Chapter 10:
Authentication and Access Control

Outline

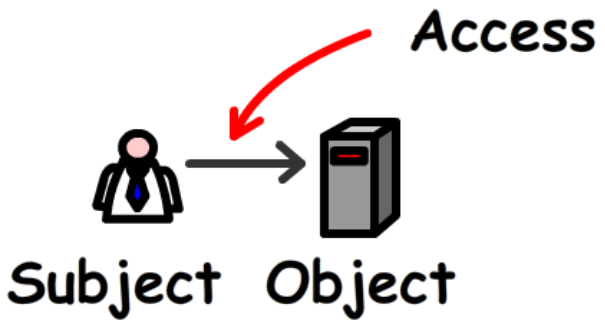
- Overview of access control
- Authentication and Authorization
- Identification and authentication techniques
- Access control techniques
- Access control methodologies, implementations and administration

Access Controls

- Access control is a security technique that regulates who or what can view or use resources in a computing environment.
- It permits management to specify
  - what users can do,
  - which resources they can access, and
  - what operations they can perform on a system.

Access Control: Overview

- Access Controls: The security features that control how users and systems communicate and interact with one another.
- Access: The flow of information between subject and object
- Subject: An active entity that requests access to an object or the data in an object
- Object: A passive entity that contains information
- Security Principle
  - CIA Traid



Identification, Authentication, and Authorization

Identification, Authentication, and Authorization are distinct functions.

- Identification
  - Method of establishing the identity of subject's (user, program, process).
- Authentication
  - Method of proving the identity.
- Authorization
  - Determines whether the proven identity has the right to access the requested resources not.

Identification

Identification

- Method of establishing the identity of subject's (user, program, process).
  - Use of user name or other public information.
  - Know identification component requirements.
    - Each value should be unique, for user accountability;
    - A standard naming scheme should be followed;
    - The value should be non-descriptive of the user's position or tasks.

Authentication

Authentication

- Method of proving the identity.
- Knowledge -Something you know, such as a password, passphrase or PIN.
- Ownership -For example, tokens and Smart cards.
- Characteristics -Biometrics are digitized representations of physical features (such as fingerprints) or physical actions (such as signatures).

Strong Authentication is important

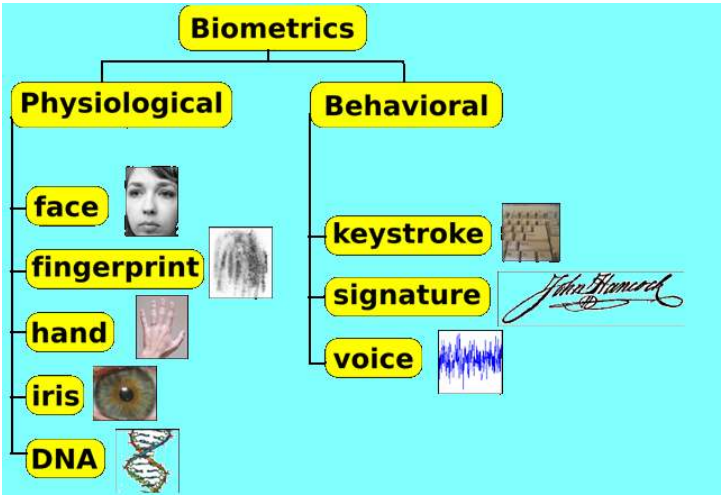
- Multi-factor authentication
  - two-or three-factor authentication



Authentication

Biometrics

- Verifies an identity by analyzing a unique person attribute or behavior (e.g., what a person "is").
- Most expensive way to prove identity, also has difficulties with user acceptance.
- Many different types of biometric systems



Authentication

Biometric systems can be hard to compare.

Type I Error: False rejection rate.

