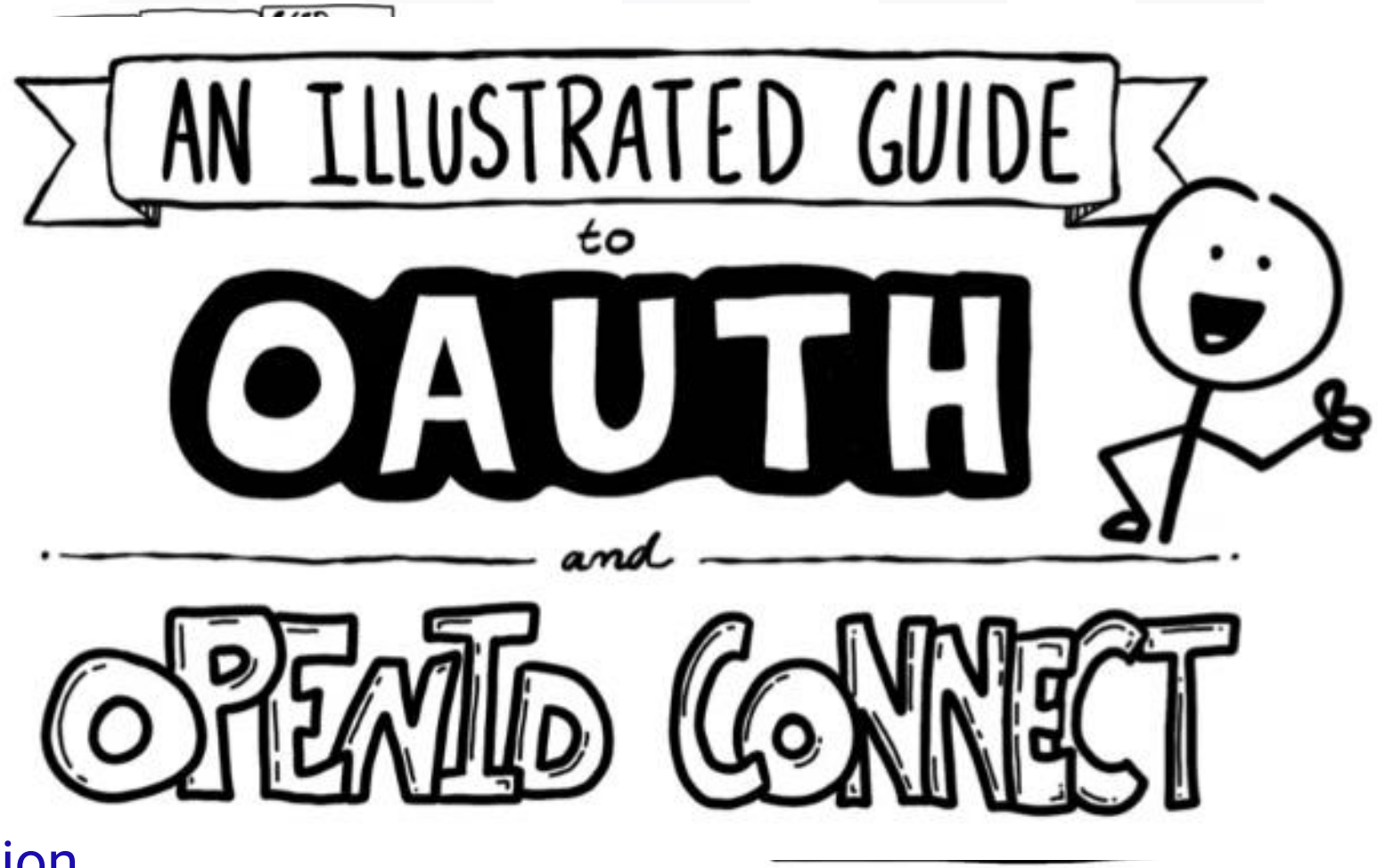
Domain 5: Identity and Access Management

Implement Authe

OpenID Connect

- Authentication fun
  federates identity r
- Similar to SSO
- Implemented on W
  Providers (Google,

GO RIGHT NOW!



