Access Control

Domain 1

INFOSEC INSTITUTE

Overview

The access control domain addresses the concepts, methodologies, and techniques to manage access control; understand access control attacks; assess the effectiveness of implemented access controls; and helps to identify and access the provisioning lifecycle for access control.

Key Areas of Knowledge

A. Control access by applying the following concepts/ methodologies/ techniques

A.1 Policies

A.2 Types controls (preventative, detective, corrective, etc.)

A.3 Techniques (e.g., non-discretionary, discretionary and mandatory)

A.4 Identification and Authentication

A.5 Decentralized/distributed access control techniques

A.6 Authorization mechanisms

A.7 Logging and monitoring

Key Areas of Knowledge (continued)

B. Understand access control attacks

B.1 threat modeling

B.2 asset valuation

B.3 vulnerability analysis

B.4 access aggregation

C. Assess effectiveness of access controls

C.1 User entitlement

C.2 Access review & audit

D. Identify and access provisioning lifecycle (e.g., provisioning, review, revocation)

Agenda

- Control access by applying concepts/ methodologies/ techniques
- Understand access control attacks
- Assess effectiveness of access controls
- Identify and access provisioning lifecycle

Purpose of Access Control

Access Control Mechanisms

- Protect information and resources from unauthorized disclosure, modification, and destruction

- First line of defense against unauthorized entry, access, and use

- Main types of mechanisms
  - Physical
  - Administrative
  - Technical

General Control Layers

Administrative Controls

- Development of policies, standards, and procedures
- Screening personnel, security awareness training, monitoring system and network activity, and change control

Technical Controls

- Logical mechanisms that provide password and resource management, identification and authentication, and software configurations

Physical Controls

- Protecting individual systems, the network, employees, and the facility from physical damage

Security Controls - Administrative

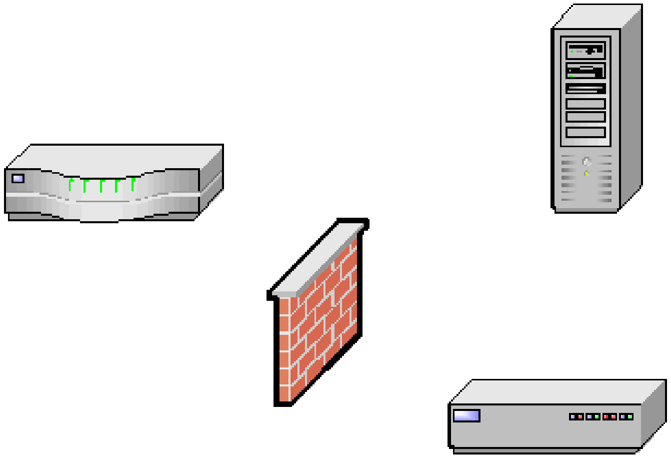
Administrative Controls

- Developing a security program
- Determining compliancy levels and consequences of non-compliance
- Indicating who has authorized access and who is unauthorized
- Classifying data and enforcing the necessary protection required for that classification
- Developing policies and standards and enforcing them when they are broken
- Developing an incident response program
- Developing a business continuity and disaster recovery plan
- Operational and continuity testing (i.e., Penetration Testing)

Security Controls – Technical

Technical Controls

- Implementing access control - requiring users to authenticate before accessing a system or data
- Encrypting data where it is stored and/or is transmitted
- Implementing firewalls and IDS
- Fault tolerance and load balancing
- Auditing



Security Controls – Physical

Physical Controls

- Locks and alarms on exterior doors
- Security guards watching for suspicious individuals and activities
- Intrusion detection systems to physically protect the facility
- Removing floppy drives so information cannot be copied and brought out of a building
- Storing backup data in a fire proof safe and/or at an offsite facility

Access Control Types/Categories

- **Preventative**
  - Controls used to prevent undesirable events from taking place
- **Detective**
  - Controls used to identify undesirable events that have occurred
- **Corrective**
  - Controls used to correct the effects of undesirable events
- **Deterrent**
  - Controls used to discourage security violations
- **Recovery**
  - Controls used to restore resources and capabilities
- **Compensation**
  - Controls used to provide alternative solutions
- **Directive**
  - Policies used to preclude or mandate actions to reduce risk

Control Combinations

Preventative – Administrative

- Policies and procedures
- Pre-employment background checks
- Data classification and labeling
- Security awareness

Preventative – Physical

- Badges and swipe cards
- Guards, dogs, motion detectors, CCTV
- Fences, locks, man-traps, alarms

Preventative – Technical

- Passwords, biometrics, smart cards
- Encryption, protocols, call-back systems, database views, constrained user interface
- Anti-virus software, ACL's, firewalls, routers, clipping levels

Control Combinations

Detective – Administrative

- Job rotation
- Sharing responsibilities
- Inspections
- Incident response

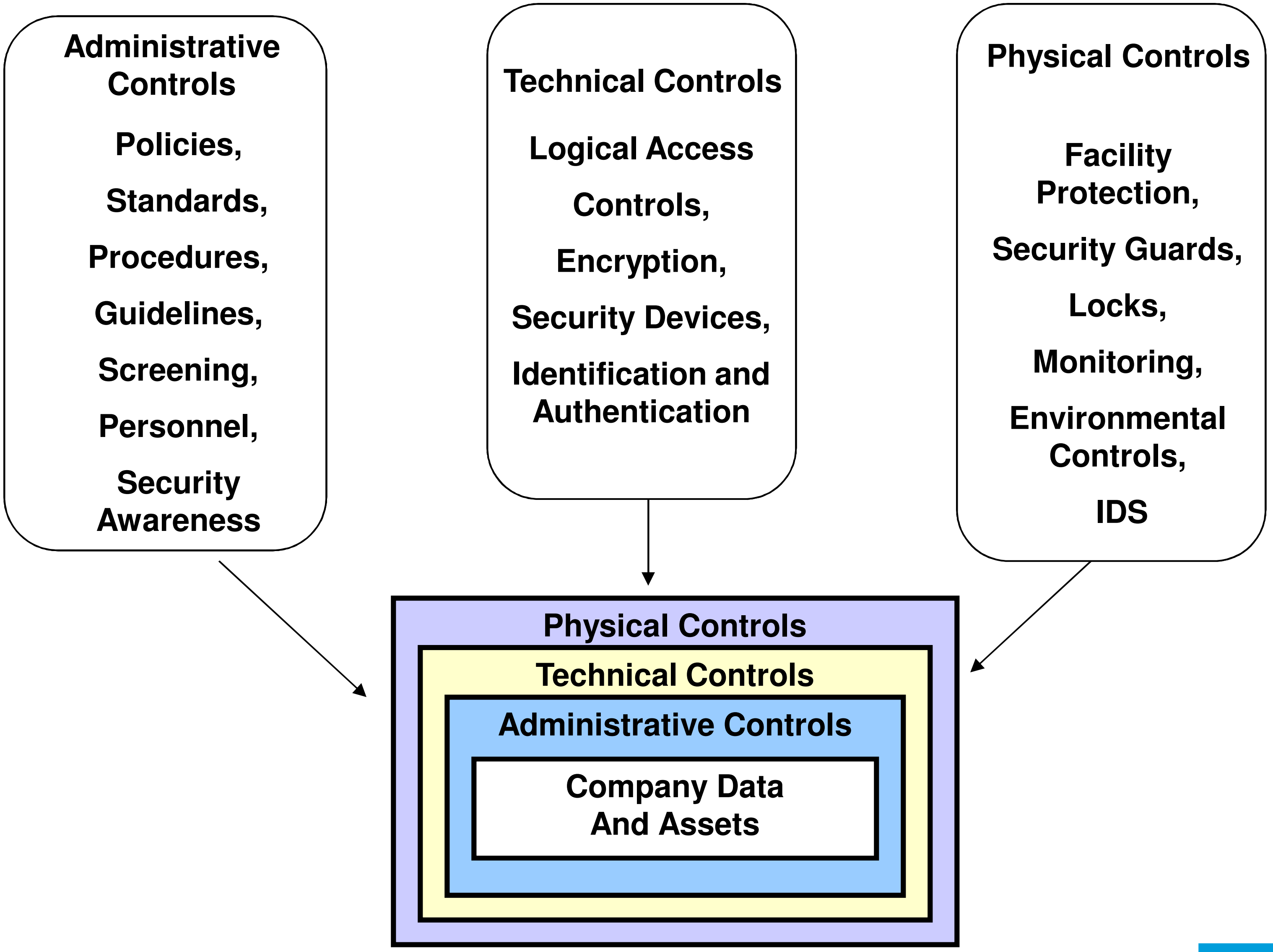
Detective – Technical

- IDS
- Reviewing audit logs
- Reviewing violations of clipping levels

Detective – Physical

- Human evaluation of output from sensors or cameras
  - Motion detectors, intrusion detection, video cameras

How Controls Work Together



Administrative Controls

Policies,

Standards,

Procedures,

Guidelines,

Screening,

Personnel,

Security Awareness

Technical Controls

Logical Access

Controls,

Encryption,

Security Devices,

Identification and Authentication

Physical Controls

Facility Protection,

Security Guards,

Locks,

Monitoring,

Environmental Controls,

IDS

Physical Controls

Technical Controls

Administrative Controls

Company Data And Assets

Access Control Definitions

Subject

- Active entity that requests access to an object or the data within an object

Object

- Passive entity that contains information

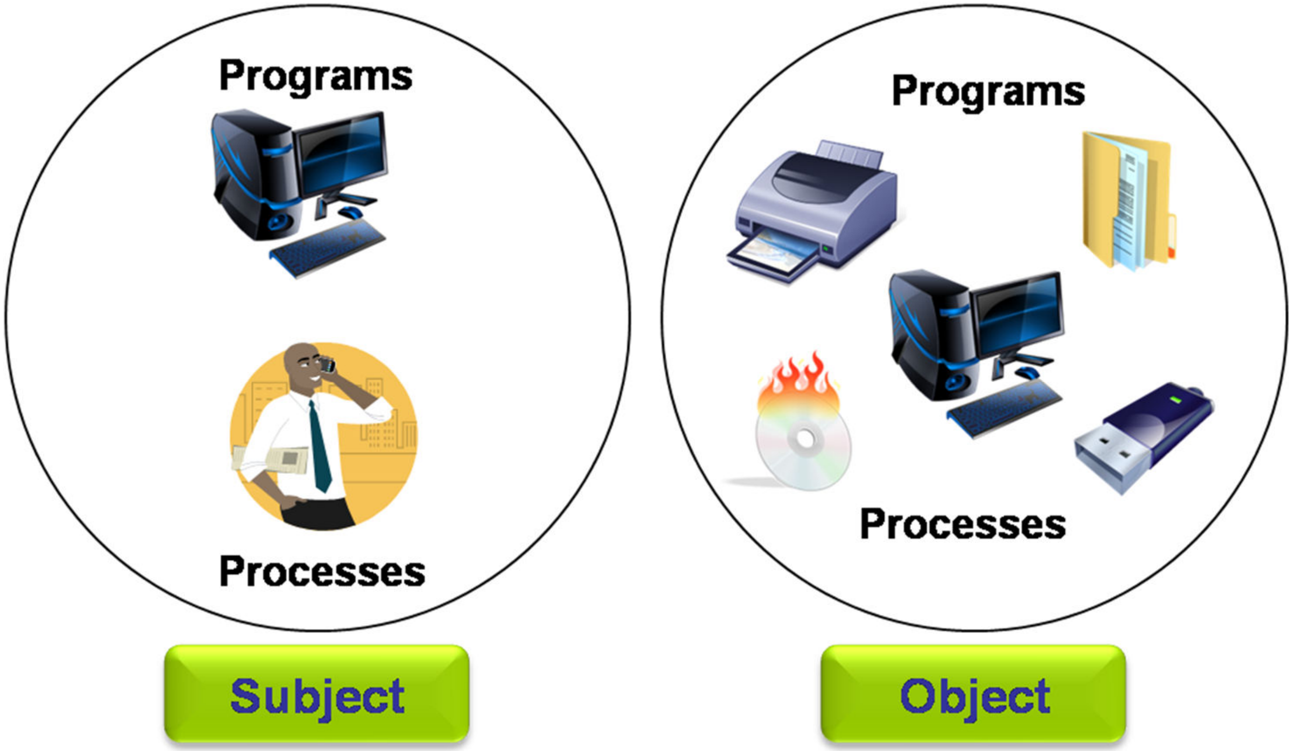
Access

- Ability of subject to “do something”
  - Read, create, delete, modify
- Flow of information between a subject and an object

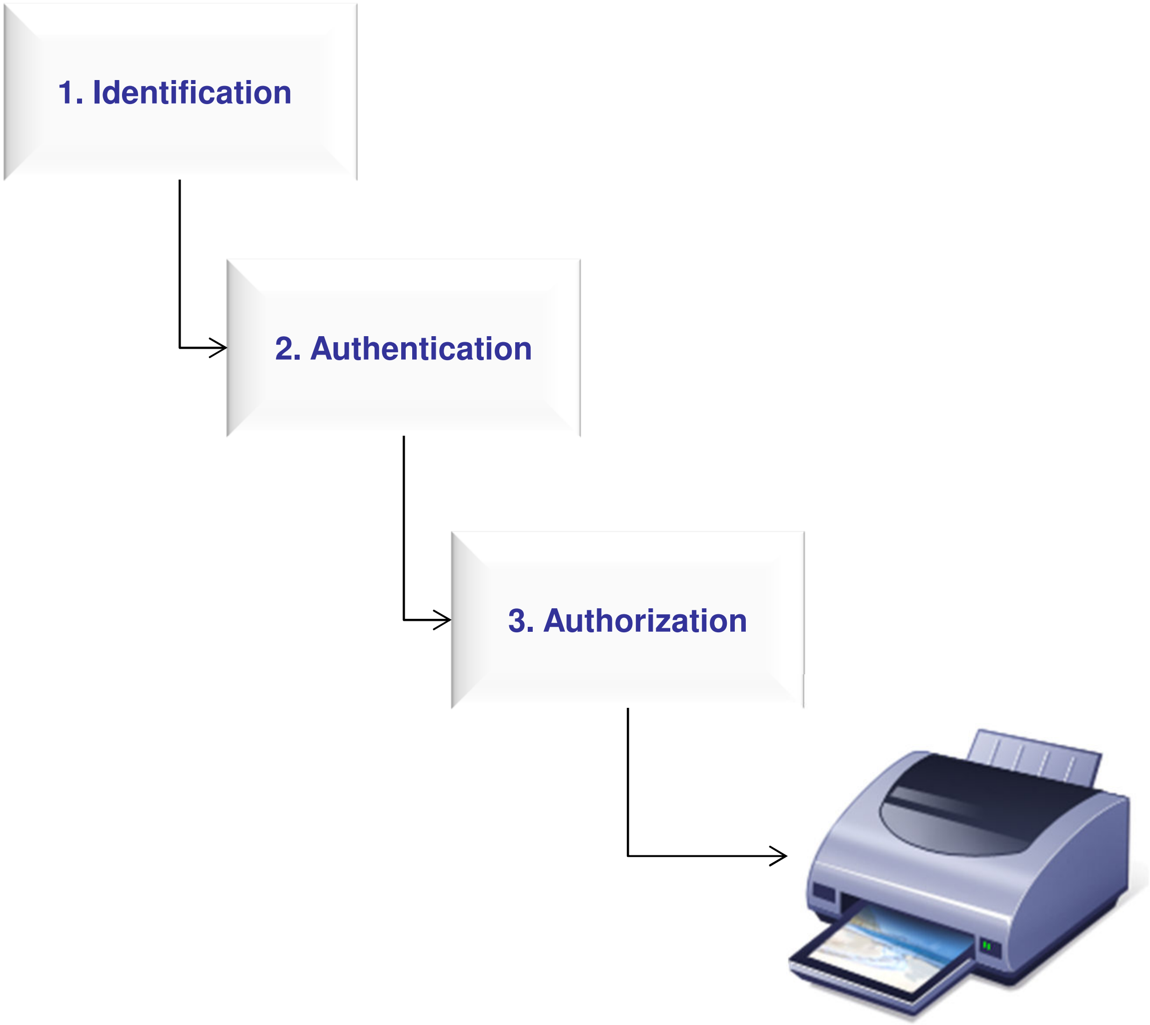
Access Control

- Security features that control how subjects and objects communicate and interact with other subjects and objects

Subject and Object Relationship



Steps of Access Control



1. Identification

2. Authentication

3. Authorization

Who are you?

Identification

- Identifying the subjects
  - Username, smart card, memory card

Authentication

- Proving the subject is who it claims to be with a second piece of a credential set

Authorization

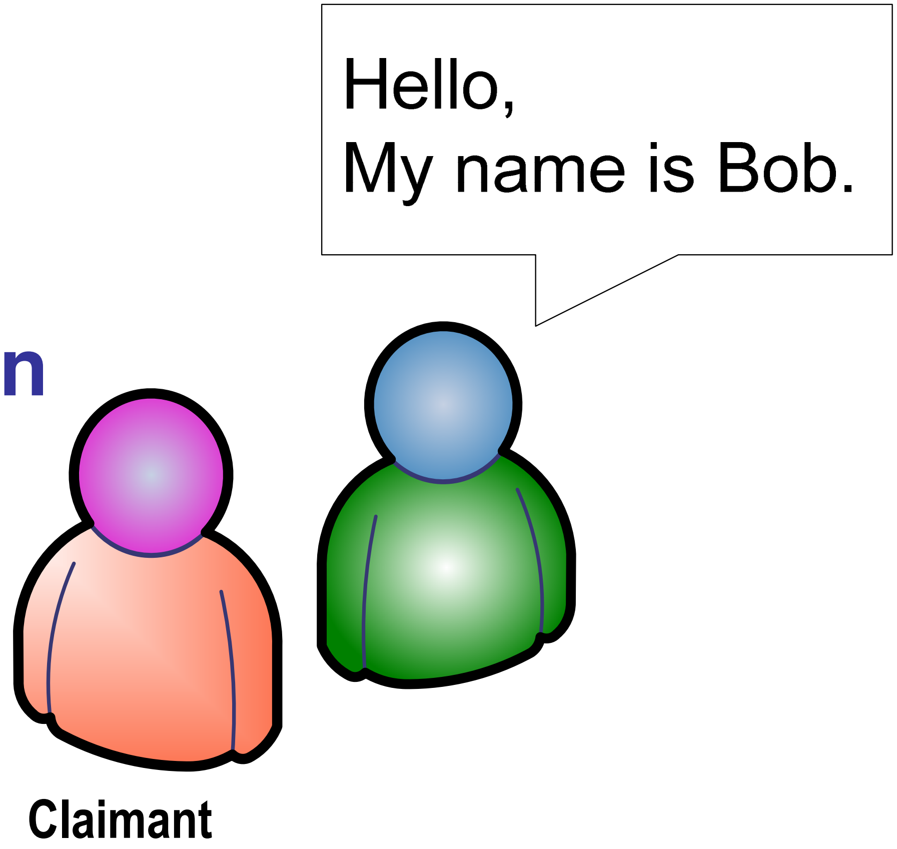
- Granting access to resources based on a criteria