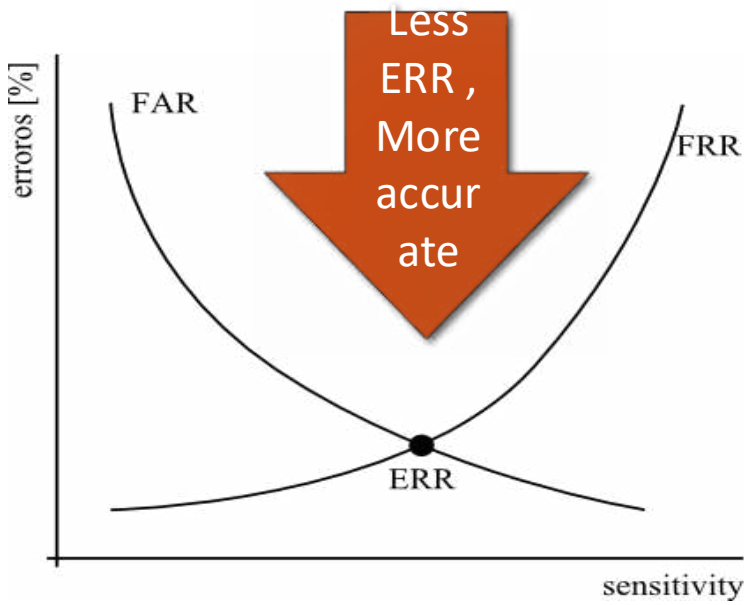
- When a biometric system rejects an authorized individual

Type II Error: False acceptance rate.

- When a biometric system accepts an individual, who should have been rejected
- This is an important error to avoid.

Crossover Error Rate

- Rating stated as a percentage and represents the point at which **the false rejection rate equals the false acceptance rate**.



Authentication

Passwords

- most common identification, authentication scheme.
- Weak security mechanism, must implement strong password protections (**password complexity**)

Techniques to attack passwords

- Electronic monitoring
- Access the password file
- Brute Force Attacks
- Dictionary Attacks
- Social Engineering

Authentication

One Time Passwords (aka Dynamic Passwords)

- Used for authentication purposes.
- This type of system is not vulnerable to electronic eavesdropping, sniffing, or password guessing.

Two types of Token Devices (aka Password Generator)

- Synchronous
  - Time Based
    - Token generate the OTP in synch with server
- Asynchronous
  - Challenge based authentication
    - Server sends a challenge value.
    - user should enter the challenge value to token to generate OTP, then send to server.



Authorization

Authorization

- Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.
- Granting access rights to subjects should be **based on the level of trust** a company has in a subject and the subject's need to know.
- Is a core component of every operating system and established whether a user is authorized to access a particular resource and what actions he is permitted to perform on the resource

Authorization

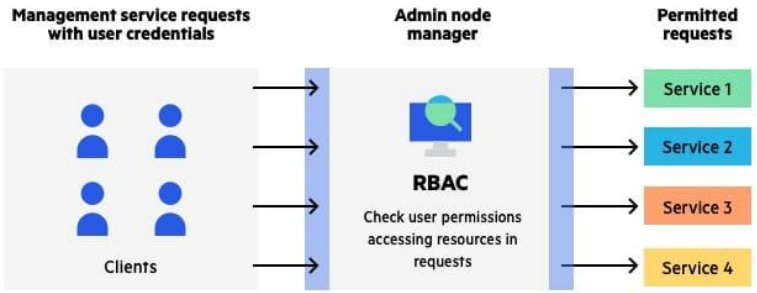
Access Criteria can be thought of as:

- **Roles**
  - Is an efficient way to assign rights to a type of user who performs a certain task. (job assignment or function: managers, clerks, cashiers, supervisors, etc.)
- **Groups**
  - When several users require same type of access to information and resources
- **Location**
  - To restrict unauthorized individuals from being able to get in and reconfigure the server remotely.
- **Time**
  - Restrict the times that certain actions or services can be accessed.
- **Transaction Types**
  - Can be used to control what data is accessed during certain types of functions and what commands can be carried out on the data.

Authorization

Authorization concepts to keep in mind:

- **Authorization Creep**
  - When new access rights and permissions assigned to employee without the old permissions being reviewed and removed.
- **Default to Zero**
  - All access controls should be based on the concept of starting with zero access and then building on top of that.
- **Need to Know Principle**
  - individuals should be given access only to the information that they absolutely require in order to complete their job duties.
- **Access Control Lists**
  - A list of subjects that are authorized to access a particular object.