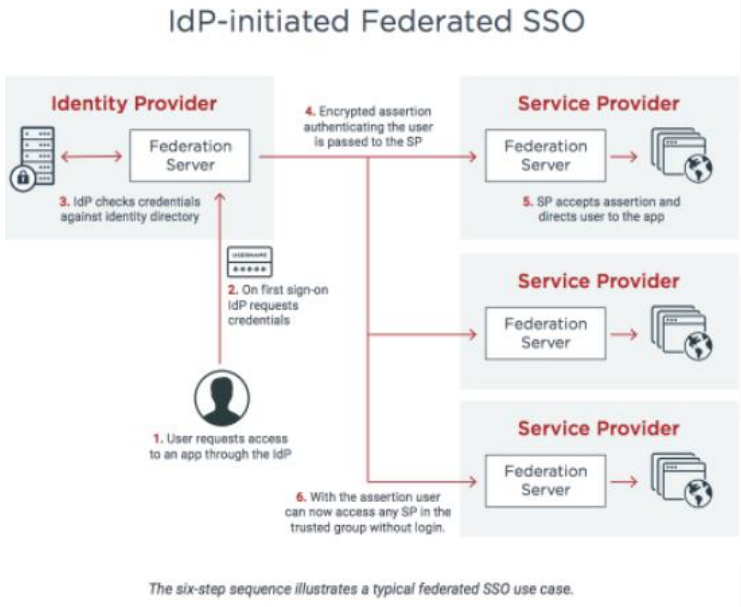
Key steps of OIDC authentication (developer.okta.com/blog/2019/10/21/illustrated-guide-to-oauthand-oidc)

Domain 5: Identity and Access Management

Implement Authentication Systems

Security Assertion Markup Language (SAML)

- An eXtensible Markup Language (XML)-based framework to format messages regarding identities, resources, and access information like authentication and authorization
- Current version: 2.0
  [OASIS Standard]
- Three Roles:
  - User Agent (UA)
  - Service Provider (SP)
  - Service Provider (IdP)



Slide 95

Domain 5: Identity and Access Management

Implement Authentication Systems

Security Assertion Markup Language (SAML)

Four components:

- ***Assertions*** define SAML attributes - how authentication and authorization message protocols or frameworks are to be used by the services.
- ***Bindings*** define the request-response pairs to be used by the three roles to communicate.
- ***Protocols*** include HTTP and simple object access protocol (SOAP), which are used to package and exchange messages between roles.
- ***Profiles*** are the combination of assertions, bindings, and protocols in use within a specific SAML implementation.

OASIS SAML v2.0 Standard (https://wiki.oasis-open.org/security/FrontPage)

Domain 5: Identity and Access Management

Implement Authentication Systems

Kerberos

- A third-party authentication service that may be used to support Single Sign-On
- Kerberos (https://web.mit.edu/kerberos/) was the name of the three-headed dog that guarded the entrance to Hades (also called Cerberus) in Greek mythology (and Harry Potter)
- The three heads of the mythical Kerberos were meant to signify the three “A”s of AAA systems:
  - authentication,
  - authorization, and
  - accountability

Highly Testable

Domain 5: Identity and Access Management

Implement Authentication Systems

Kerberos

- A third-party authentication service that may be used to support Single Sign-On
- Kerberos (https://web.mit.edu/kerberos/) was the name of the

What is Kerberos?

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.

The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerab Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.

Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure than a computer which is not connected to the network --- and powered off!) In many places, these restriction are simply unrealistic and unacceptable.

Kerberos was created by MIT as a **solution to these network security problems**. The Kerberos protocol uses **strong cryptography** so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove th identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Kerberos is freely available from MIT, under copyright permissions very similar those used for the BSD operating system and the X Window System. MIT provides Kerberos in source form so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy. In addition, for those who prefer to rely on a professionally supported product, Kerberos is available as a product from many different vendors.

In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture.

- accountability

Highly Testable

Domain 5: Identity and Access Management

Implement Authentication Systems

Kerberos

Kerberos FAQ (http://www.faqs.org/faqs/kerberos-faq/user/)

- Kerberos is a network authentication system for use on physically insecure networks
- Based on the key distribution model presented by Needham and Schroeder
- Allows entities communicating over networks to prove their identity to each other while preventing eavesdropping or replay attacks
- Provides for data stream integrity (detection of modification) and secrecy (preventing unauthorized reading) using cryptography systems such as DES (Data Encryption Standard)