Accounting

- Keeping records of activity

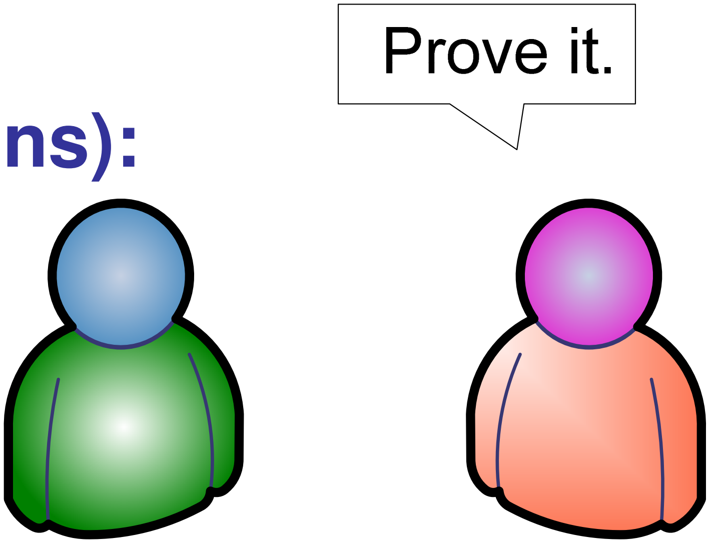
Identification

- **Claimed identity**
- **Public information**
- **Forms of Identification**
  - Username/ User ID
  - PIN
  - RFID
  - MAC & IP Addresses



Authentication

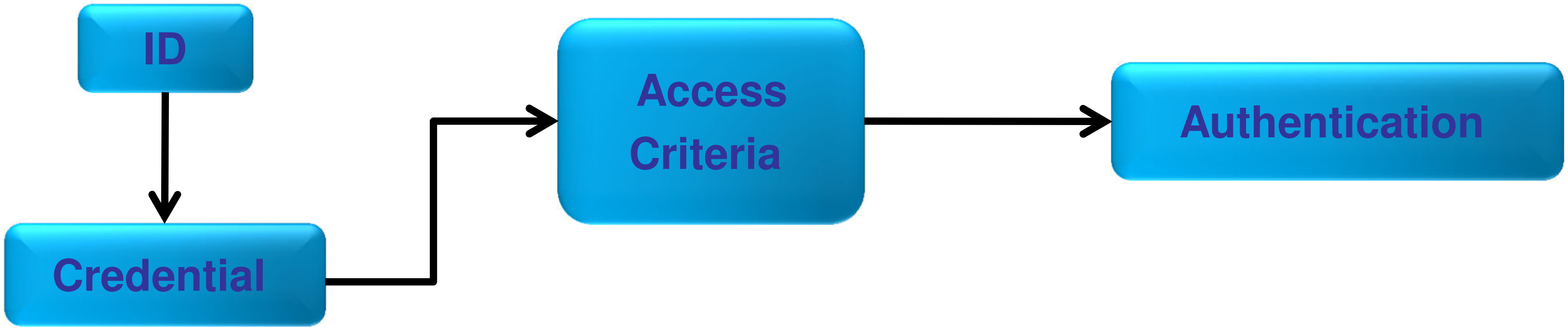
- **A subject must prove its identity**
  - Verifying the claimant
- **Types (implementation options):**
  - Something you know
  - Something you have
  - Something you are



- **Two factor authentication**
  - Strong authentication employs two out of these three options
- **Mutual authentication**
  - Also called two-way authentication

Authentication Components

- Biometrics
- Passwords
- Token devices
- Memory cards
- Smart cards
- Cryptographic keys



Type 1 – Something the User Knows

- Password
- Personal History
- Passphrase
- PIN
- Graphical

Passwords

Password Characteristics

- Cheapest, least secure, most widely used authentication technology
- Least secure because users choose easy passwords, share them, write them down, or do not change them
- Lack of strict password policy enforcement reduces security
- Password generators can create complex passwords, but users will just write them down

Password Best Practices

- At least eight characters (alphanumeric and symbols) with upper and lower case values
- User should not be able to use same password or share passwords
  - Password history
  - Passwords should not be easily guessed or dictionary words
- Threshold (clipping level) of acceptable number of failed logins logged
- Audit log should contain date, time, user ID, and workstation logged in from
- Password lifetime should be short, but practical

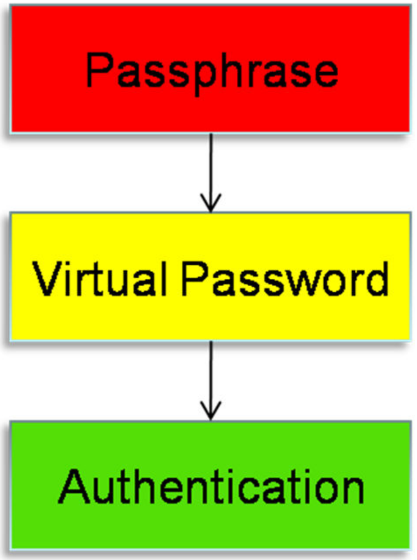
Password Types

Cognitive Passwords

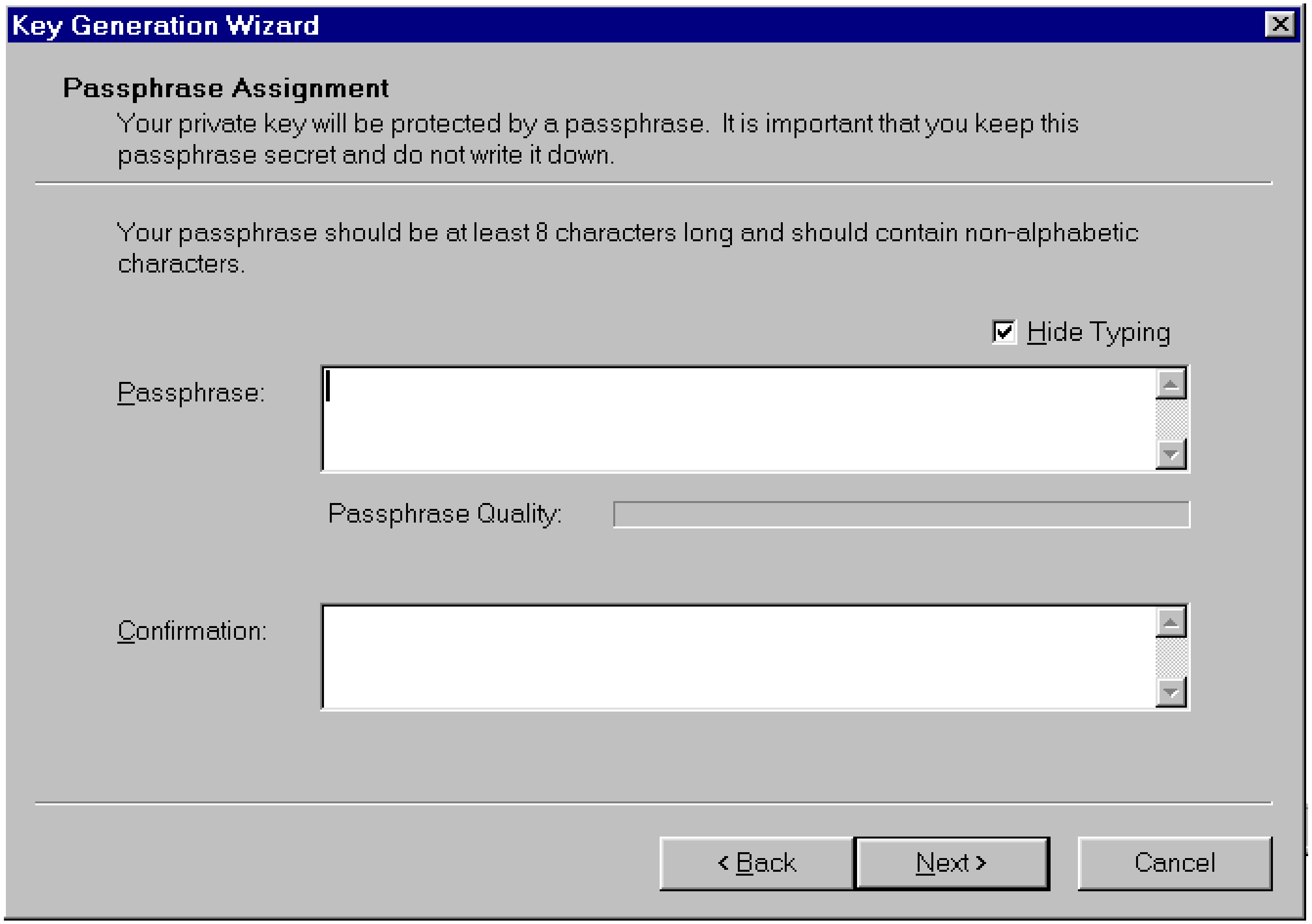
- Fact or opinion-based information used to verify an individual’s identity
- Enrollment phase includes questions about one’s life
  - Mother’s maiden name
  - Pet’s name
  - Favorite color
- Easier to remember than a password

Authentication Mechanism – Passphrase

- **A sequence of characters longer than a password**
  - More secure than a password because it’s longer
- **Once entered, the software transforms it into a virtual password**
- **Usually easier for a user to remember**



Passphrase



Key Generation Wizard

Passphrase Assignment

Your private key will be protected by a passphrase. It is important that you keep this passphrase secret and do not write it down.

Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.

☑ Hide Typing

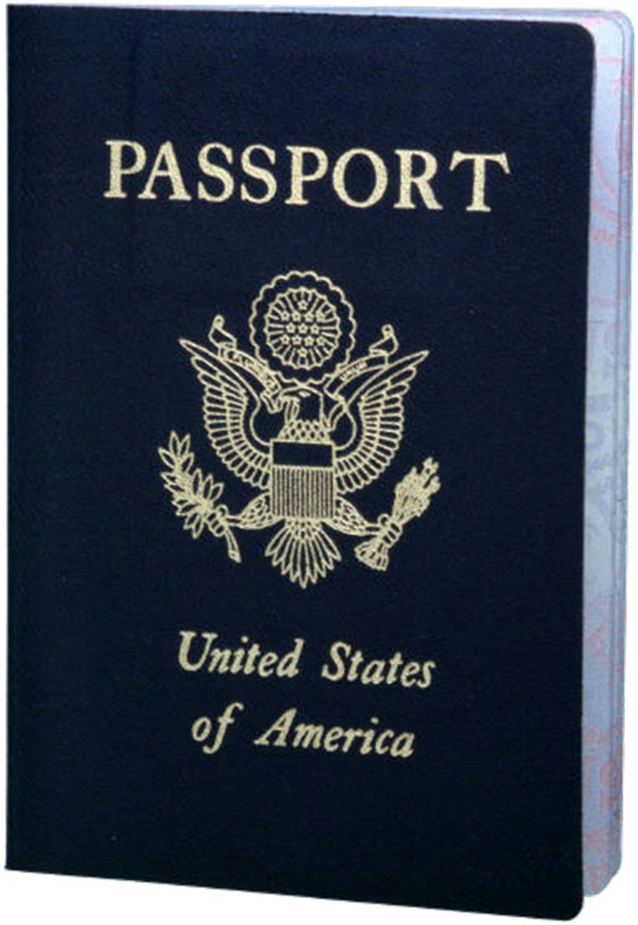
Passphrase:

Passphrase Quality:

Confirmation:

Type 2 – Something the User Has

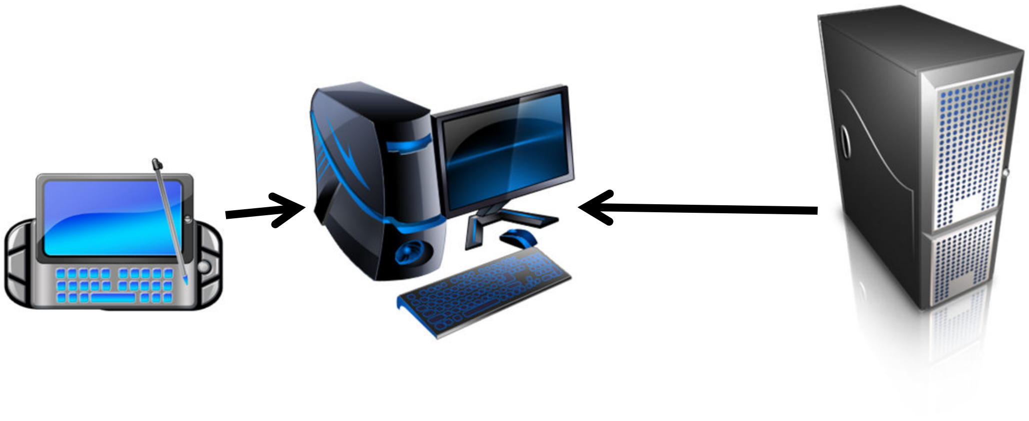
- Token Device
  - Synchronous
  - Asynchronous
- Cryptographic Keys
- Memory Cards
- Smart Cards



One-Time Password Generators

One-Time Password

- Dynamic password that is good for only one u
- Useless if an attacker obtains password
- Usually created via token device
  - Hand-held device with a LCD display and keypad



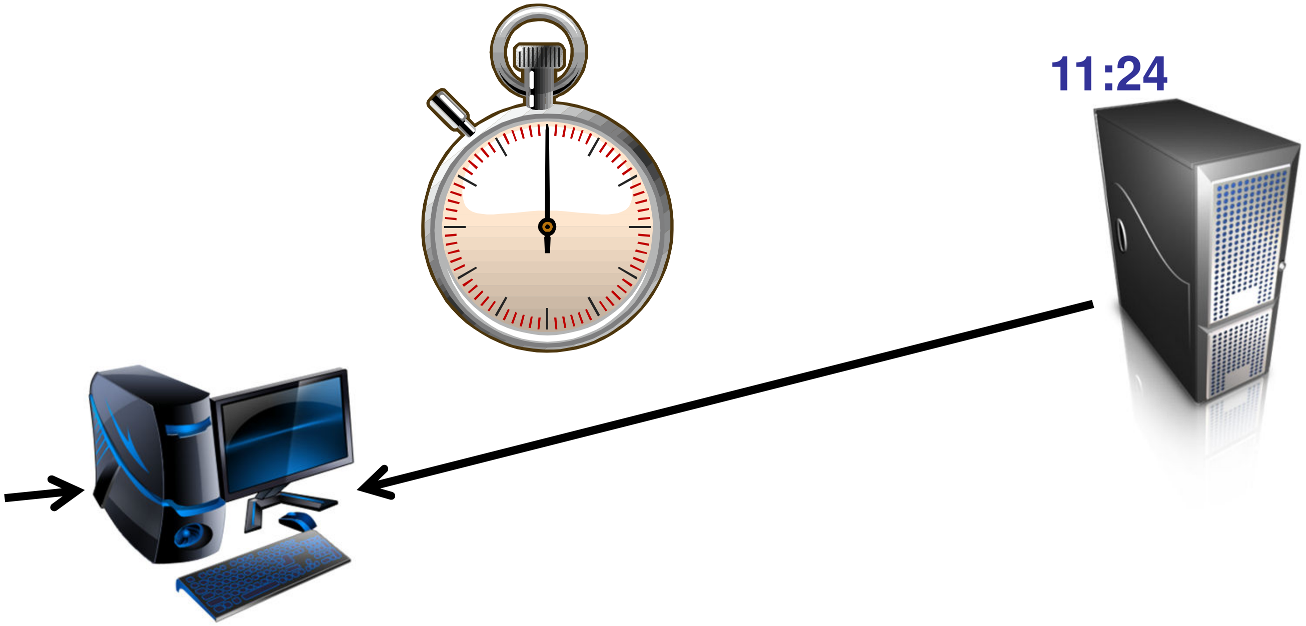
Synchronous One-Time Password

Synchronous Token Device

- Synchronizes with the authentication service by using time or an event as the core piece of the authentication process
- Time or event driven
- Time value on device encrypted and s
- User types in value and username
- Sent to authentication server

Synchronous One-Time Password

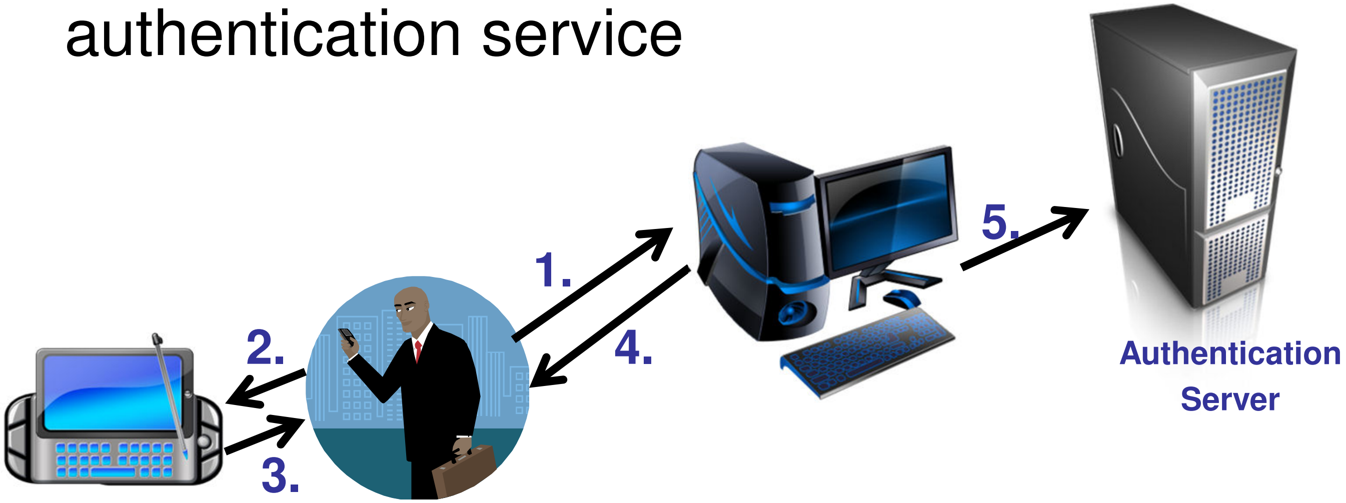
- Synchronous Token Device



Asynchronous One-Time Password

Asynchronous Token Device

- Challenge-response scheme to communicate with the authentication service



1. Challenge Value displayed on workstation
2. User enters Challenge Value and PIN into token device
3. Token device presents a different value to the user
4. User enters new value into the workstation
5. Value sent to authentication service on server
6. Authentication service is expecting a specific value
7. User is authenticated and allowed access to workstation

Token Devices – Pros and Cons

Disadvantages:

- Token devices can be lost
- Both token schemes can fall prey to masquerading if the user shares identification information

Advantages:

- Not as vulnerable to electrical eavesdropping, replay attacks, and password guessing as other password methods
- Provides a higher level of protection than static passwords

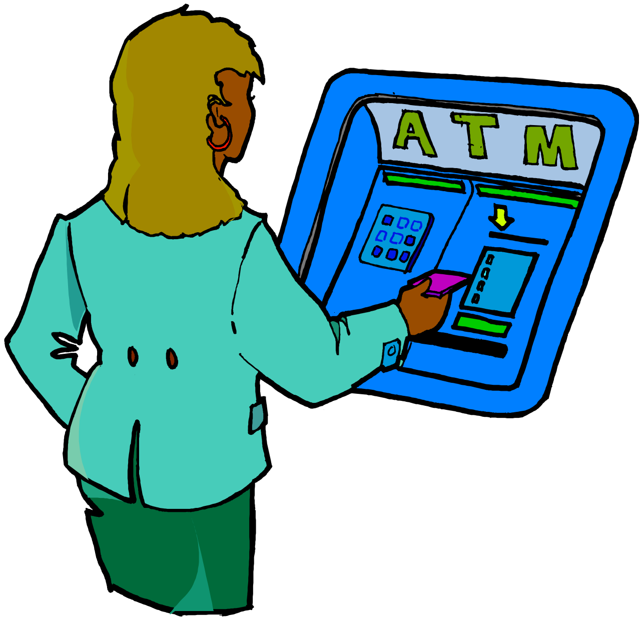
Authentication Mechanism – Keys

Cryptographic Keys

- Private key or digital signature can be used to prove one's identity
  - Private key is a secret cryptographic value that should only be in the possession of one person
  - Digital signature is encrypting a hash value with the private key
- Used when more security is required than static passwords can provide