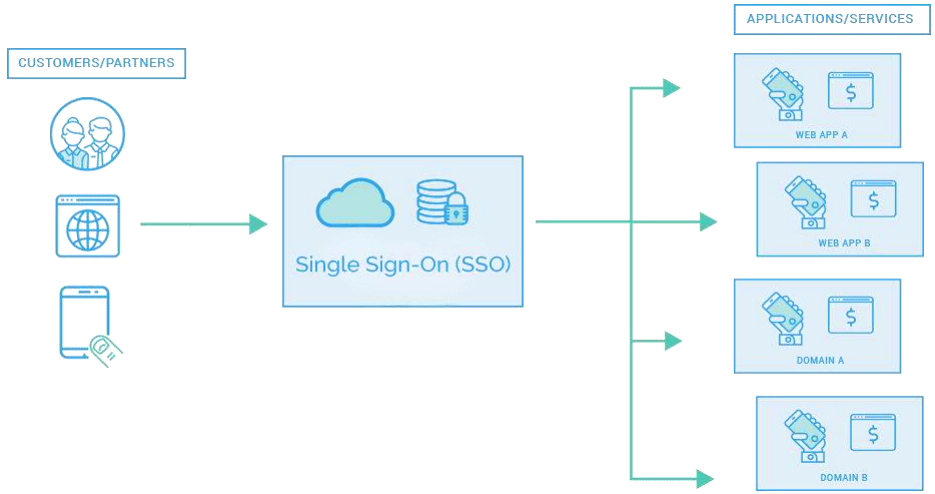
Authorization

Single Sign On (SSO) Capabilities

- Allow user credentials to be entered one time and the user is then able to access all resources in primary and secondary network domains

SSO technologies include:

- Kerberos
- Sesame
- Security Domains
- Directory Services
- Dumb Terminals



SSO Process

- SSOs enable users to logon to the **authentication server** and still obtain access to all additional authorized networked systems without additional identification and authentication.
- SSO is also referred to as reduced sign-on, and is used in web-based environments **in federated ID management systems**.



SSO : Pros and Cons

Pros :

- **Efficient log-on process** -The user logs on only once to access all authorized systems.
- **Encourages users to create stronger passwords** -With only one password to remember and control, users may be inclined to use passwords that are harder and more difficult to crack. Fewer passwords to manage should also result in fewer being written down in unsafe locations.
- **Centralized administration** -Ensures consistent application of policy and procedures.

Cons :

- **Single point of compromise** -A single compromised sign-in allows the intruder into all of the account owner‟s authorized resources.
- **Legacy Interoperability**-It may be difficult to include unique computers or legacy systems in the single sign on network.
- **Implementation difficulties**-Unusual types of systems may not interface well with SSO software.

Access Control Models

Three Main Types

- Discretionary (Unrestricted)
- Mandatory
- Non-Discretionary (Role Based)

Discretionary Access Control (**DAC**)

- A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.
- **Access control is at the discretion of the owner.**

Access Control Models

Mandatory Access Control (**MAC**)

- Access control is **based on a security labeling system**. Users have security clearances and resources have security labels that contain data classifications.
- ***This model is used in environments where information classification and confidentiality is very important*** (e.g., the military).

Non-Discretionary (Role Based) Access Control Models

- Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
- **Is the best system for an organization that has high turnover.**

Access Control Techniques

There are several different access controls and technologies available to support the different models.

- Rule Based Access Control
- Constrained User Interfaces
- Access Control Matrix

Access Control Techniques

Rule Based Access Control

- Uses specific rules that indicate what can and cannot happen between a subject and an object.
- Not necessarily identity based.
- Traditionally, rule based access control has been used in MAC systems as an enforcement mechanism.

```
Rule r1 (
   Subject S1 {attributes <'role' = 'Manager'>},
   Object O1,
   Action Read
) -> Accept

Rule r2 (
   Subject S2 {attributes <'role' = 'Employee'>},
   Object O1,
   Action Read
) -> Deny
```

- **FIREWALL**

```
Access(
    Subject S1 {attributes <'role' = 'Manager'>},
    Object O1,
    Action Read
)
```