Domain 5: Identity and Access Management

Implement Authentication Systems

Kerberos

- Uses secret key encryption
- Provides mutual authentication of both clients and servers
- Protects against network sniffing and replay attacks
- Current version of Kerberos is version 5, described by RFC 4120 (http://www.ietf.org/rfc/rfc4120.txt)
  14 Mar 2022 – krb5-1.19.3 (as of this recording)

Domain 5: Identity and Access Management

Implement Authentication Systems

Kerberos Components

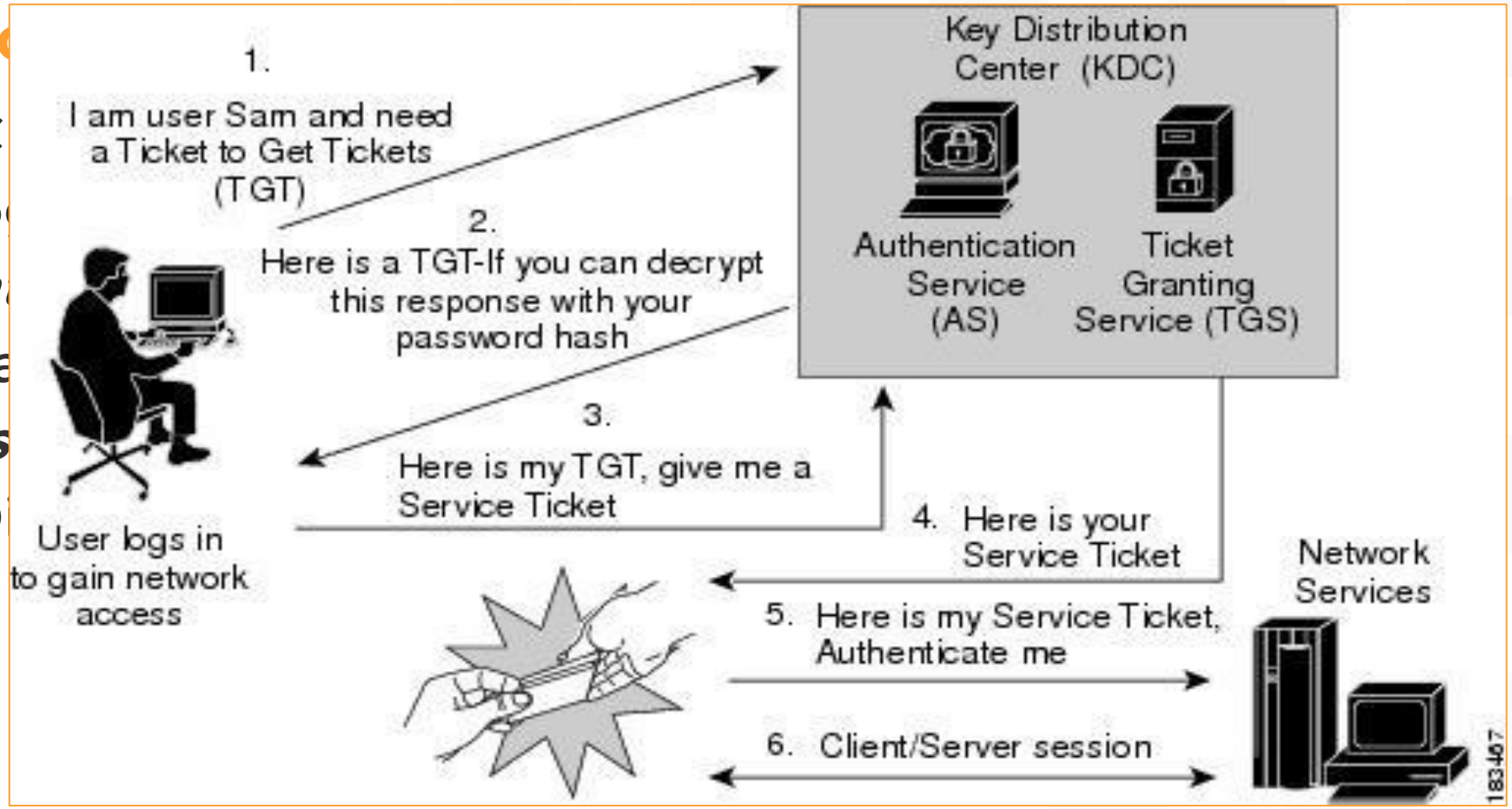
- ***Principal***: Client (user) or service
- ***Realm***: A logical Kerberos network
- ***Authentication Server*** (AS): Authenticating principles
- ***Ticket***: Data that authenticates a principal's identity
- ***Credentials***: a ticket and a service key
- ***KDC***: Key Distribution Center, which authenticates principals
- ***TGS***: Ticket Granting Service
- ***TGT***: Ticket Granting Ticket
- ***C/S***: Client Server, regarding communications between the two