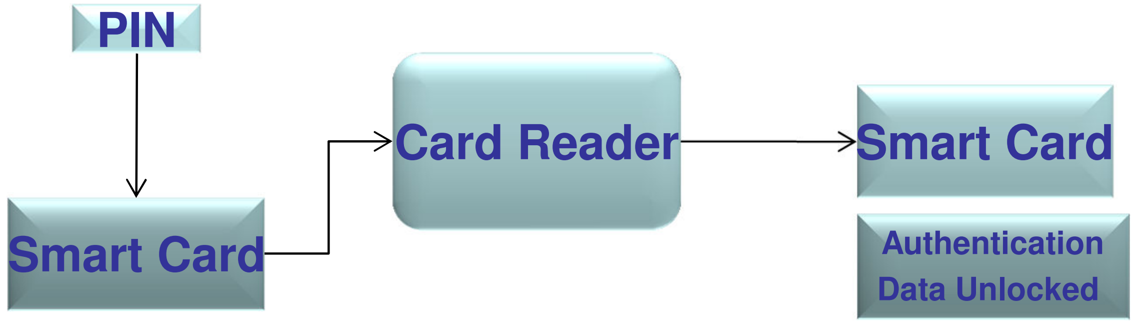
Authentication – Memory Card

- Card holds user authentication information
- User puts card into reader and enters username or PIN
- Card can only hold information, not process information
- Added cost of reader, card creation,
  and maintenance



Authentication Mechanism – Smart Card

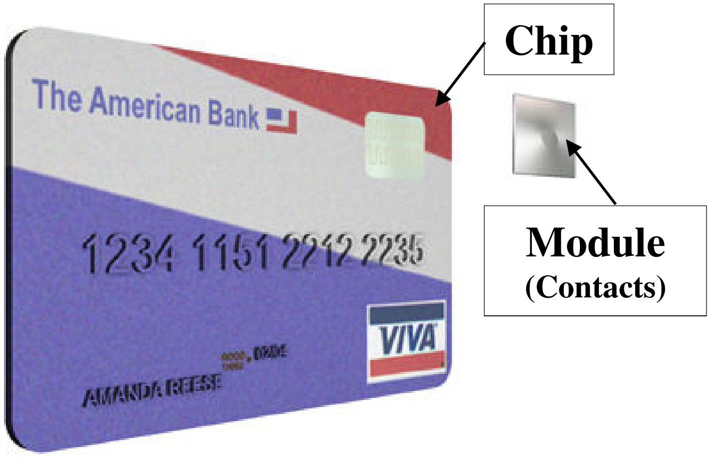
- Has a microprocessor
- Tamperproof mobile storage of user authentication data
- Can work with PKI to provide mutual authentication of parties
- After a threshold of failed login attempts, it can render itself unusable

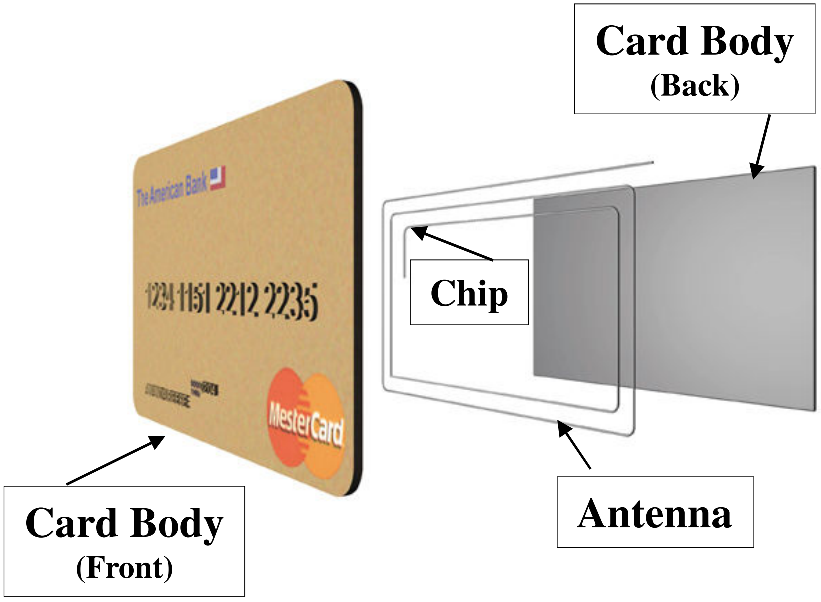


Authentication Mechanism

Two general categories:

- Contact
- Contactless





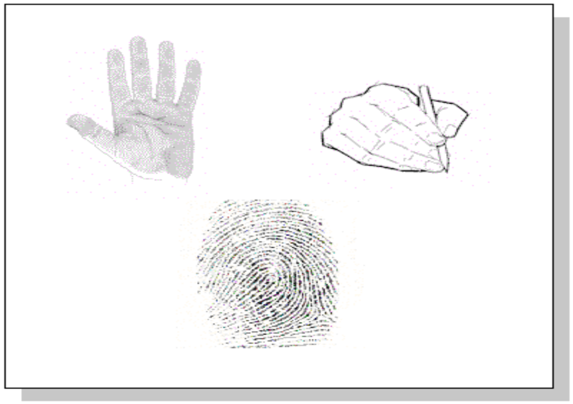
Type 3 – Something the User "Is"

- Sophisticated
- Expensive
- Type 1 error – false reject rate (FRR)
- Type 2 error – false accept rate (FAR)
- Crossover error rate (CER)

Biometrics

Physical Attributes for Authentication

- Verifies an individual's identity by a unique personal attribute
- Most accurate, sophisticated, and expensive way of identifying individuals
- Low acceptance rate by society
- Categories
  - Static (physiological; what you are)
  - Dynamic (behavioral; what you do)



Biometrics

Characteristics

- Biometrics reference files can be stored in a database or on a portable token, as in a smart card
  - Smart card has a biometric template
- It can be a 1-to-1 matching process (Authentication)
  - Compared against a specific reference file in the user's profile or account
  - Is he who he says he is?
- It can be a 1-to-N matching process (Identification)
  - User does not claim identity, but attribute is compared to a large database of possibilities
  - Who is this?

Biometrics Process – Enrollment

- **User must complete an enrollment process that stores the physical attributes in a reference file**
  - When the user needs to authenticate, his attributes are compared to this file
  - Process looks at highly detailed information, so it is prone to errors
    - (Type I error) – rejects authorized individual
      - Also known as False Reject Rate (FRR)
    - (Type II error) – accepts impostor
      - Also known as False Acceptance Rate (FAR)

Crossover Error Rate (CER)

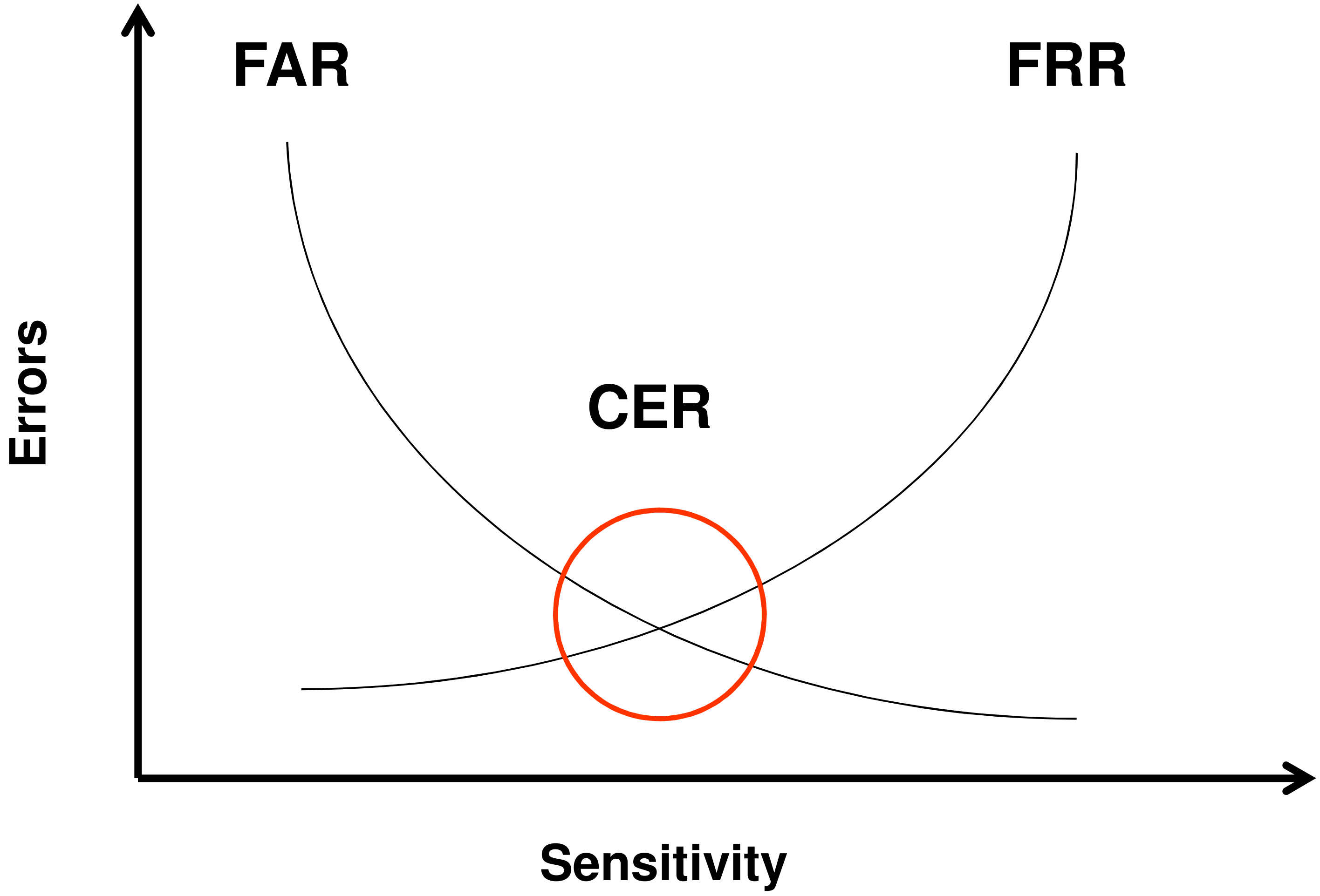
- A rating that represents the point at which the Type I errors equal the Type II errors

- Rating that attempts to combine two metrics of a biometric system:
  - Error level
  - Sensitivity setting

- Example:
  - System A has 1 out of 100 Type I errors = 1%
  - System A has 1 out of 100 Type II errors = 1%

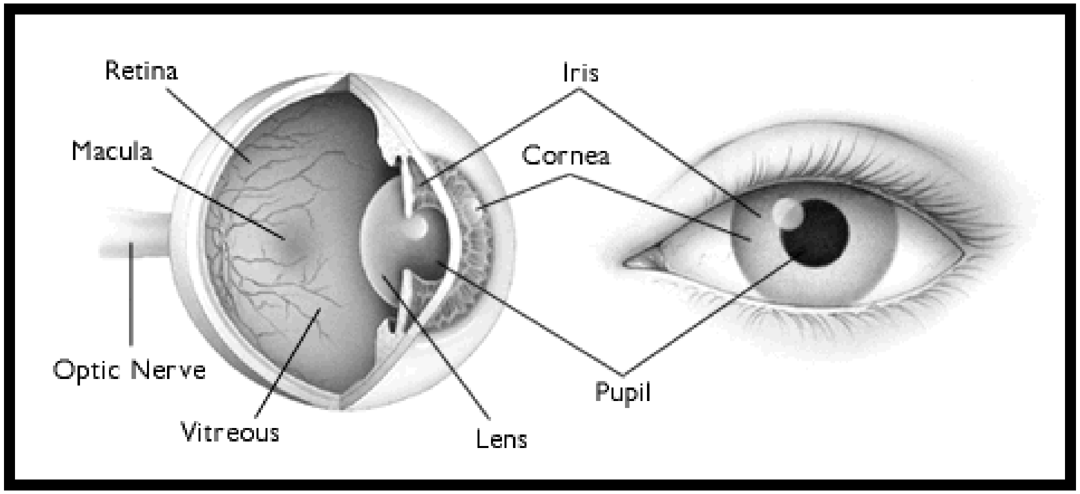
- System with a CER of 3 is more accurate than a system with a CER of 4

Crossover Error Rate (CER)



Types of Biometrics

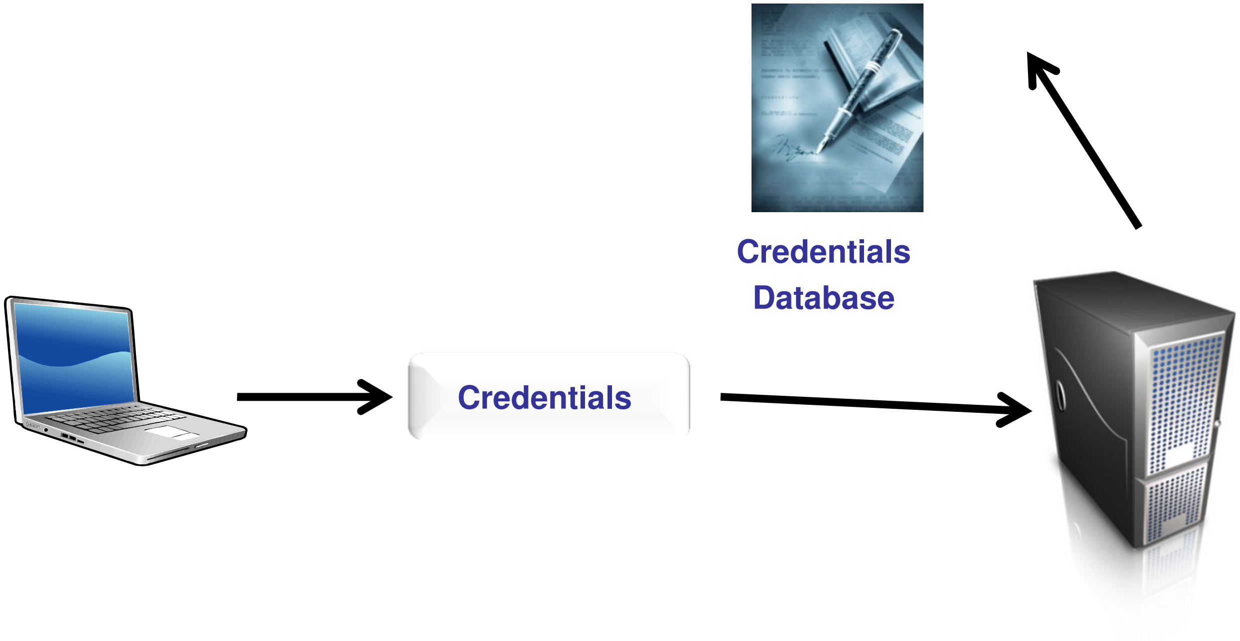
- Fingerprint
- Palm Print
- Finger Scan
- Hand Geometry
- Retina Scan
- Iris Scan
- Facial Scan
- Hand Topology
- Signature Dynamics
- Keyboard Dynamics
- Voice Print



American Academy of Ophthalmology

Authorization

- **Before a subject can access an object:**
  - It must be identified, authenticated, and authorized
  - Authorization is the process of comparing a subject's credentials and permissions to an access criteria



Access Criteria Characteristics

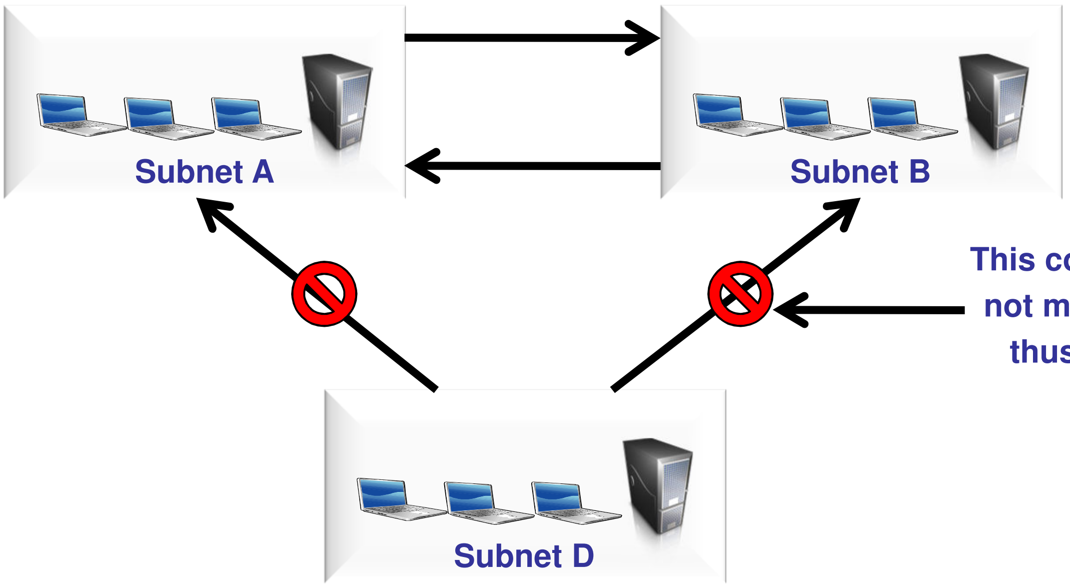
- Clearance
- Need-to-know
- Least Privilege
- Default to “no access”

<u>Access Control List</u>

Subnet A can access Subnet B

Subnet D cannot access Subnet A

Subnet B can access Subnet A



This communication path is not mentioned in the ACL, thus it is automatically disallowed

Splitting Control

Separation of Duties

- Dividing roles and responsibilities of individuals or departments so that one critical task cannot be performed by one entity
  - Key escrow, developers, and QA
- Security should be separated from operations
  - Separate security officer
  - Security has more independence, attention, and resources

Dual Control

- Ensuring that more than one individual has to be involved in completing a task

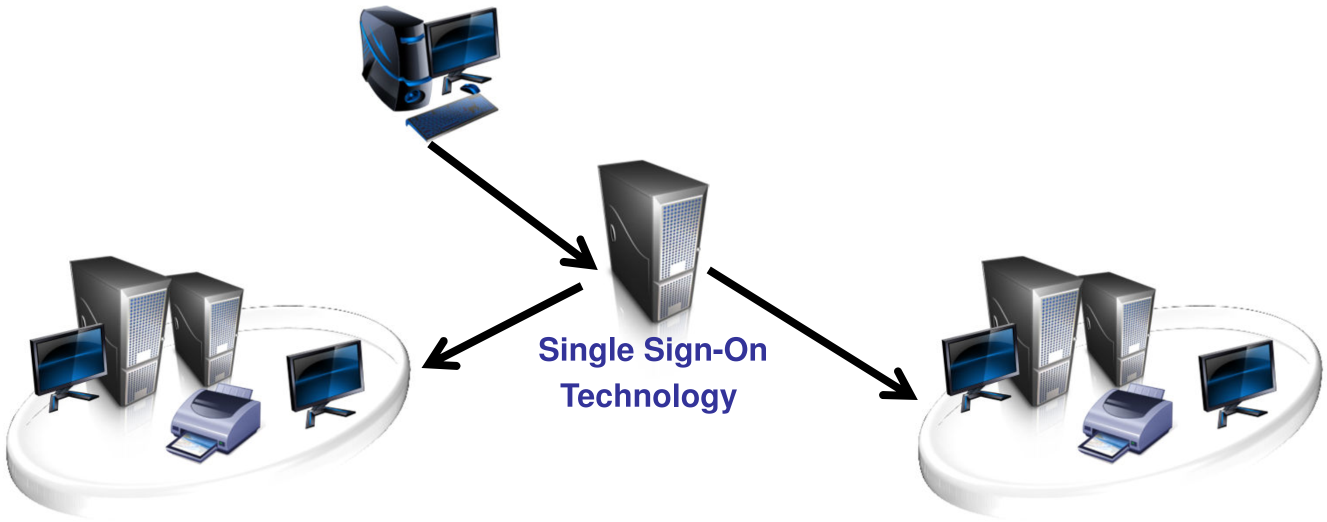
Dual Control

- Two people are required to complete a process
- May be physical; e.g. two persons required to unlock the Data Safe
- May be logical; e.g. A manager level authorization is required for transaction above $15K
- Parties would need to be in collusion to abuse
- For greater security, it could be 2 pair of 2 people
- Trusted Operating Systems enforce this requirement
- Dual control allows for separation of duties
- Overall it provides substantially greater security