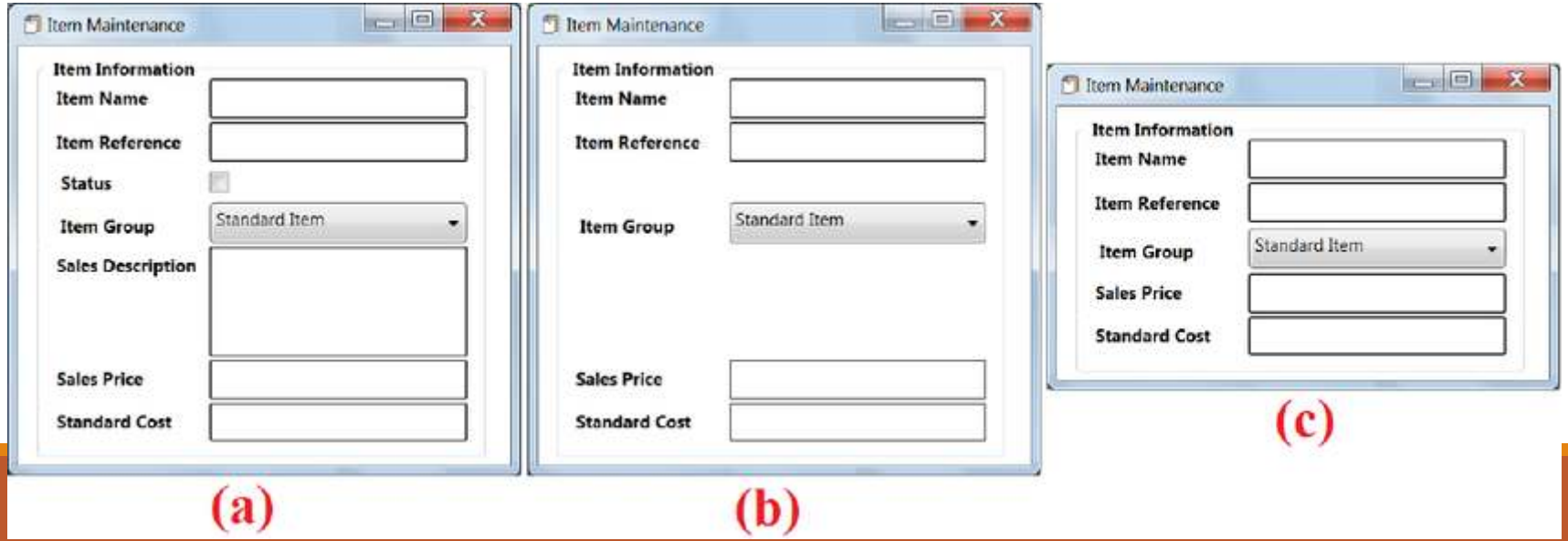
Access Control Techniques

Constrained User Interfaces

- Restrict user's access abilities by not allowing them certain types of access, or the ability to request certain functions or information

Three major types

- Menus and Shells
- Database Views
- Physically Constrained Interfaces



Access Control Techniques

Access Control Matrix

- Is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.
- Two types
  - Capability Table (bound to a subject)
  - Access Control List (bound to an object)

	O1	O2	O3	O4	O5	O6
S1	orw	r	rw	o	R	rwx
S2	r	orwx				r
S3	rwx			r	R	r

Access Control Matrix





	File 1	File 2	Obj.	Obj.
User	X		X	
User	X	X	X	X
Group		X		X
Subject		X		X

Object-Oriented Capability Table: Is a collection of access control lists implemented by comparing the column of objects to the rows of subjects.

Subject-Oriented Capability Table: Is a collection of access control lists implemented by comparing the column of users or subjects to their rights of access to protected objects.





	User	User	Group	Subject
File 1	X		X	
File 2	X	X	X	X
Folder 1		X		X
Object		X		X

Access Control Administration

Centralized Access Control Administration:

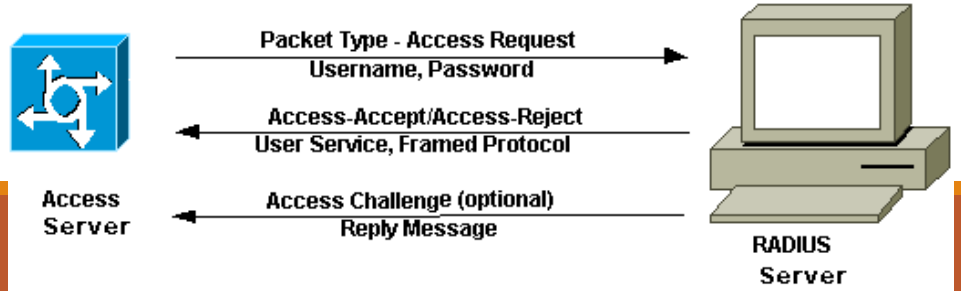
- One entity is responsible for overseeing access to all corporate resources.
- Provides a consistent and uniform method of controlling access rights.
  - Protocols: Agreed upon ways of communication
  - Attribute Value Pairs: Defined fields that accept certain values.