Domain 5: Identity and Access Management

Implement Authentication Systems

Kerberos C

- ***Principal***: C
- ***Realm***: A lo
- ***Authentica***
- ***Ticket***: Data
- ***Credentials***
- ***KDC***: Key D
- ***TGS***: Ticket
- ***TGT***: Ticket
- ***C/S***: Client



Domain 5: Identity and Access Management

Implement Authentication Systems

Kerberos

Strengths

- Provides mutual authentication of client and server
- If a rogue KDC pretended to be a real KDC, it would not have access to keys
- mitigates replay attacks (where attackers sniff Kerberos credentials and replay them on the network) via the use of timestamps

Weaknesses

- A compromise of the KDC (physical or electronic) can lead to the compromise of every key in the Kerberos realm
- KDC and TGS are single points of failure: if they go down, no new credentials can be issued
- Replay attacks
- Any user may request a session key for another user
- Kerberos does not mitigate a malicious local host: plaintext keys may exist in memory or cache

Domain 5: Identity and Access Management

Implement Authentication Systems

Remote Authentication Dial In User Service (RADIUS)

- Originally designed in the 1990s
- A third-party authentication system
- Uses the User Datagram Protocol (UDP) ports:
  - 1812 (authentication) and
  - 1813 (accounting)
- Specified in IETF RFC 2865, https://datatracker.ietf.org/doc/html/rfc2865

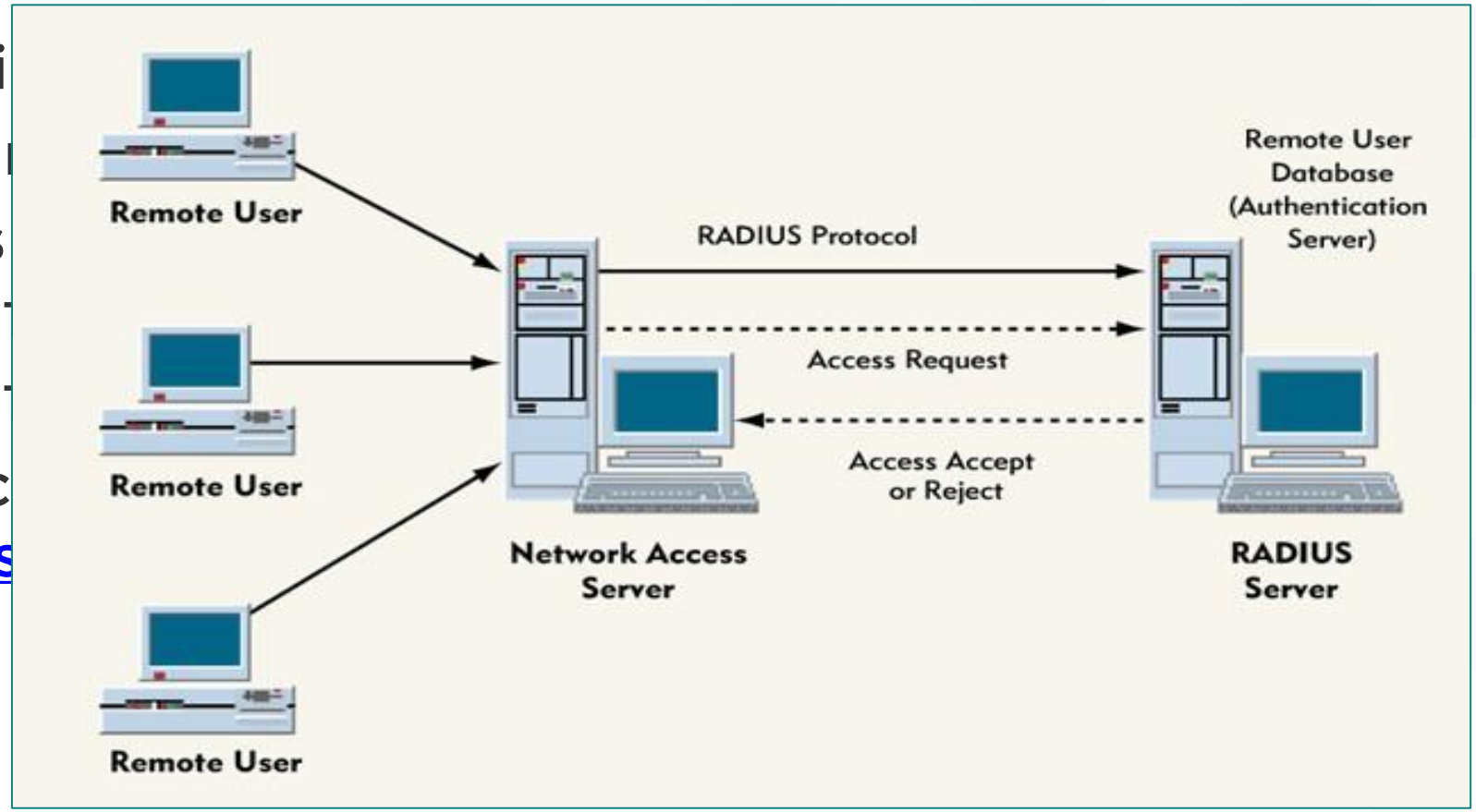
Evan talked about this last session, sooooooo….