Single Sign-On Technology

Single Sign-On Technology

- Requires users to present their credentials once
- Users can then access all resources
- Less administration
- Centralization of user information
- Users only need to remember one set of credentials



Single Sign-On Technologies

Technologies:

- Scripts
- Directory Services
- Kerberos
- SESAME
- Thin Clients

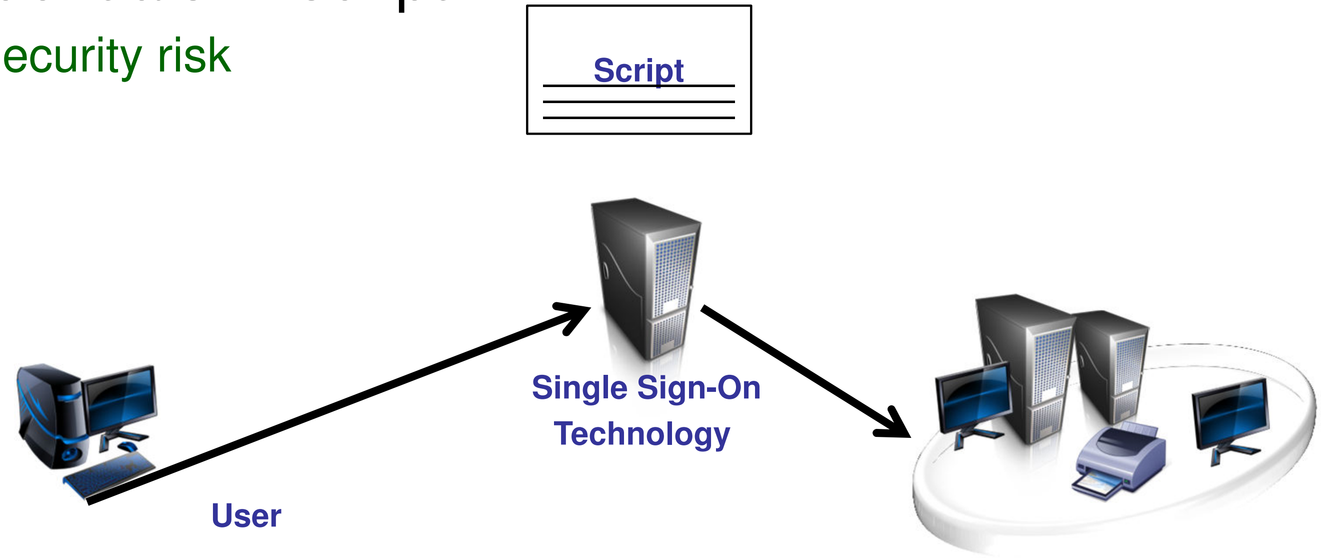
Issues:

- Interoperability
- Security

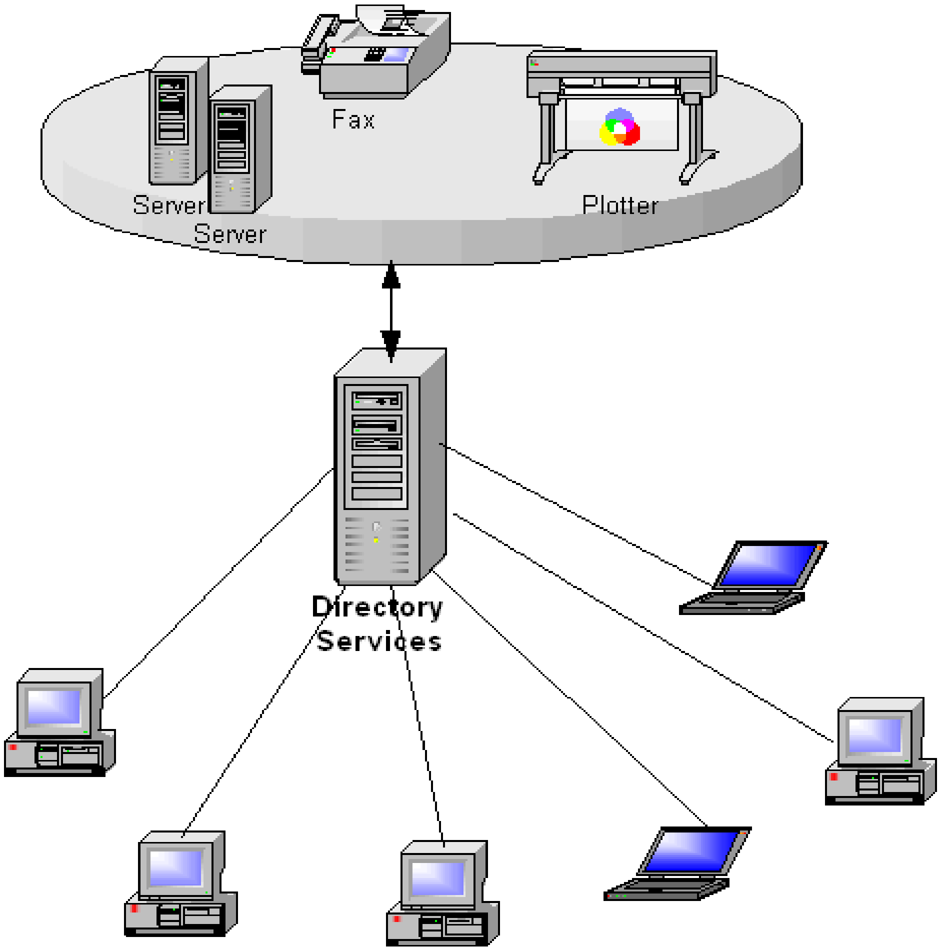
Single Sign-On Technology – Scripts

Scripting

- Login script to perform users' manual steps
- Hard to maintain
- Credentials in script
  - Security risk



Single Sign-On – Directory Services



Single Sign-On Technology

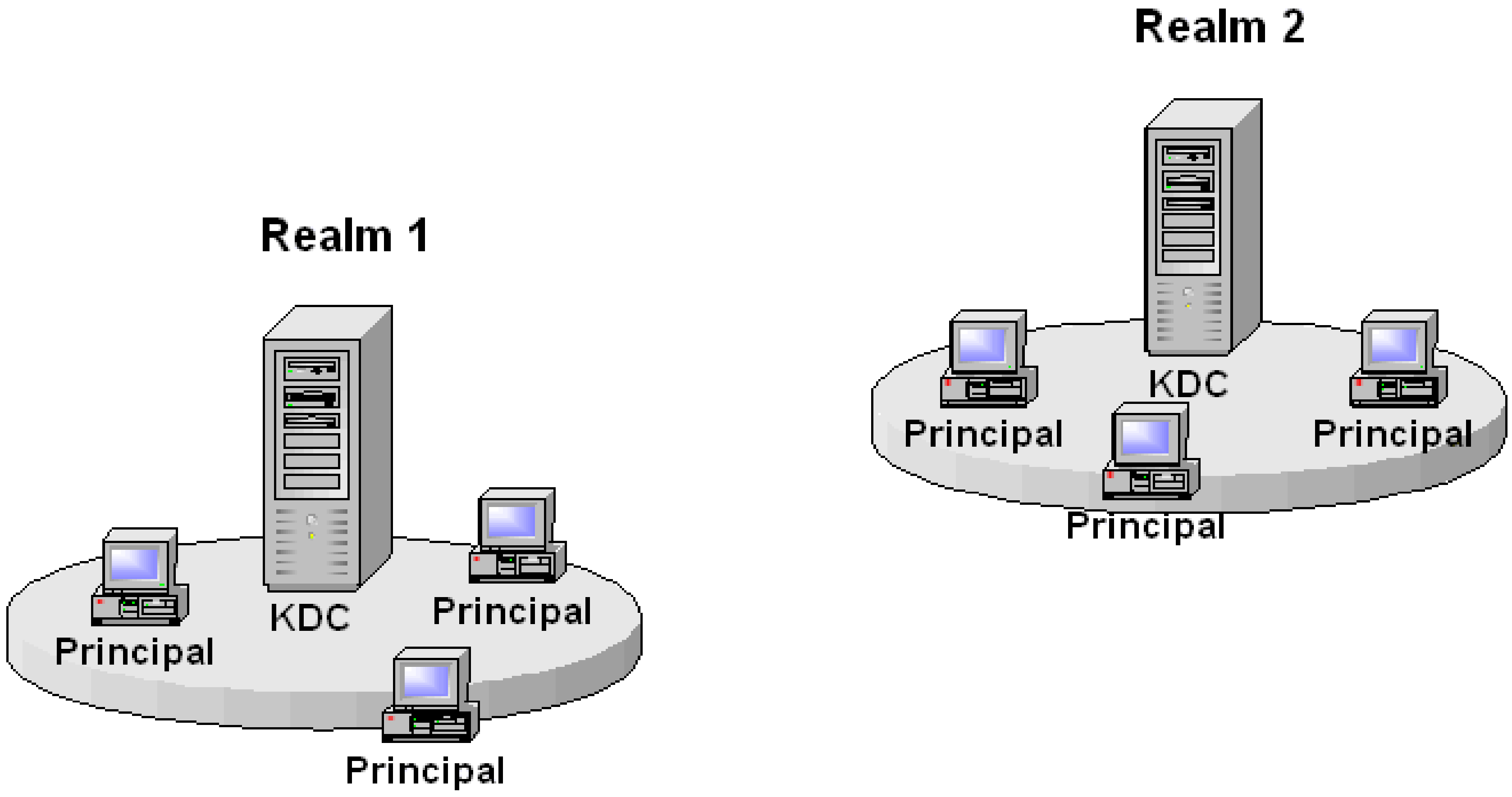
Kerberos

- Authentication protocol designed in mid-1980 as part of MIT’s Project Athena
- Uses symmetric key cryptography (DES) for authentication and encryption
- A ticket-based authentication technology

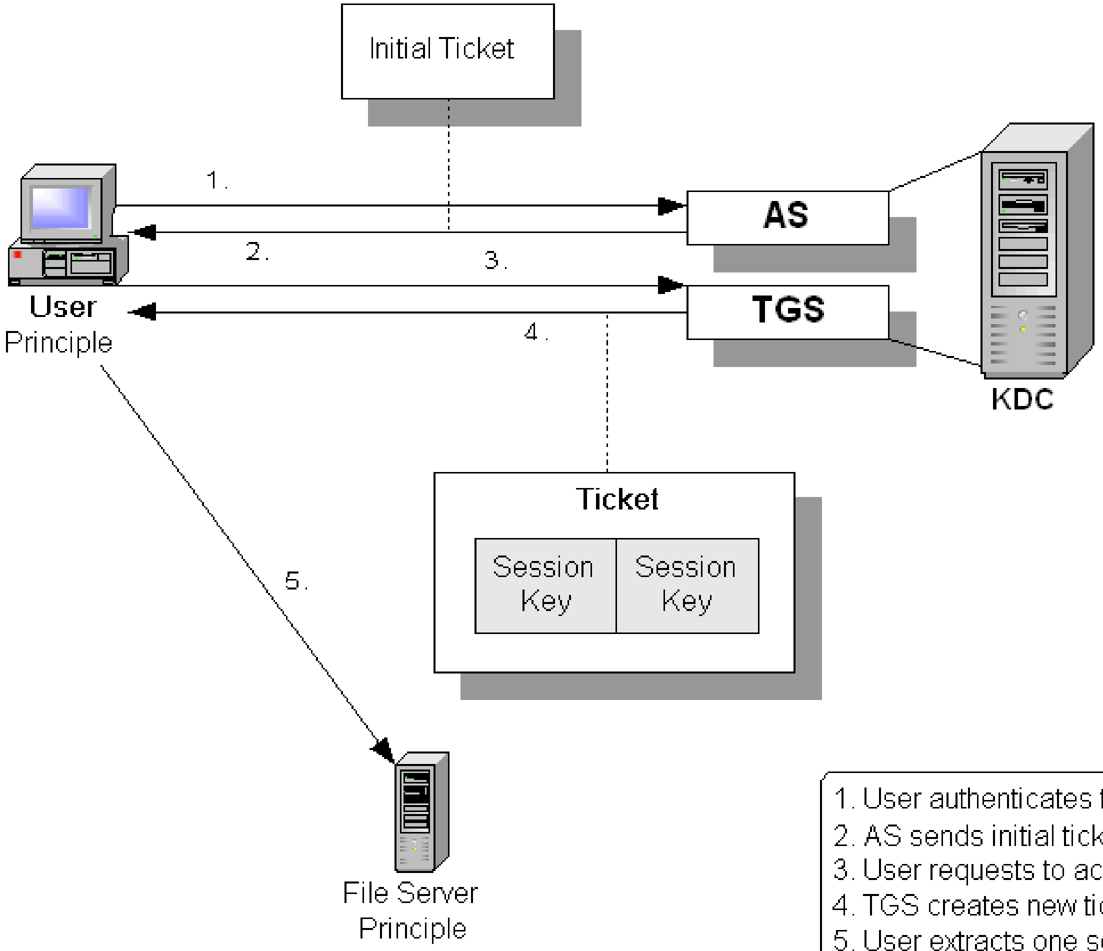
Kerberos Components

- Key Distribution Center (KDC)
- Principals
  - users
  - applications
  - services
- Realm
- Ticket Granting Service (TGS)
- Authentication Server (AS)
- Ticket Granting Ticket (TGT)
- Ticket
- Secret and Session Keys

Kerberos Components



Kerberos Steps



1. User authenticates to AS
2. AS sends initial ticket to user
3. User requests to access file server
4. TGS creates new ticket with session keys
5. User extracts one session key and sends ticket to file server

Kerberos – Process

Authentication Process:

1. User authenticates to authentication service (AS) on KDC
2. AS verifies credentials and responds with ticket granting ticket (TGT) for TGS
3. When user wants to use a resource, requests session ticket (ST) from TGS
4. ST has two instances of a session key: one for user, other for resource
5. User sends ST to resource for authentication
6. Authentication communication is encrypted

Kerberos Weaknesses

- Provides authentication, confidentiality, and integrity only
- The KDC is a single point of failure
- Keys are stored on the users' workstations
  - In cache or key table
- Kerberos is vulnerable to password guessing
  - Cannot detect a dictionary attack
- All principals must be "Kerborized"
  - Software changed to accept this type of authentication

Single Sign-On Technology – SESAME

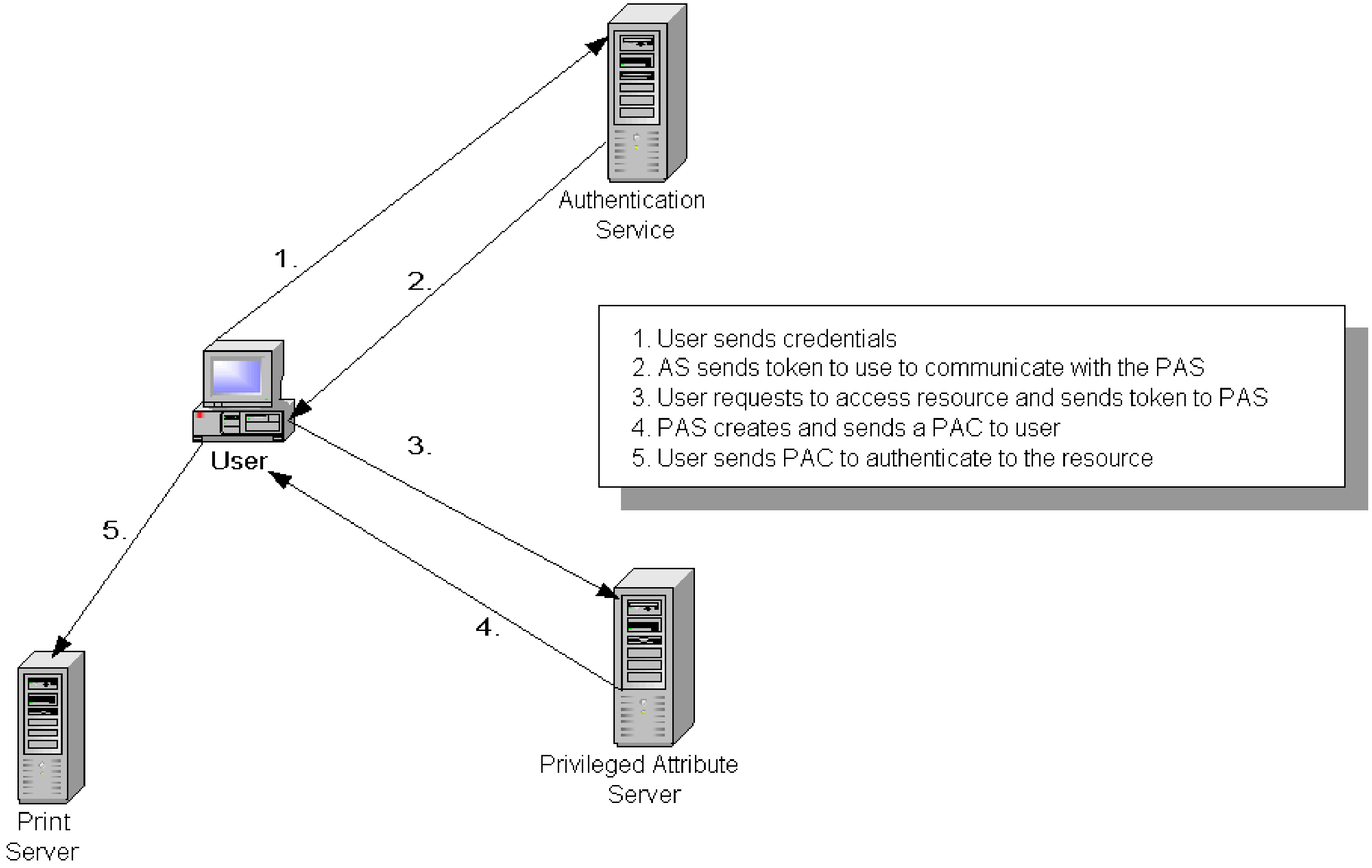
- The Secure European System for Applications in a Multi-vendor Environment (SESAME) project

- Uses public key cryptography for the distribution of secret keys, which reduces key management overhead
  - Secret key encrypts data

- SESAME adds more access control features than Kerberos, has scalability of public key systems, and is easier to manage

- SESAME is vulnerable to password guessing, as is Kerberos

SESAME



1. User sends credentials
2. AS sends token to use to communicate with the PAS
3. User requests to access resource and sends token to PAS
4. PAS creates and sends a PAC to user
5. User sends PAC to authenticate to the resource

Access Control Model

- A framework that dictates how subjects access objects

- It uses technologies and methods to enforce the rules and objectives of the security policy

- Two model types from TCSEC:
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)

- Another (from NIST):
  - Role-Based Access Control (RBAC)

Discretionary Access Control

DAC Characteristics

- Data owner specifies who can access resources
- Data owner is usually the creator and has full control of object
- Called discretionary because control of access is based on the discretion of the owner
- Mostly implemented through ACL's, based on “need-to-know”
- DAC model is used in environments that do not require a high level of centralized security
- User-controlled sharing that reduces central system administration
- End users are usually not the owners of all the objects they access – the corporation is the actual owner

DAC

DAC Characteristics

- Access is allowed solely on the identity of subjects who are trying to access the objects
- Explicitly identifying individuals provides identity-based controls
- Data owners determine who can access their resources