Types of Centralized Access Control

- Radius
- TACAS
- Diameter

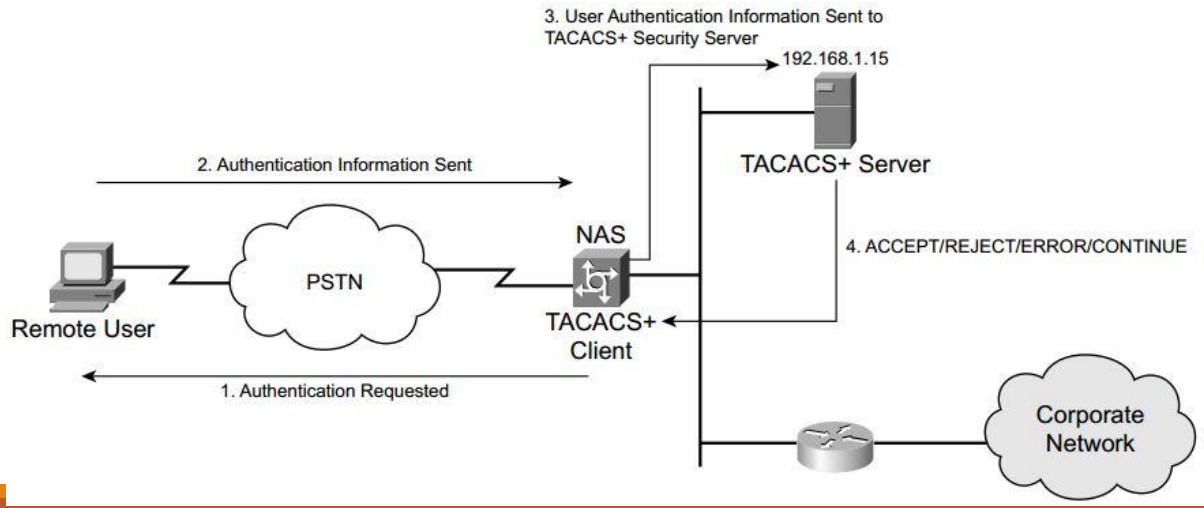
RADIUS

- **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice.
- Is a client/server authentication protocol and authenticates and authorizes remote users.
- **Most ISPs uses Radius to authenticate customers before they are allowed to access the Internet.**
- Radius is an open protocol and can be used in different types of implementations.
- Uses **UDP** as a transport protocol
- **Only encrypts the user's password** as it is being transmitted from Radius client to the radius server.
- Is appropriate protocol when simplistic username/password authentication can take place and users only need an "accept" or "deny" for obtaining access.



TACACS

- **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem
- Uses **TCP** as a transport protocol.
- **Encrypts all user data** and does not have the vulnerabilities that are inherent in the radius protocol.
- **Presents true AAA** (Authentication, authorization, and accounting) architecture.

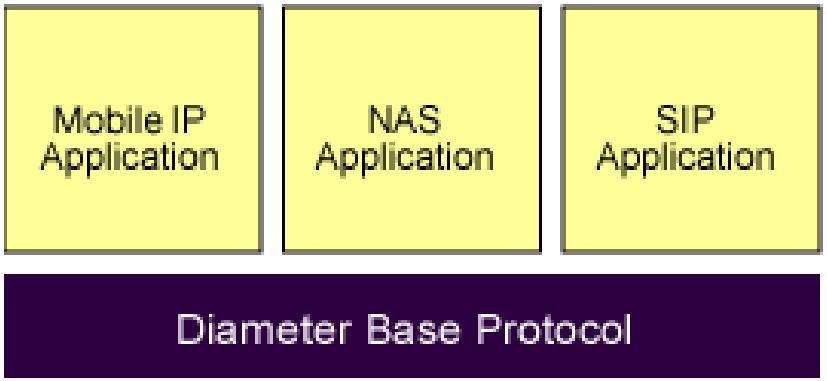


RADIUS vs. TACACS

	TACACS+	RADIUS
protocol and ports	TCP 49	UDP 1812, 1813
Encryption	Encrypts the entire packet, except the standard TACACS header.	Encrypts only the password field in the packet.
Authentication and authorization	Separates authentication from authorization so that they can be implemented on different security servers.	Combines authentication and authorization.

Diameter

- Protocol that has been developed to build upon the functionality of radius and overcome many of its limitations.
- It is an IETF standard defined in (RFC 3588)
- The various applications that require AAA functions can define their own extensions on top of the Diameter base protocol, and can benefit from the general capabilities provided by the Diameter base protocol.