Domain 5: Identity and Access Management

Implement Authentication Systems

Remote Authentication Dial In User Service (RADIUS)

- Origi
- A thi
- Uses
  - 18
  - 18
- Spec
  https

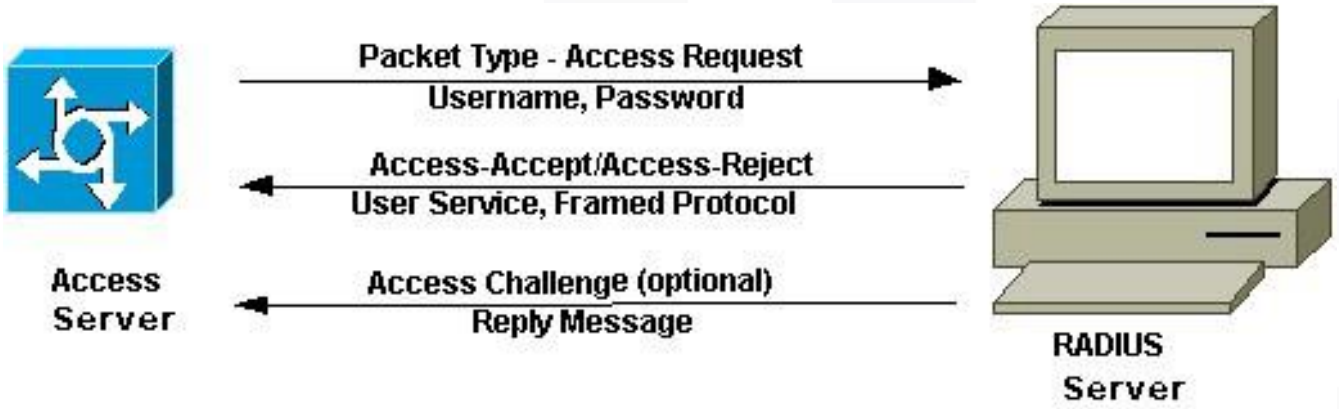


Domain 5: Identity and Access Management

Implement Authentication Systems

Remote Authentication Dial In User Service (RADIUS)

- Request and response data is carried in Attribute Value Pairs (AVPs)
- According to RFC 2865 (http://tools.ietf.org/html/rfc2865), RADIUS supports the following codes:
  - Access-Request
  - Access-Accept
  - Access-Reject
  - Accounting-Request
  - Accounting-Response
  - Access-Challenge
  - Status-Server (experimental)
  - Status-Client (experimental)



Domain 5: Identity and Access Management

Implement Authentication Systems

Terminal Access Controller Access Control System (TACACS+)