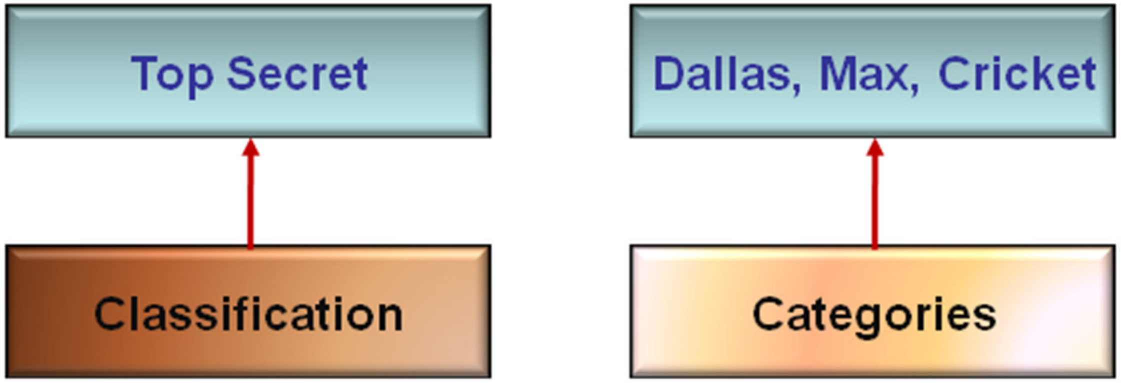
Mandatory Access Control

MAC Characteristics

- Access is based on security clearance of subject and classification of object
- Each user is assigned a clearance, and each object has a classification and compartment stored in its security label
- Access is decided by the system and not up to the discretion of a data owner
  - Subject cannot pass access permission to another subject
- Used in environments that require higher levels of security and structure
  - DAC can be used for unclassified data
  - MAC is used for classified data
- Used in many military institutions

Security Labels

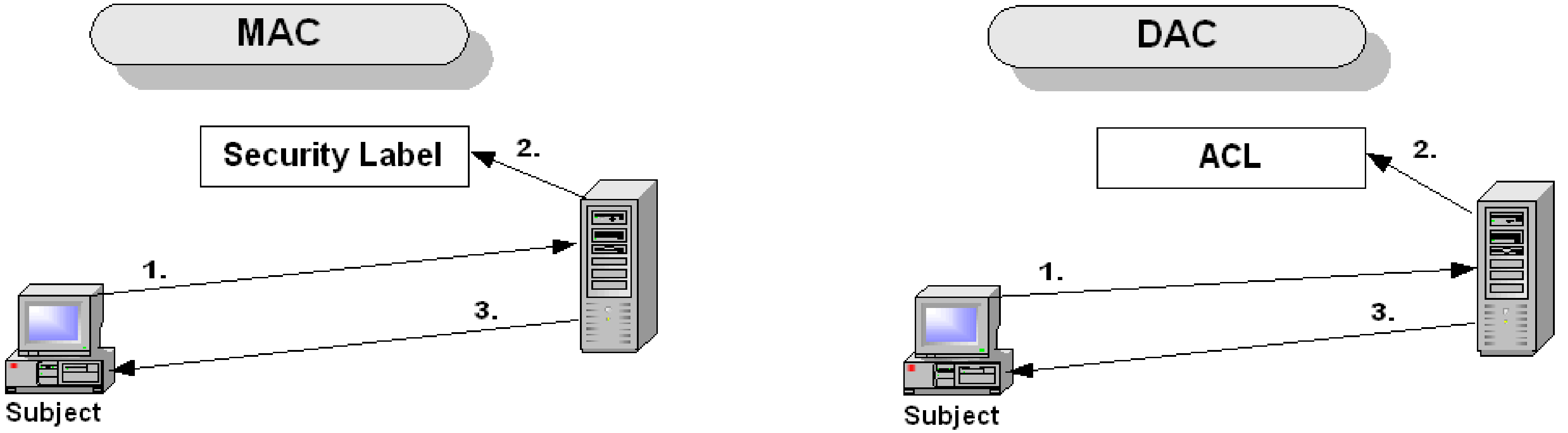
- Each object has a security label indicating its classification
- Compartments or Categories enforce a need-to-know
- In MAC, access decisions are based on these labels
  - Access within DAC is usually based on ACL's



Labels

- **Key to Mandatory Access Control decision making**
- **To access and modify an object, the subject's label must dominate the object's label**
- **A physically unique label is not necessary for every object**
  - All files on one system can share the same label
- **Trusted computer system ensures that labels cannot be arbitrarily changed**
  - Installed and maintained by specified systems administrators
- **Trusted computer controls flow of information between classification levels**

MAC Versus DAC

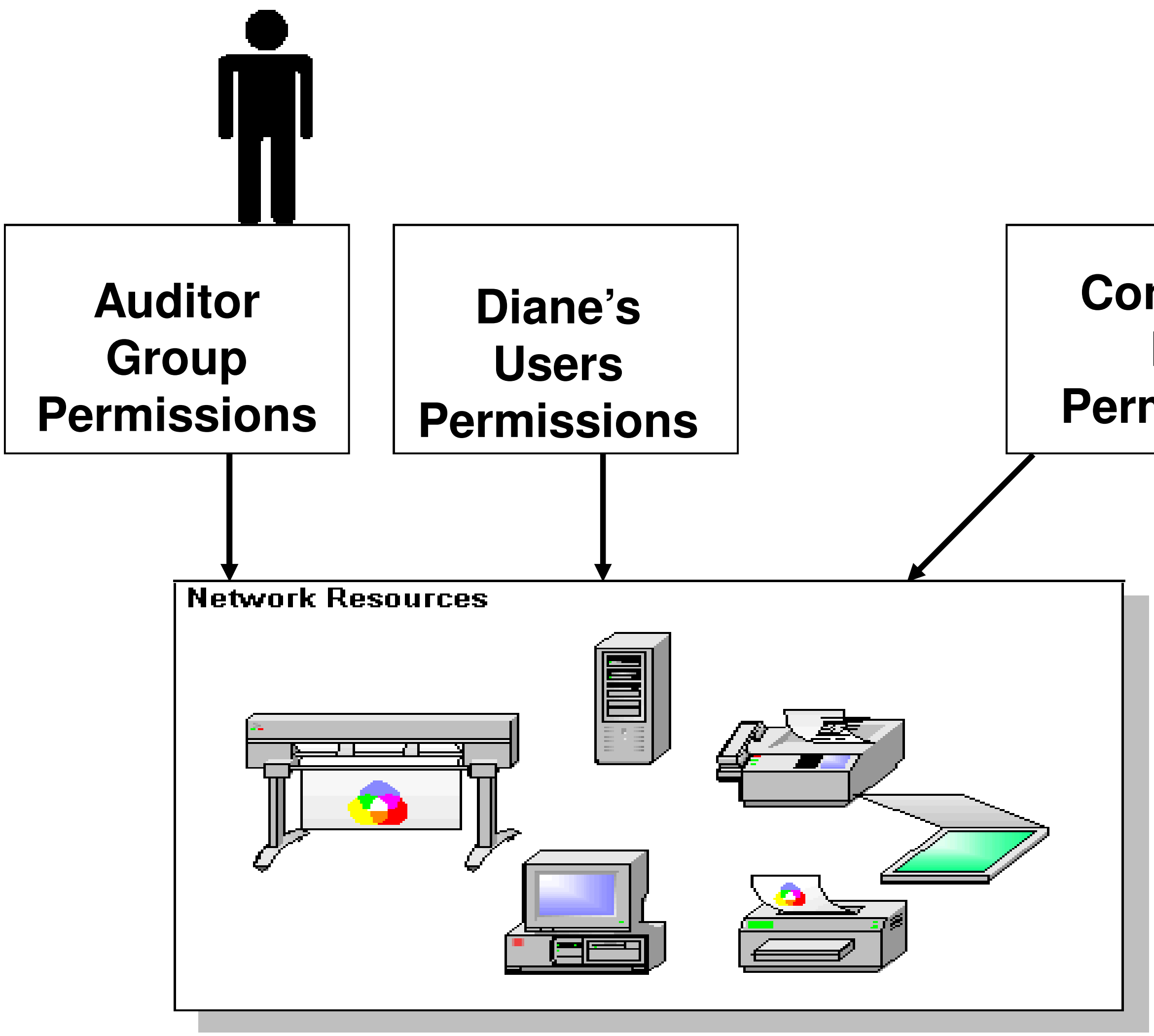


Role-Based Access Control

RBAC Characteristics

- Allows access to objects based on the role the user holds within the company
- Administrators assign a user to a role and then assign access rights to that role, not directly to the user
- This is best used in environments with a high rate of turnover of employees
- Roles can be based on
  - Role user fulfills in organization
  - Tasks user performs

Permissions Assigned to Role


Auditor Group Permissions
Diane’s Users Permissions
Contractor Role Permissions
Network Resources

Other Access Control Technologies

- Rule-based
- Restricted interface
- Content-dependent

Rule-based Access Control

Characteristics

- Security policy based on global rules imposed for all subjects

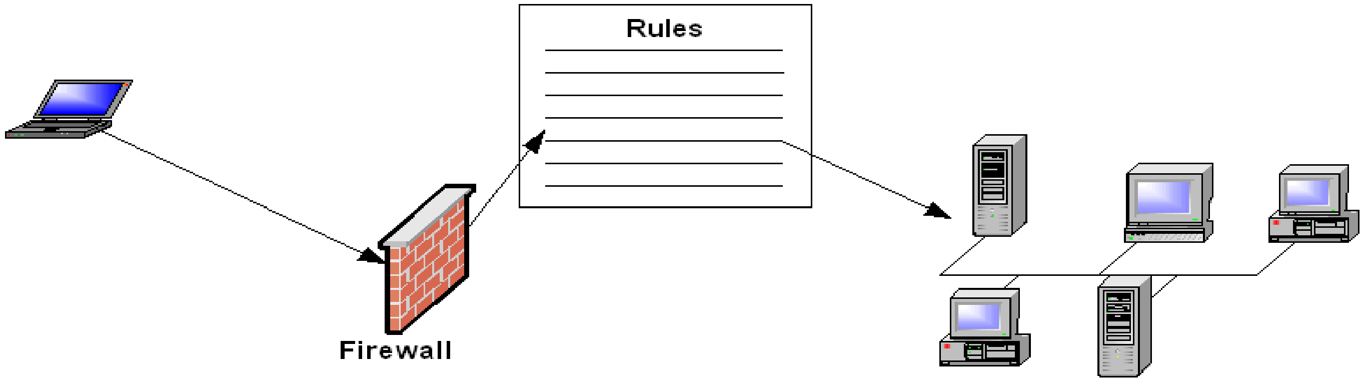
- Mandatory Access Control is an example of a Rule-based Access Control approach

Access Control Technique – Rule-based

Rule-based Access

- Rule-based Access Control techniques are based on specific rules that indicate what can and cannot happen to an object

- Access is not necessarily granted based on subject's identity



ccess

Access Control Technique

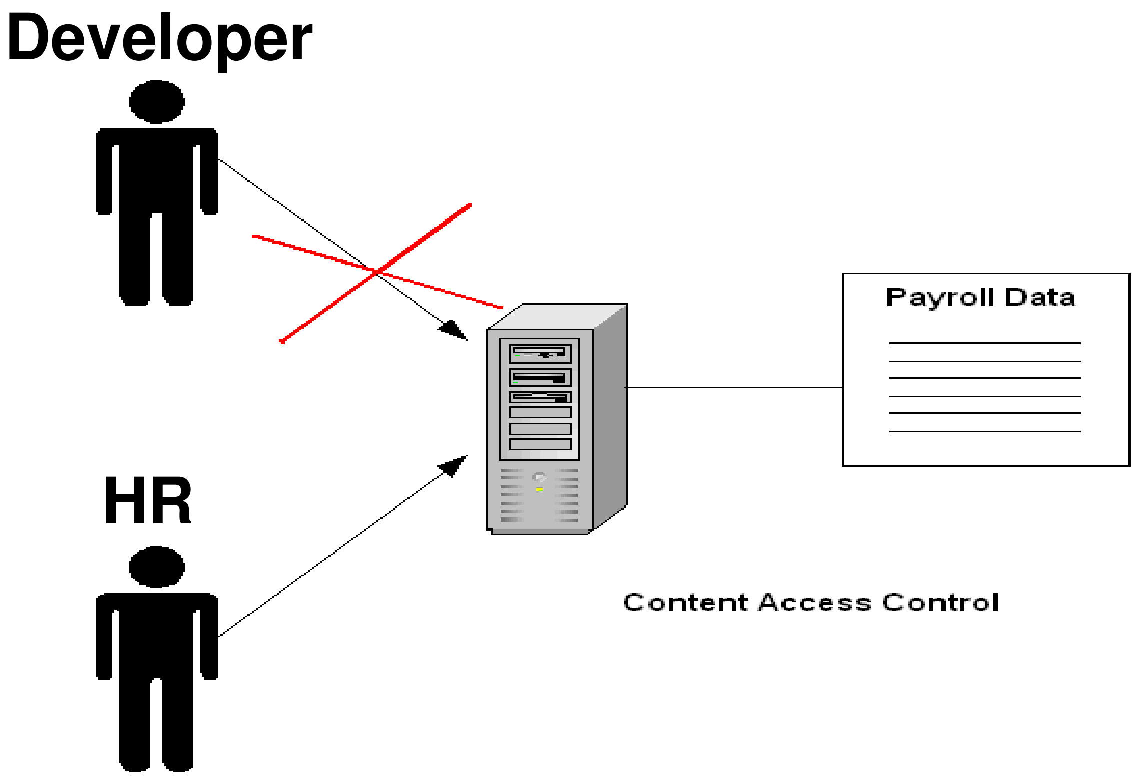
Restricted Interfaces

- Menus – only the functions that the administrator wants a user to be able to perform are provided in a menu.
- Shells – only the commands that the administrator wants a user to be able to run will be available in the shell environment.
- Database Views – databases can be configured to only show certain information to different users, depending upon their credentials.
- Physically Constrained – only providing a limited keypad or touch buttons on a screen as in ATM machines
- Encryption – requires a decryption key to unmask sensitive information.

Access Control Technique

Content-dependent Access Control

- Access to objects can be determined by the sensitivity of the content within the objects



Access Control Matrix Model

Model Characteristics

- Two-dimensional matrix representing subjects in rows and objects in columns
- Specifies the operations and access rights allowed for each subject as it relates to specific objects
- Operating systems implement this model in
  - Capabilities
  - Profiles
  - Access Control Lists

Access Control Matrix Implementations

Capabilities

- Capability identifies the object and specifies the subject’s access rights
- Bound to the subject
- Row-based within matrix

Profiles

- List of objects associated with each subject
- Detailed description of a subject’s environment
- Each object’s name must be unique, and full pathnames must be used
- Profiles must be checked for each access attempt
- A lot of overhead and, as the objects increase, so does the complexity

Access Control Technique

Capability Table and ACL's

- A capability table specifies the access rights a certain subject possesses pertaining to specific objects

- Access Control Lists (ACL's) are used to authorize a subject to access an object

Capability Table and ACL's

Capabilities Table

Plotter – Print

Printer1- Print

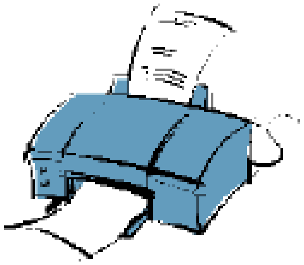
Printer2 - No Access

Accounting.xls – Full Control

Accounting.doc – Read Write

Payroll.xls – No Access

Clipart – Full Control



Access Control Lists

Tom Harris – Print

Dan Swenson – Full Control

Maynard Harris – No Access

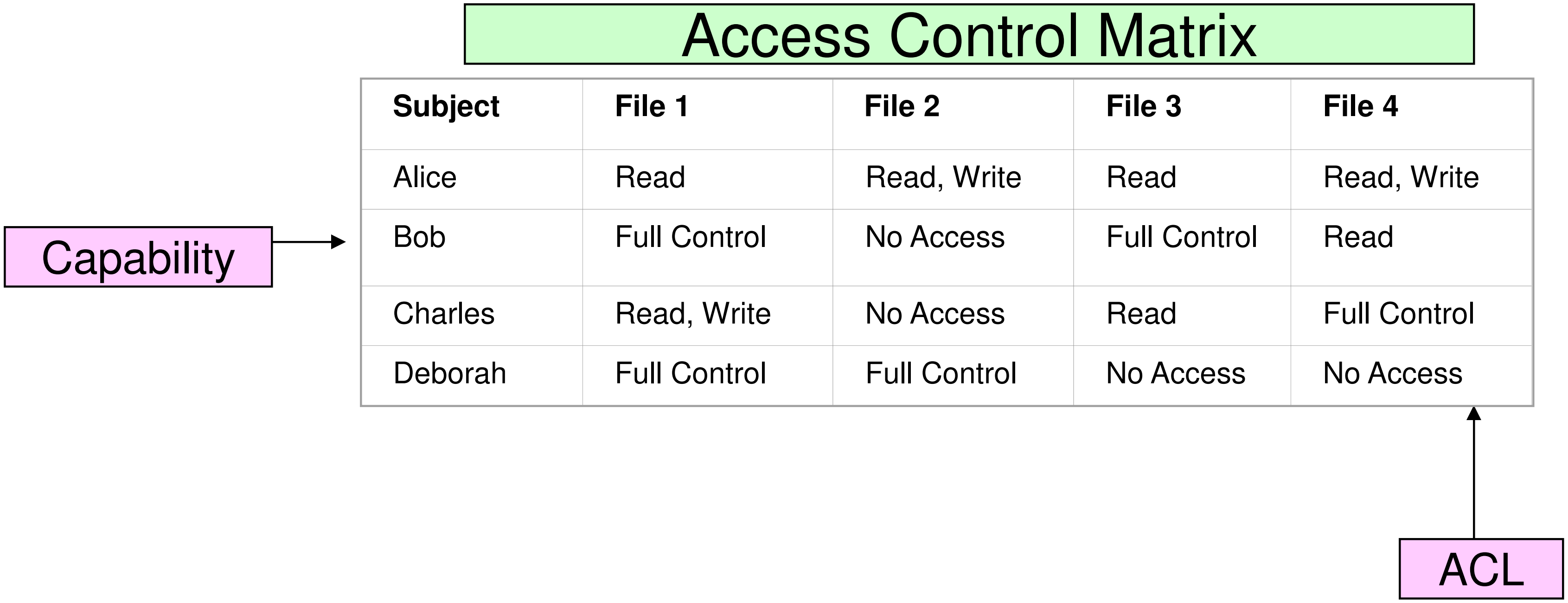
Evelyn Seaton- Print

Iqqi Hammond – Full Control

David Arnold - Print

Capability and ACL Relationship

- Capability – a row in the matrix
- ACL – a column in the matrix



Access Control Matrix

Subject	File 1	File 2	File 3	File 4
Alice	Read	Read, Write	Read	Read, Write
Bob	Full Control	No Access	Full Control	Read
Charles	Read, Write	No Access	Read	Full Control
Deborah	Full Control	Full Control	No Access	No Access

Capability

ACL

What is Identity Management

- **Set of technologies that offers greater ease and flexibility to manage users.**
- **Host**
  - The system, User, Application, or service providing an interface for Identification and Authentication
- **Requestor**
  - Sometimes referred to as Network Access Server (NAS), it provides a challenge to the host
- **Authenticator**
  - The systems that performs the validation of User’s Credentials.