Access Control Administration

Decentralized Access Control Administration:

- Gives control of access to the people who are closer to the resources
- Has no methods for consistent control, lacks proper consistency.

Accountability

Accountability is tracked by recording user, system, and application activities.

Audit information must be reviewed

- Event Oriented Audit Review
- Real Time and Near Real Time Review
- Audit Reduction Tools
- Variance Detection Tools
- Attack Signature Tools

Accountability

Other accountability concepts

- **Keystroke Monitoring**
  - Can review and record keystroke entries by a user during an active session.
  - May have privacy implications for an organization

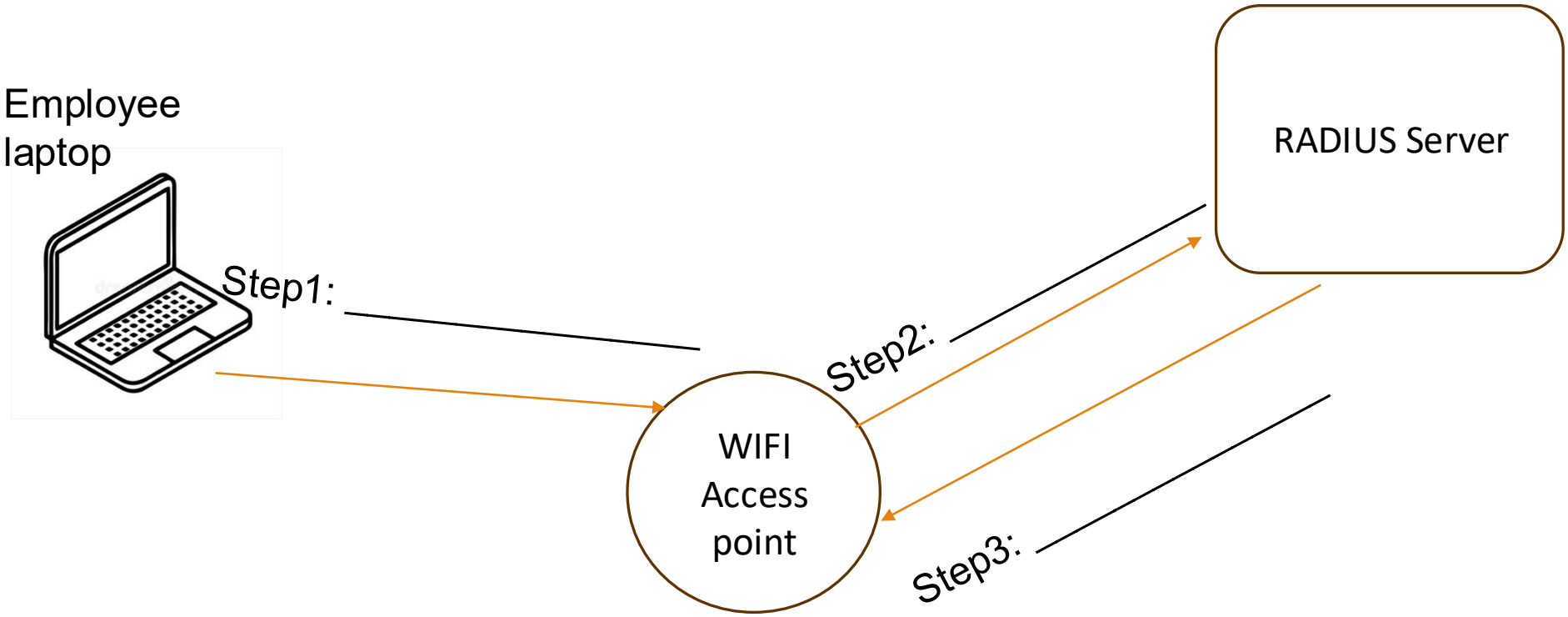
- **Scrubbing: Removing specific incriminating (unpleasant) data within audit logs**

Access Control Best Practices

Know the access control tasks that need to be accomplished regularly to ensure satisfactory security.

Best practices include:

- Deny access to anonymous accounts
- Enforce strict access criteria
- Suspend inactive accounts
- Replace default passwords
- Enforce password rotation
- Audit and review
- Protect audit logs


Employee
laptop
Step1:
WIFI
Access
point
Step2:
Step3:
RADIUS Server

Thank You !