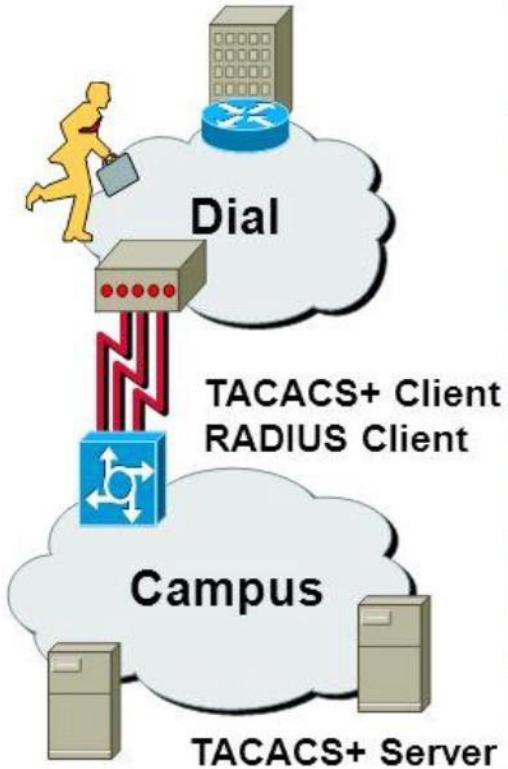
- Centralized access control system that requires users to send an ID and static (reusable) password for authentication
- TACACS uses UDP port 49 (and may also use TCP)
- Reusable passwords have security vulnerability: the improved TACACS+ provides better password protection by allowing two-factor strong authentication
- TACACS+ is not backwards compatible with TACACS
- TACACS+ uses TCP port 49 for authentication with the TACACS+ server
- The actual function of authentication is similar to RADIUS
- RADIUS only encrypts the password (leaving other data, such as username, unencrypted); TACACS+ encrypts all data below the TACACS+ header
- Specified in IETF RFC 8907 at datatracker.ietf.org/doc/html/rfc8907.

Domain 5: Identity and Access Management

Implement Authentication Systems

Terminal Access Controller Access Control System (TACACS+)

- Centralized a
(reusable) pa
- TACACS uses
- Reusable pas
better passw
- TACACS+ is n
- TACACS+ use
- The actual fu
- RADIUS only
unencrypted
- Specified in I



	TACACS+	RADIUS
Functionality	Separates AAA	Combines Authentication and Authorization
Transport Protocol	TCP	UDP
Challenge/ Response	Bidirectional	Unidirectional
Protocol Support	Full Support	No ARA No NetBEUI
Confidentiality	Entire Packet-Encrypted	Password-Encrypted

Domain 5: Identity and Access Management

Implement Authentication Systems

Federated Identity Management (FIdM) & Identity as a Service (IDaaS)