Goal of Identity Management

ID management addresses Identity in the business context instead of the Security Context. Goals are:

- Integrity and Non-Repudiation
- Confidentiality
- Authentication and Authorization
- Identity Provisioning
- Representing and Managing Authorization Policy
- Allows Interoperability
- Makes use of standards
- A lot more than user management

Who can use Identity Management

- Operating Systems
- Servers
- Users
  - Employee, Contractors, Partners, Vendors, Customers
- Human Resource
- Payroll
- Different Applications
- Customer Relationship Management (CRM)
- E-Commerce
- Enterprise Resource Management Systems Planning (ERP)

Example of Identity Management

- **Microsoft Passport**
  - One name for all passport enable sites and services
- **Liberty Alliance**
  - Consortium of vendors
  - Privacy, Security, and Trust is maintained
  - Universal Open Standard for Single Sign-on
  - Decentralized authentication
  - Support multiple providers, could be state level ID
- **Open ID**
  - Google, IBM, Microsoft, VeriSign, and Yahoo
  - Single online identity

Benefits of Identity Management

- **Reduce Duplication of user accounts**
  - A single profile for access to all systems
- **Reduce number of Orphan Accounts**
- **Reduce number of passwords being used**
- **Can scale to VERY large enterprises**
- **Work with Single Sign-On**
- **Can be viewed as Super Sign-On**
  - From one company to another
  - From one service provider to another
  - Can be federated to VERY large scale
  - B2B, B2C, etc…

Lexicon of ID Management (1 of 2)

- **Subject**
  - Person, Group, corporation, software program, or other entity making a request to access a resource (Object)
- **Resource (Object)**
  - Web Page, Database Data, File, Transaction
- **Attributes**
  - Medical History, Past purchases, bank balance, credit rating, dress size, age, sex, and so on.
- **Preferences**
  - Desires such as Airline Seat, Brand Name, Use of a specific crypto Standard, Currency, Color, and so on

Lexicon of ID Management (2 of 2)

Traits

- Features of the Subject that are Inherent
- Blue Eyes, How and Where a company was formed

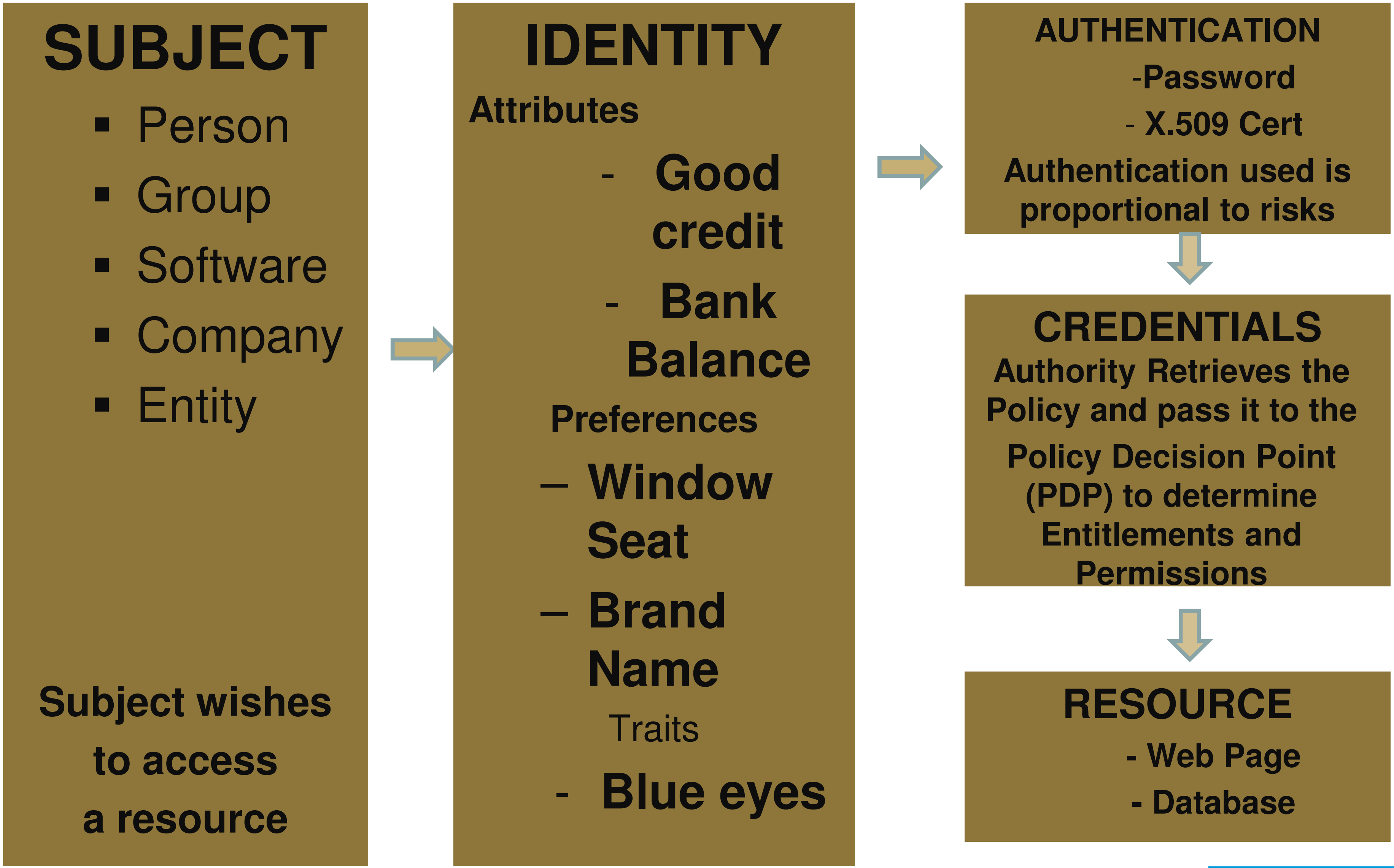
Identity

- Collection of data representing Attributes, Preferences, and Traits
- Needed to access a resource

Credentials

- Proof that a subject can assert a particular identity.
- A way of transferring trust between Identities
- Must present credentials to access a resource

Overview of ID Management



SUBJECT

- Person
- Group
- Software
- Company
- Entity

Subject wishes to access a resource

IDENTITY

Attributes

- **Good credit**
- **Bank Balance**

Preferences

- **Window Seat**
- **Brand Name**

Traits

- **Blue eyes**

AUTHENTICATION

-Password

- X.509 Cert

Authentication used is proportional to risks

CREDENTIALS

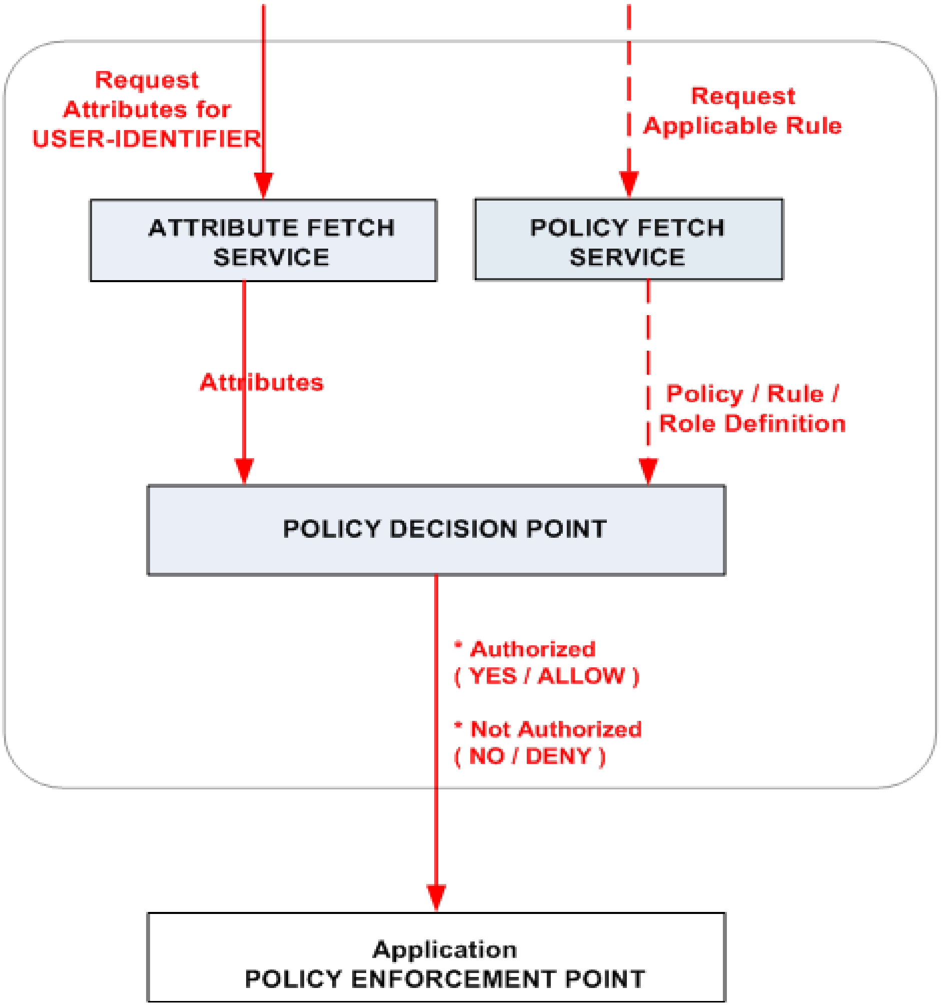
Authority Retrieves the Policy and pass it to the Policy Decision Point (PDP) to determine Entitlements and Permissions

RESOURCE

- Web Page

- Database

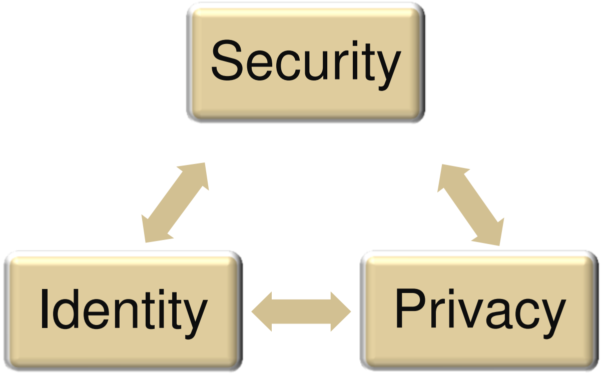
Entitlement and Permissions



Graphic from:
http://middleware.internet2.edu/

- Entitlement
  - Services Allowed
  - Resources Allowed
    - Bandwidth
    - Disk Space
    - Credit Limit
- **Permissions**
  - Actions allowed
    - Withdraw Funds
    - Complete Purchase
    - Update a record

The Identity, Security, Privacy Triangle



Privacy prevent an Identity from being disseminated beyond the subject need for a particular transaction.

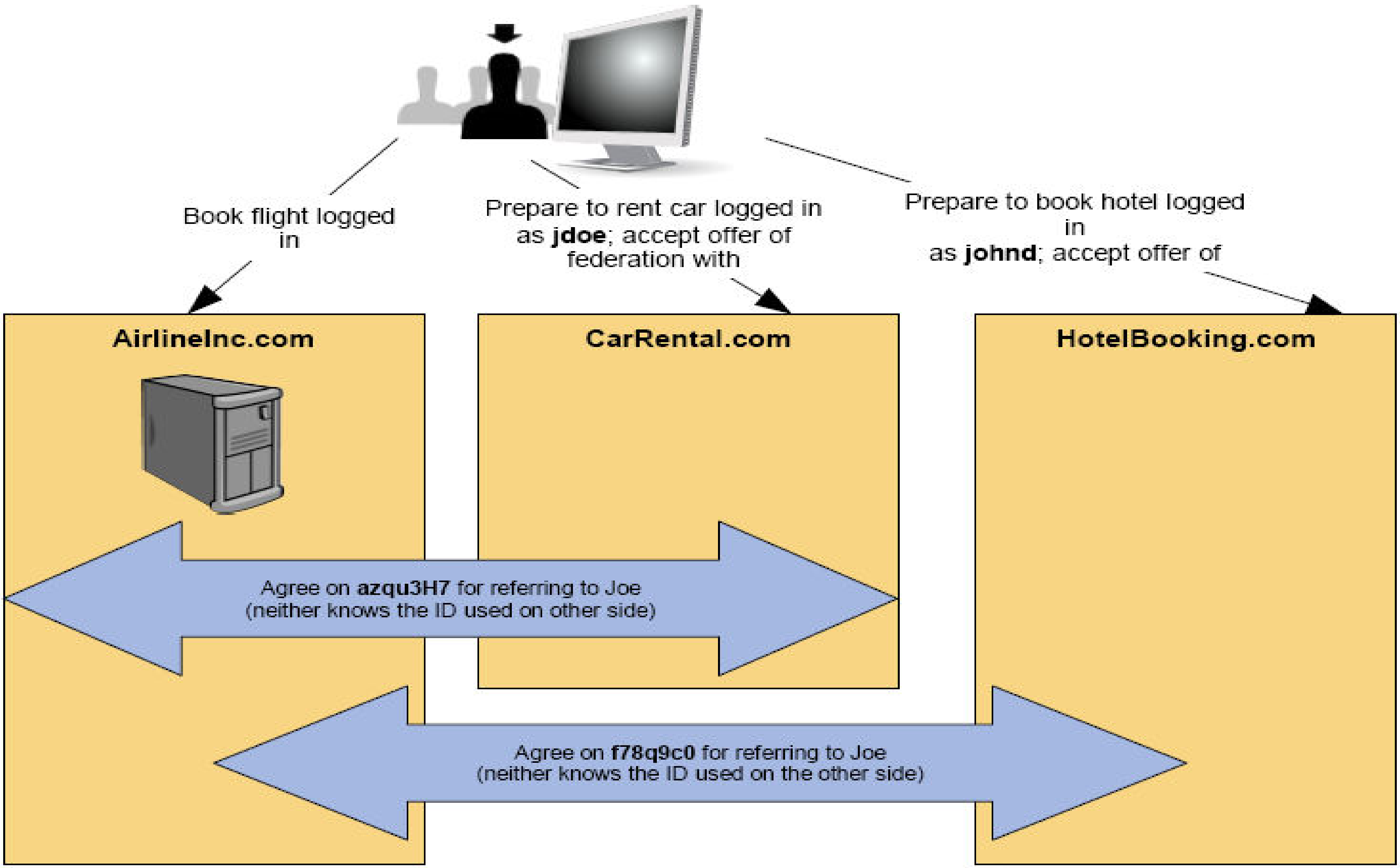
- **Security Protects CIA against:**
  - Unauthorized Access
  - Destruction
  - Alteration
- **Privacy Protects your Identity:**
  - Attributes
  - Preferences
  - Traits
  - Relies on Identity Management
- **Identity Ensures:**
  - Identification
  - Authorization
  - Access Control to resources

Security Assertion Markup Language

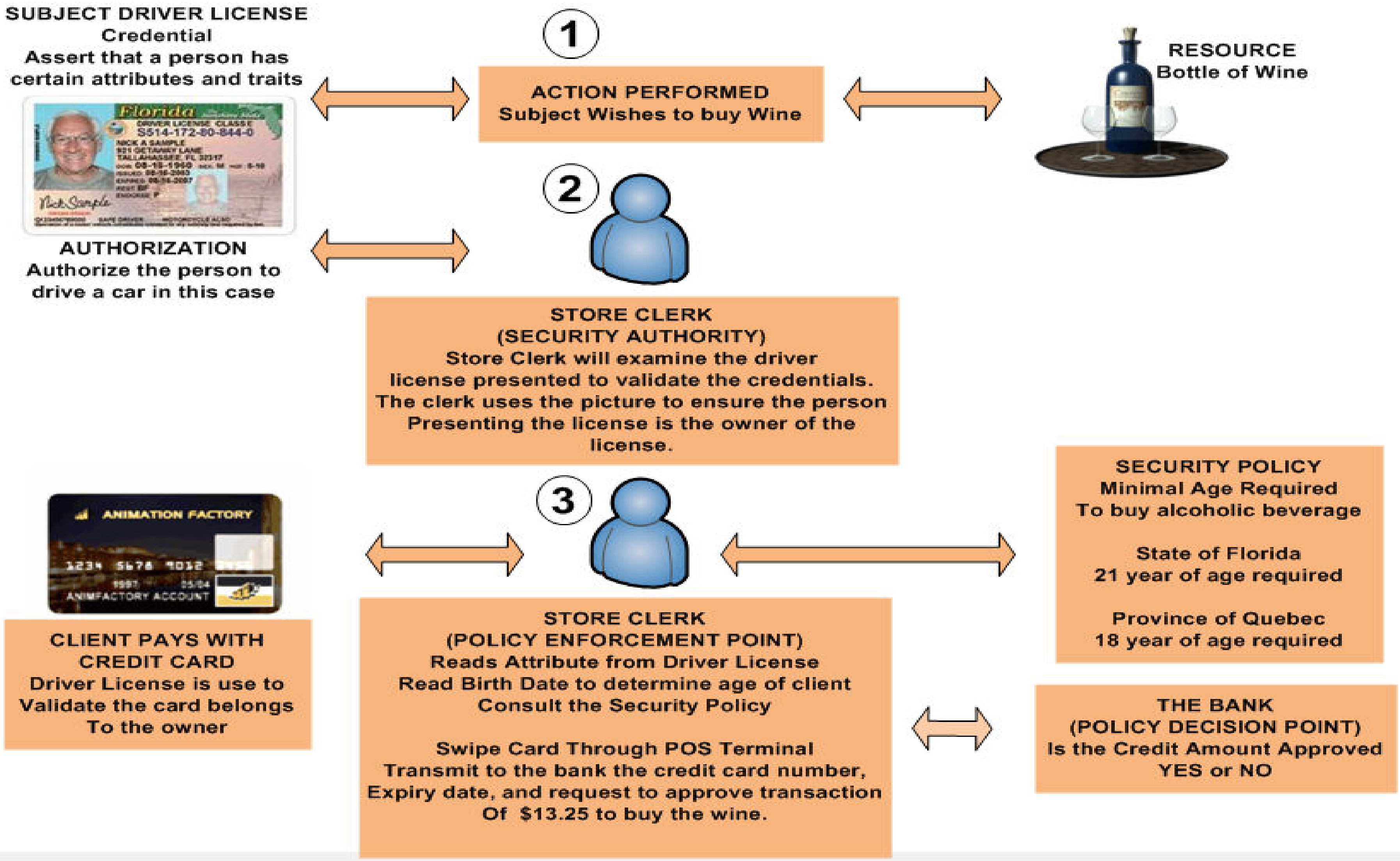
SAML

- Framework for authorization and authentication
- Allow exchange of security information between vendors
- Provides
  - Single Sign-On
  - Federated Identity
  - Web Services
  - SOAP (Simple Object Access Protocol)
  - Credential Transport in a SOAP Message
    - Uses Web Service Security (WS-Security)
  - XML Signature
    - For Integrity and Authentication
    - Non-Repudiation with PKI infrastructure
  - XML Encryption

Federated Identity


Book flight logged in
Prepare to rent car logged in as **jdoe**; accept offer of federation with
Prepare to book hotel logged in
as **johnd**; accept offer of
AirlineInc.com
CarRental.com
HotelBooking.com
Agree on **azqu3H7** for referring to Joe
(neither knows the ID used on other side)
Agree on **f78q9c0** for referring to Joe
(neither knows the ID used on the other side)

Overview of a Transaction



SUBJECT DRIVER LICENSE
Credential
Assert that a person has
certain attributes and traits

AUTHORIZATION
Authorize the person to
drive a car in this case

ACTION PERFORMED
Subject Wishes to buy Wine

RESOURCE
Bottle of Wine

STORE CLERK
(SECURITY AUTHORITY)
Store Clerk will examine the driver
license presented to validate the credentials.
The clerk uses the picture to ensure the person
Presenting the license is the owner of the
license.