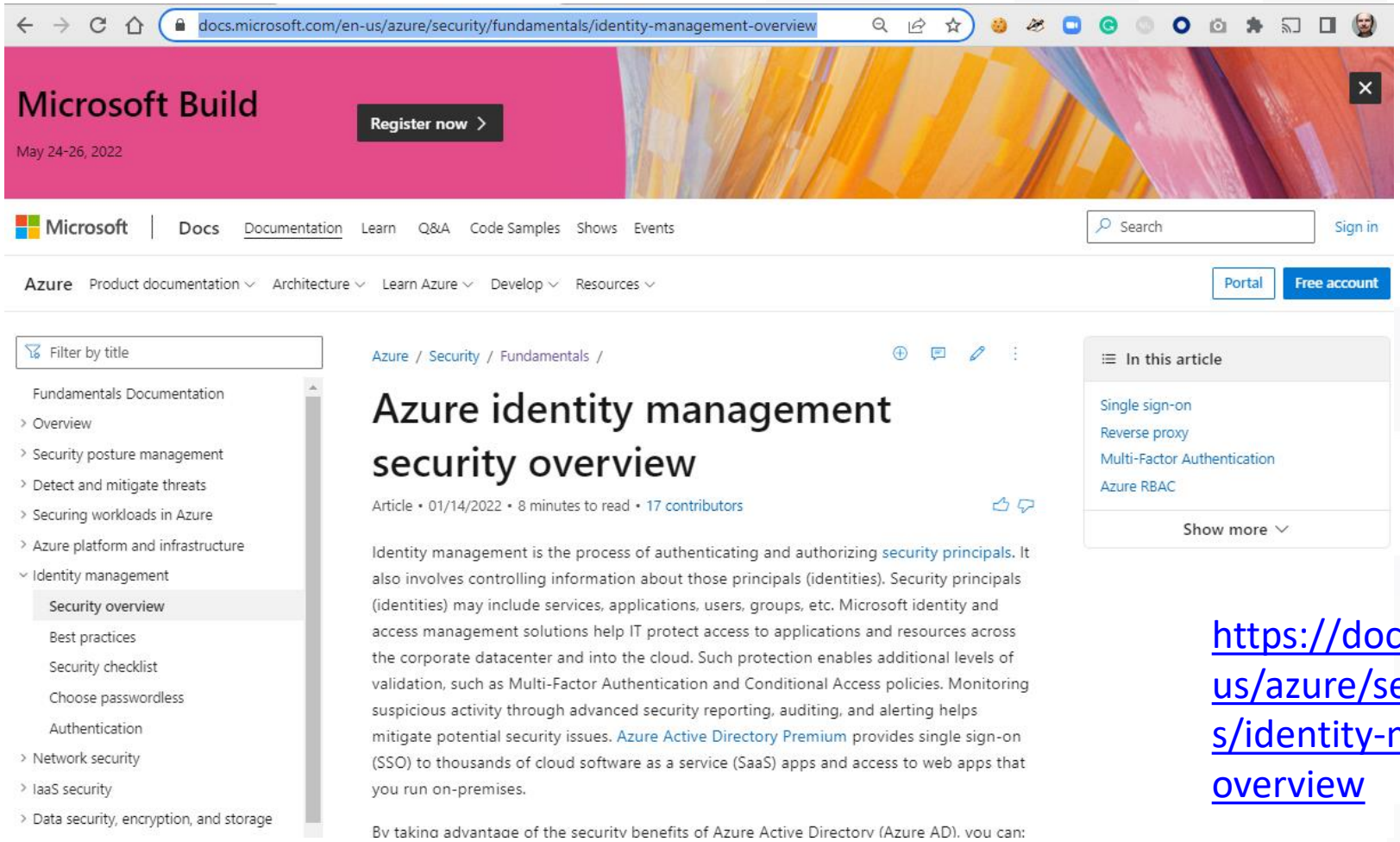
- Open Authorization (OAuth) / OpenID Connect
- Security Assertion Markup Language (SAML)
- Kerberos
- RADIUS / TACACS+

See 2021 Video for more information:
https://youtu.be/G5YSeFYqKB8

CISSP® MENTOR PROGRAM – SESSION EIGHT

Domain 5: Identity and Access Management

Bringing it home



https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview

CISSP® MENTOR PROGRAM – SESSION EIGHT

DOMAIN 5: Identity and Access Management

YAY!
Another Domain done!

Topics:

- Control Physical and Logical Access to Assets
- Manage Identification and Authentication of People, Devices, and Services
- Federated Identity
- Implement and Manage Authorization Mechanisms
- Manage the Identity and Access Lifecycle
- Implement Authentication Systems

pp. 377-418

Questions on Domain 5?

CISSP® MENTOR PROGRAM – SESSION EIGHT

SESSION 8 - FIN

We made it!

Next Session (Monday, 16 May 2022) – Domain 6 (Security Assessment & Testing)

- Design and Validate Assessment, Test, and Audit Strategies
- Conduct Security Control Testing
- Collect Security Process Data
- Analyze Test Output and Generate Report
- Conduct or Facilitate Security Audits

SESSION 8 - FIN

Homework:

Review Domains 1-5.

Take practice tests.

Review at least two of the references we provided in this class (download for later use).

Post at least one question/answer in the Slack Channel.

See you Monday!

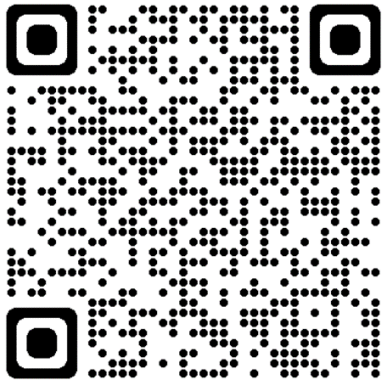
WHOAMI

Ron Woerner, CISSP, CISM

- Chief Security Officer, Cyber-AAA
- Cybersecurity Professor, Bellevue University

https://linktr.ee/cyberron

https://www.linkedin.com/in/ronwoerner/



@ronw123

Hackers Wanted
TEDx Omaha

2022

Class #8 – Domain 5

Ron Woerner

Cyber-AAA Founder & CEO & vCISO
Bellevue University CyberSecurity Studies Professor