SECURITY POLICY
Minimal Age Required
To buy alcoholic beverage

State of Florida
21 year of age required

Province of Quebec
18 year of age required

CLIENT PAYS WITH
CREDIT CARD
Driver License is use to
Validate the card belongs
To the owner

STORE CLERK
(POLICY ENFORCEMENT POINT)
Reads Attribute from Driver License
Read Birth Date to determine age of client
Consult the Security Policy

Swipe Card Through POS Terminal
Transmit to the bank the credit card number,
Expiry date, and request to approve transaction
Of $13.25 to buy the wine.

THE BANK
(POLICY DECISION POINT)
Is the Credit Amount Approved
YES or NO

Agenda

- Control access by applying concepts/ methodologies/ techniques
- Understand access control attacks
- Assess effectiveness of access controls
- Identify and access provisioning lifecycle

Log Protection

➡ Log Issues

- Attackers usually try to “scrub” logs to cover their tracks, thus only administrators should have access to them
- Integrity of logs can be protected with hashing algorithms, digital signatures, and host IDS
- Their confidentiality can be protected by storing them encrypted
- They can be stored on write-once media

Attacks on Access Controls

Unauthorized Disclosure of Information

- It can happen intentionally or unintentionally
- Object reuse
- Keyboard monitoring
- Electrical signals

Impersonation (spoofing / masquerading)

- Social engineering
- Fictitious Subscriber

Rogue Infrastructure

Replay Attacks

Social Engineering

- **Tricking someone into giving up confidential information**
  - Pretending to be a repair man
  - Spoofing e-mail
  - Impersonating another person

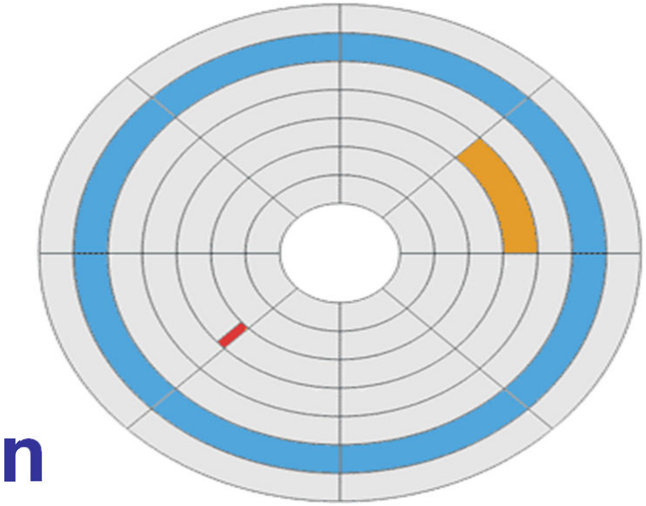
Prevent Unauthorized Disclosure

Object Reuse

- Reassigning media once it has contained sensitive information
- Media should be cleared of any residual information before given to another subject
- Many times easier than it sounds
- Degaussing may be required
- Physically destroying

Deleting a File or Formatting a Disk

- Object reuse
- Data remnants
- Clearing – Same organization
- Purging – For outside use
  - Degauss (electro-magnetic)
  - Zeroize (software overwrite)



Tracks and Cylinders

Sectors

Cluster/Block

Slack Space

Auditing Mechanism

Keystroke Monitoring

- Keystroke monitoring can be used legally to uncover bad deeds

- It can be used by attackers to capture authentication credentials

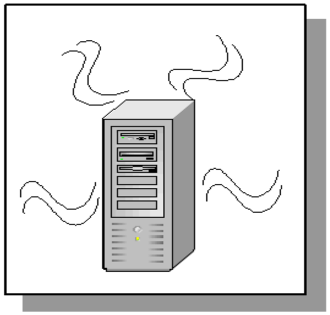
Unauthorized Disclosure

Emanation Security

- All electronic devices emit electronic radiation
- With the right equipment, an attacker can capture this data and reassemble it back into its original format, thus accessing data in an unauthorized manner
- There are three main countermeasures to protect from this type of compromise
  - TEMPEST, white noise, and control zones
- Today the word TEMPEST is not used as frequently
  - This branch of security is now referred to as Emission Security (EMSEC)

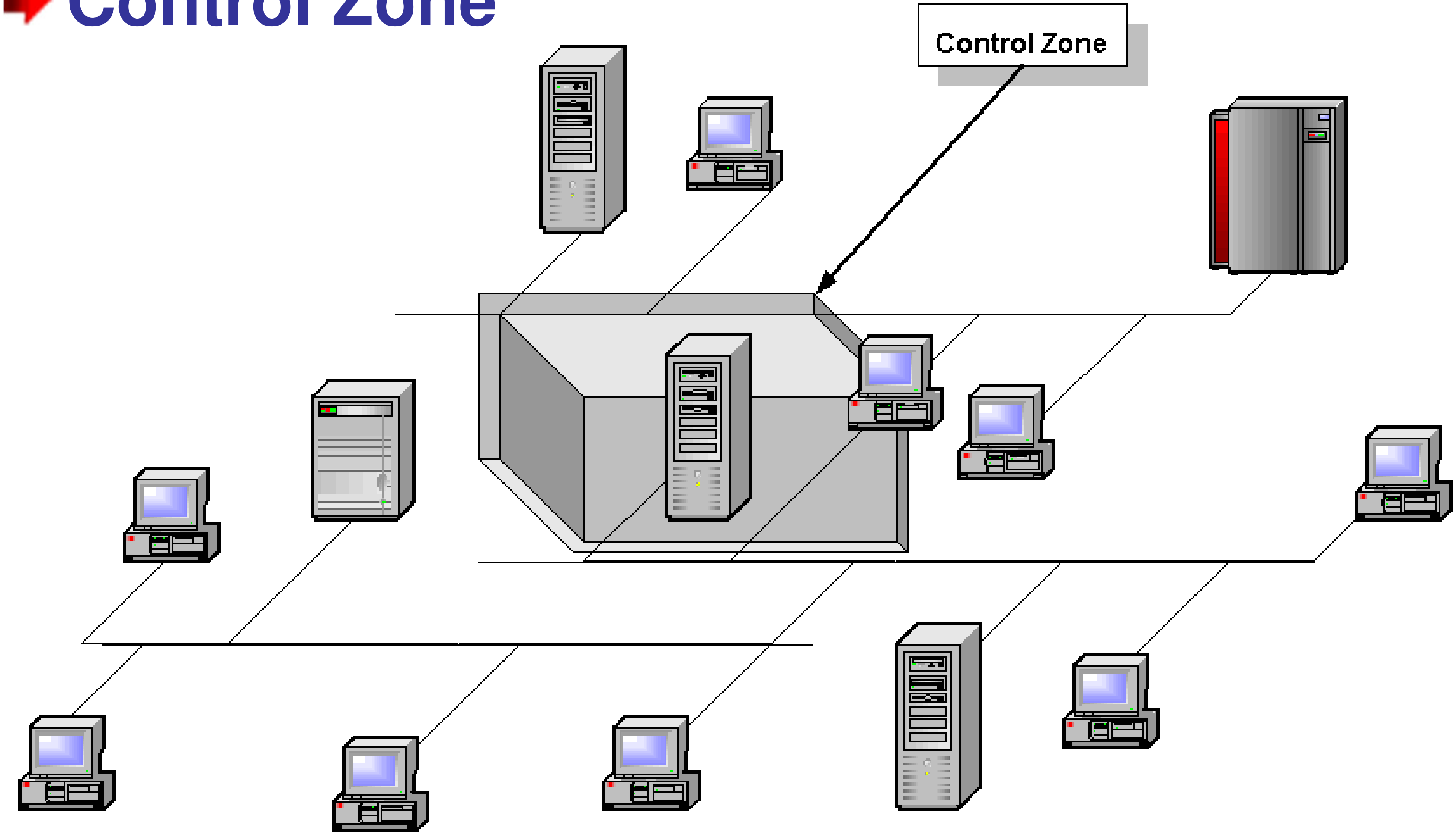
Control Against Signal Capture: TEMPEST

- A study and control of spurious electrical signals emitted
- Vendors must meet TEMPEST standard if they want their product to be considered a TEMPEST product
- Special shielding in equipment to lower amount of radiation leakage
  - Faraday cage is usually heavy metal casing
- Technology is complex and expensive, thus only used in high security areas



Controlling Signals

Control Zone

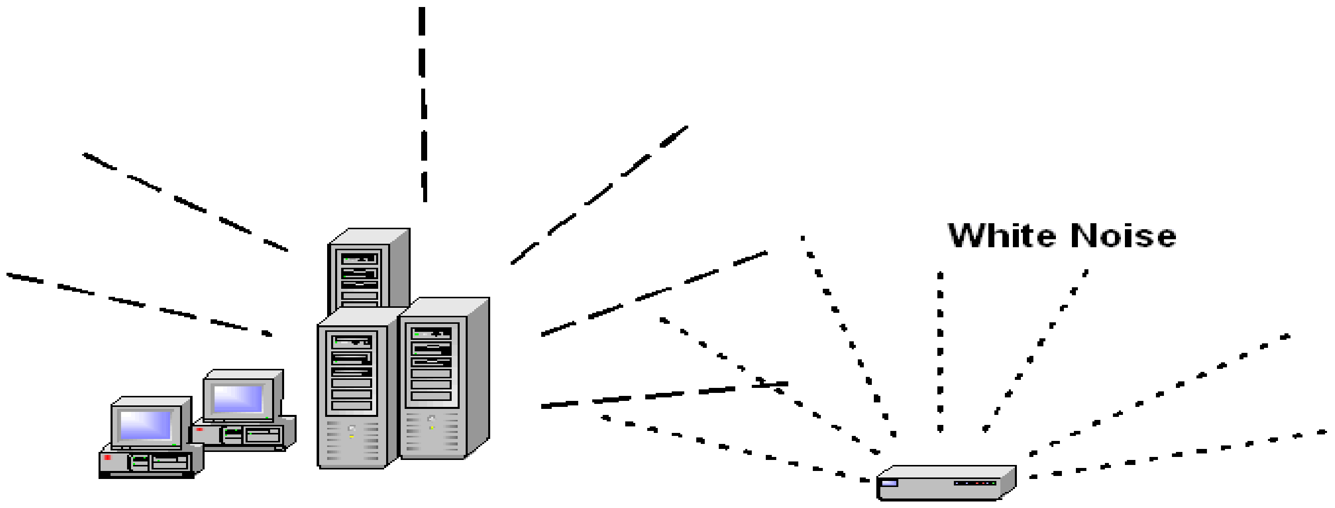


Control of Unauthorized Disclosure

White Noise

- A uniform spectrum of random electrical signals, which confounds an intruder's attempt to decipher real information from random noise

- Jamming the signal



Attacks on Passwords

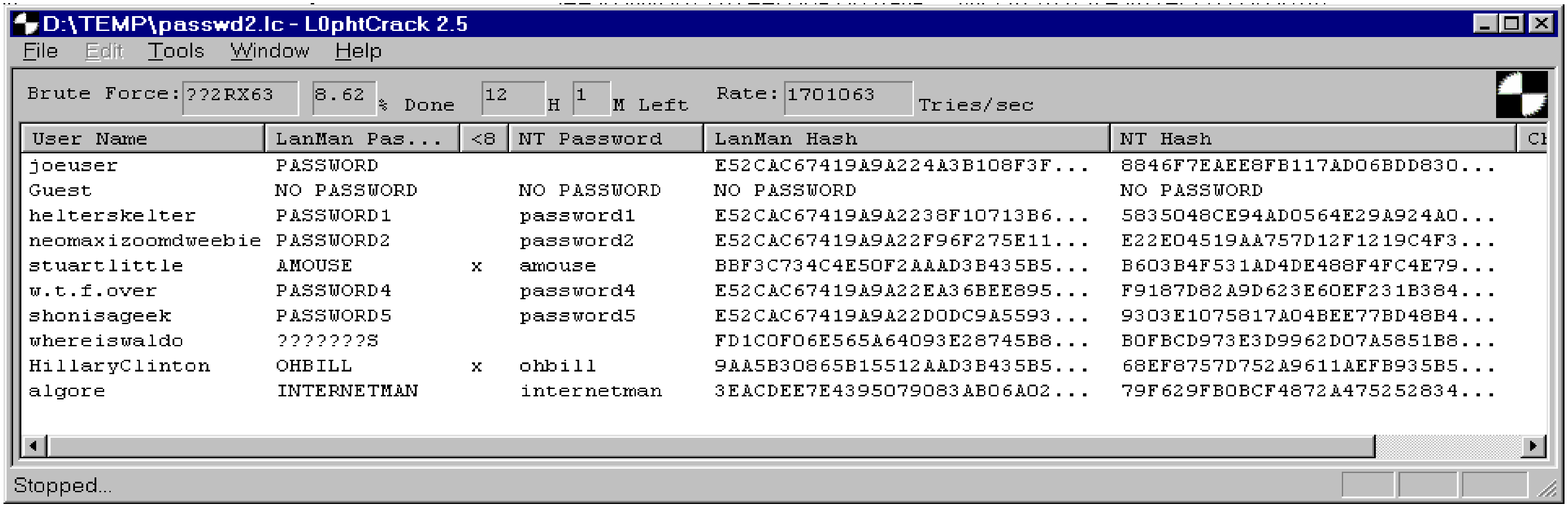
A Dictionary Attack

- Program with a file of passwords

A Brute Force Attack

- Program that tries different characters, not words

Hybrid Attacks



Brute Force: ??2RX63 8.62 % Done 12 H 1 M Left Rate: 1701063 Tries/sec

User Name	LanMan Pas...	<8	NT Password	LanMan Hash	NT Hash	Ch
joeuser	PASSWORD			E52CAC67419A9A224A3B108F3F...	8846F7EAEE8FB117AD06BDD830...	
Guest	NO PASSWORD		NO PASSWORD	NO PASSWORD	NO PASSWORD	
helterskelter	PASSWORD1		password1	E52CAC67419A9A2238F10713B6...	5835048CE94AD0564E29A924A0...	
neomaxizoomdweebie	PASSWORD2		password2	E52CAC67419A9A22F96F275E11...	E22E04519AA757D12F1219C4F3...	
stuartlittle	AMOUSE	x	amouse	BBF3C734C4E50F2AAAD3B435B5...	B603B4F531AD4DE488F4FC4E79...	
w.t.f.over	PASSWORD4		password4	E52CAC67419A9A22EA36BEE895...	F9187D82A9D623E60EF231B384...	
shonisageek	PASSWORD5		password5	E52CAC67419A9A22D0DC9A5593...	9303E1075817A04BEE77BD48B4...	
whereiswaldo	???????S			FD1C0F06E565A64093E28745B8...	B0FBCD973E3D9962D07A5851B8...	
HillaryClinton	OHBILL	x	ohbill	9AA5B30865B15512AAD3B435B5...	68EF8757D752A9611AEFB935B5...	
algore	INTERNETMAN		internetman	3EACDEE7E4395079083AB06A02...	79F629FB0BCF4872A475252834...	

Stopped...

Agenda

- Control access by applying concepts/ methodologies/ techniques
- Understand access control attacks
- Assess effectiveness of access controls
- Identify and access provisioning lifecycle

Accountability

Auditing

- Ensure that users are accountable for their actions
- Verify that the security policies are enforced
- Detect malicious activity
- Ability to undertake preventive measures when attacks are detected
- Used as investigation tools

Auditing Types

- Real-time – intrusion detection system
- Non-real-time – reviewing logs
- A well-protected environment would use both types

Agenda

- Control access by applying concepts/ methodologies/ techniques
- Understand access control attacks
- Assess effectiveness of access controls
- Identify and access provisioning lifecycle

Access Control Administration

Steps of Access Control

- Company decides upon the access control model they will implement (DAC and MAC)
- The technologies and techniques that will be used within that model are decided upon
- Next decision is how access will actually be managed
  - Centralized
  - Decentralized
  - Hybrid approach

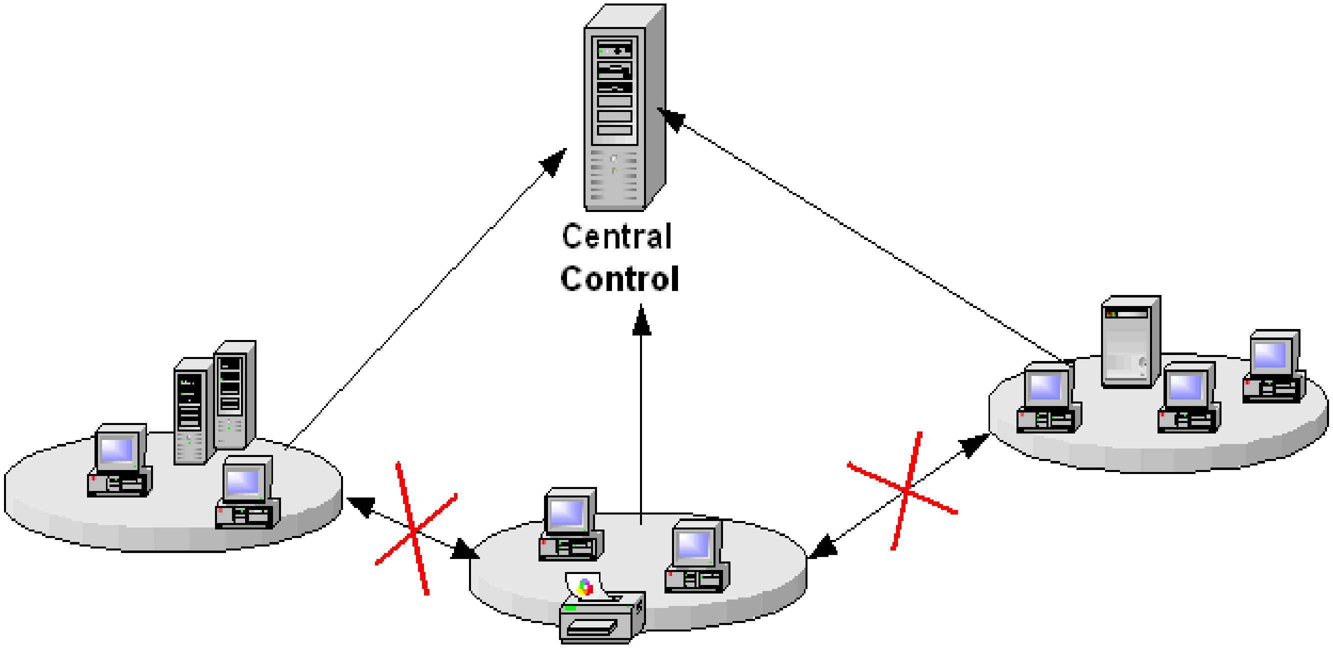
Access Control Administration

Centralized Access Control

- One entity (individual, department, or device) making access decisions
- Senior management decides what users can access specific objects, and the administration supports these directives
- Examples are RADIUS, TACACS+, and DIAMETER

Access Control Administration

Centralized Access Control

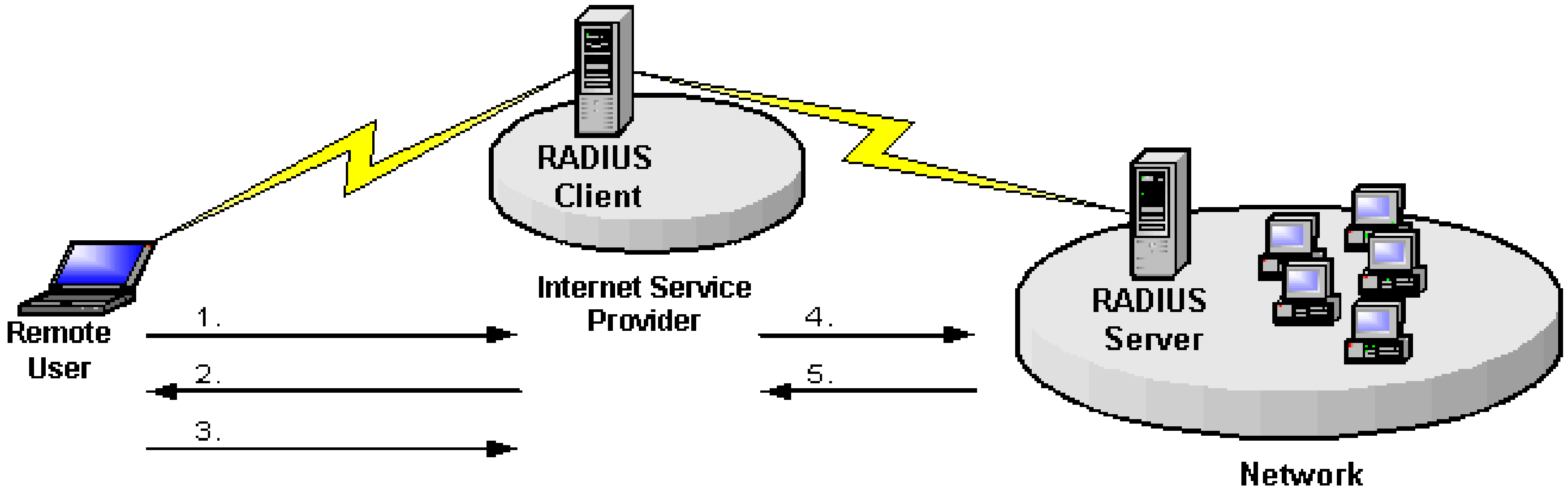


Centralized Access Control Administration

RADIUS

- Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that authenticates and authorizes users
- Handshaking protocol that allows the RADIUS server to provide authentication and authorization information to network server (RADIUS client)
- Users usually dial in to an access server (RADIUS client) that communicates with the RADIUS server
- RADIUS server usually contains a database of users and credentials
- Communication between the RADIUS client and server is protected

RADIUS Steps



1. User Initiates PPP authentication with ISP
2. RADIUS client prompts user for credential
3. User supplies credentials
4. RADIUS client sends credentials to RADIUS server
5. RADIUS server responds with Accept, Reject, or Challenge
6. If authentication is successful, RADIUS client allows access to network

Centralized Access Control Administration

TACACS+

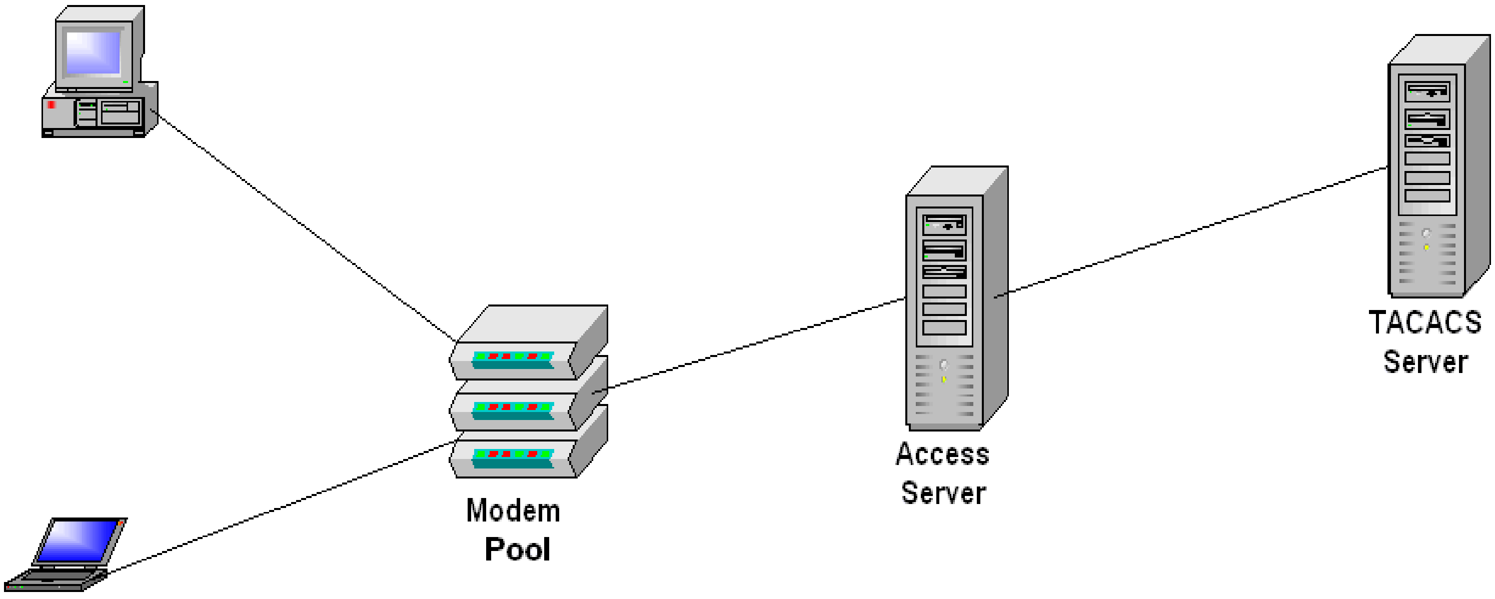
- Terminal Access Controller Access Control System (TACACS) is also an authentication protocol used to authenticate remote users

- Splits authentication, authorization, and auditing features

- Cisco proprietary protocol

Centralized Access Control Administration

TACACS+

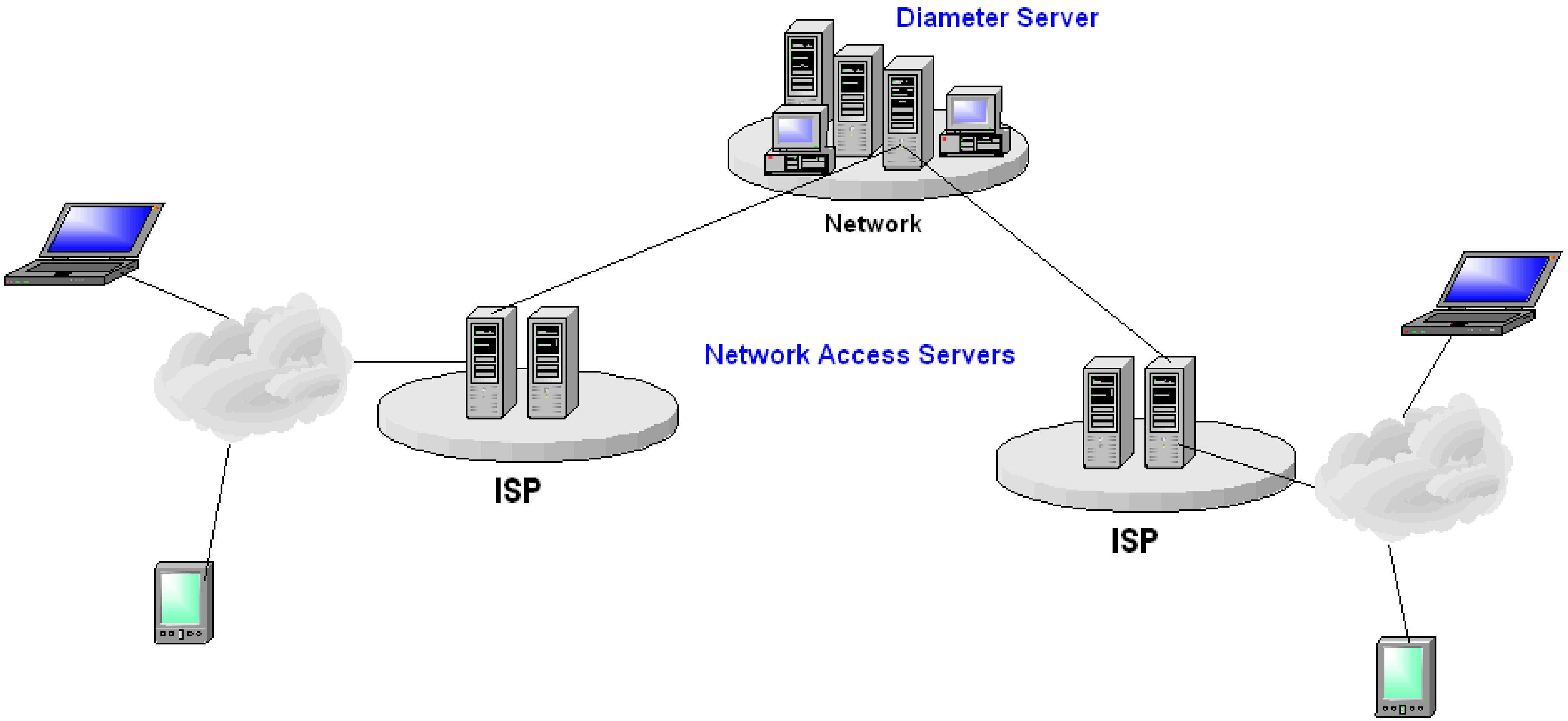


DIAMETER

Remote Authentication Protocol

- DIAMETER is a protocol designed as the next generation RADIUS
- RADIUS is limited to authenticating users via SLIP and PPP dial-up modem connections
  - Other device types use different protocol types
- Internet protocol that supports seamless and continuous connectivity for mobile devices - such as PDAs, laptops, or cell phones with Internet data capabilities
- Move between service provider networks and change their points of attachment to the Internet
- Including better message transport, proxying, session control, and higher security for AAA transactions

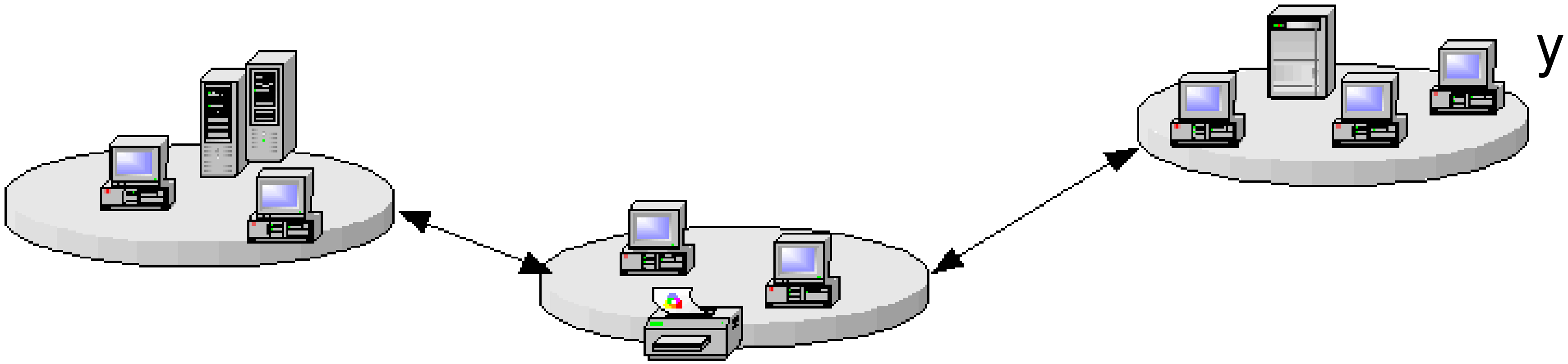
DIAMETER Authentication



Decentralized Administration

- Control is given to the people closer to the resource, as in department managers and sometimes users

- Access requests do not get processed by one centralized entity



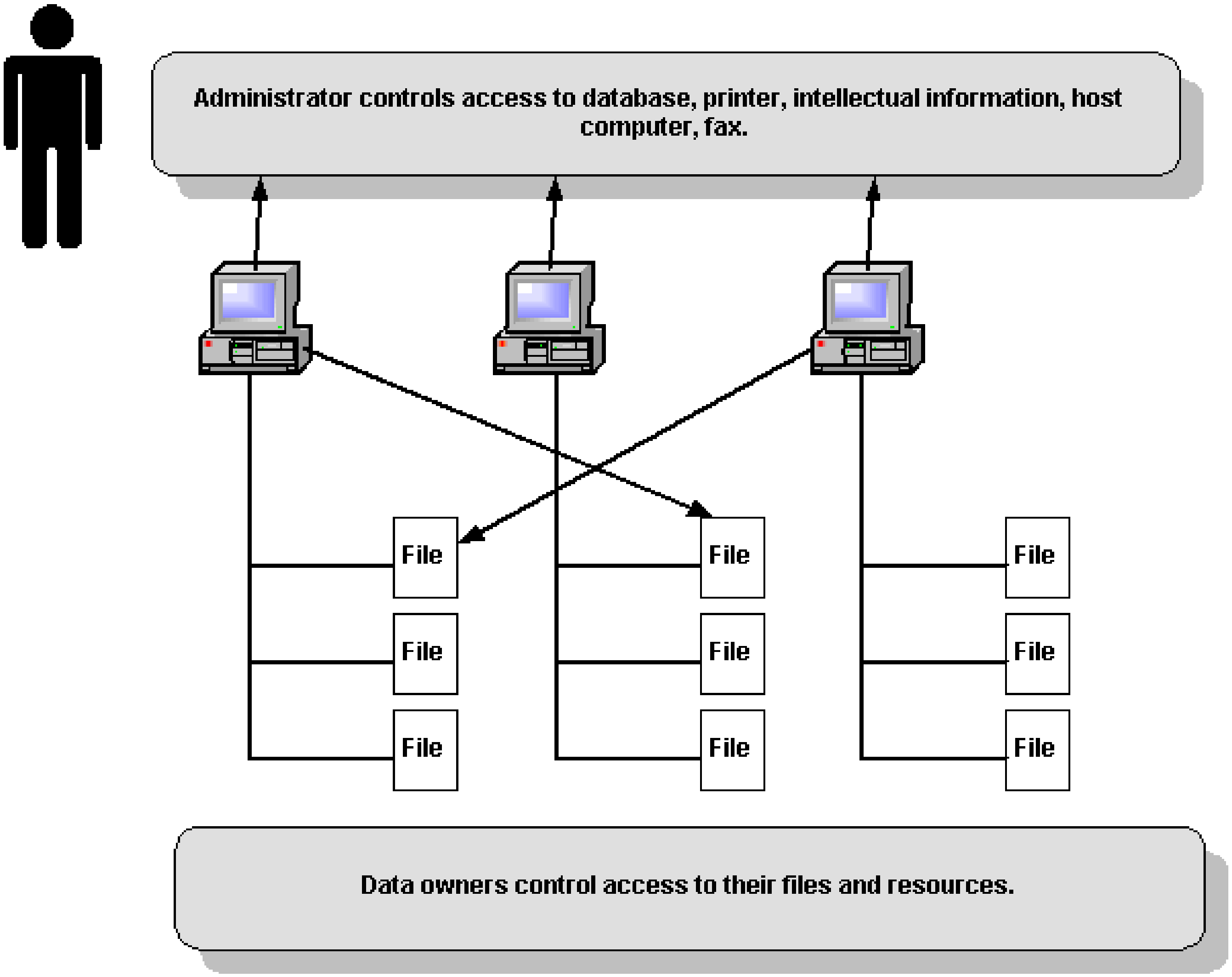
Hybrid Access Control Administration

- Combines centralized and decentralized administration methods

- One entity (network administrator) may control what users access
  - Important network resources

- Individual users are allowed to decide who accesses their own resources
  - Files, local printers

Hybrid Administration Approach



Administrator controls access to database, printer, intellectual information, host computer, fax.

Data owners control access to their files and resources.

Access Control Methodologies

Administrative:

- Group membership
- Time of day
- Transaction type

Technical:

- Directory Services
- Logical location

Physical:

- Physical location

Access Controls – Technical Layer

Technical Access Controls

- Directory Services
- Network Architecture
- Network Access
- Encryption
- Auditing

Technical Control – Directory Services

- X.500
- LDAP
- NDS
- Active Directory

Directory Services

- ISO published X.500 – LDAP adapts the directory to work over TCP/IP

- Hierarchical database is an inverted tree structure

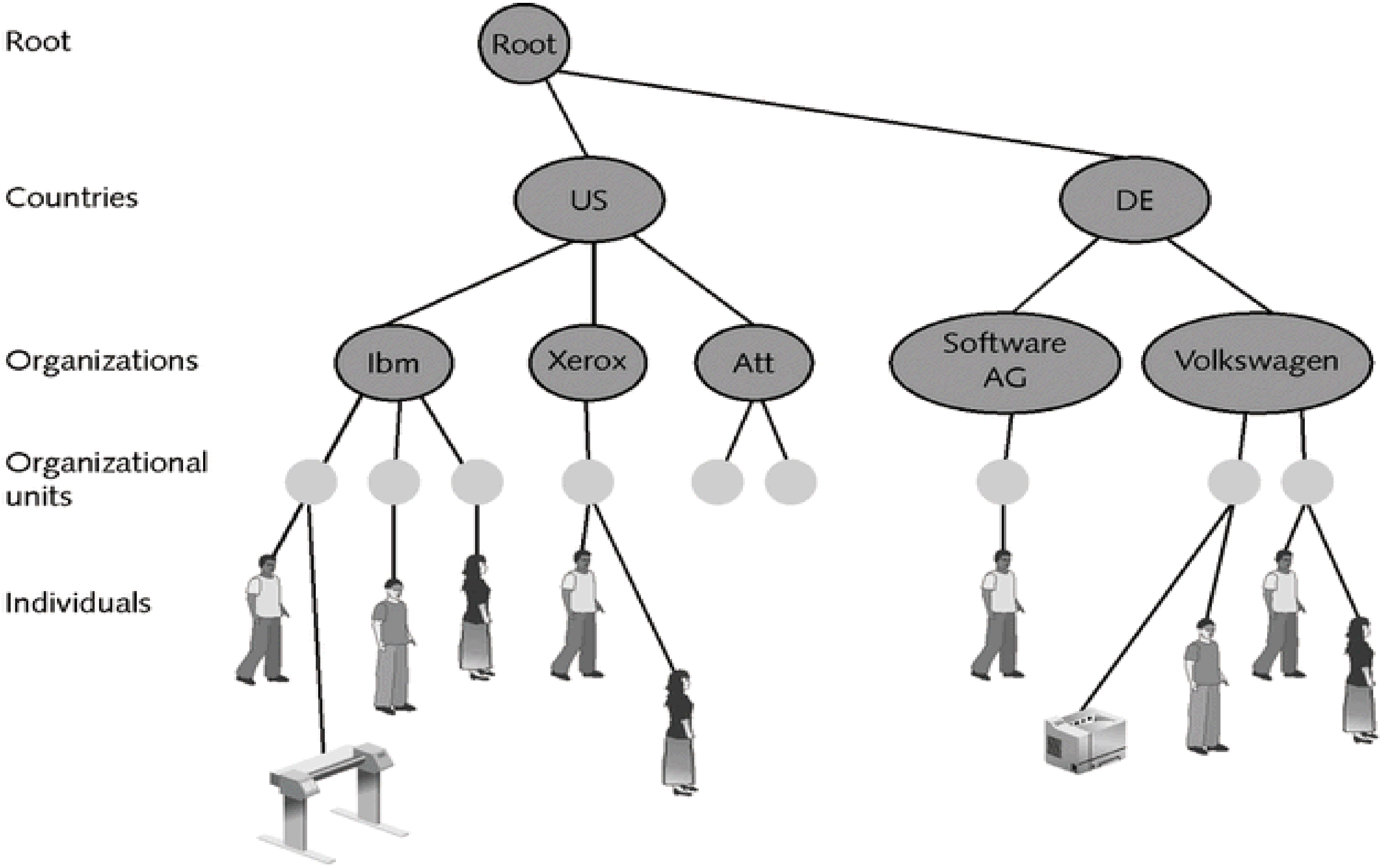
- Allows delegation of naming while maintaining (potentially) global uniqueness

Directory Service – LDAP

- The full name of a “leaf” on the tree, the Distinguished Name (DN), must be unique, and specified the path from the root of the tree to the “leaf”

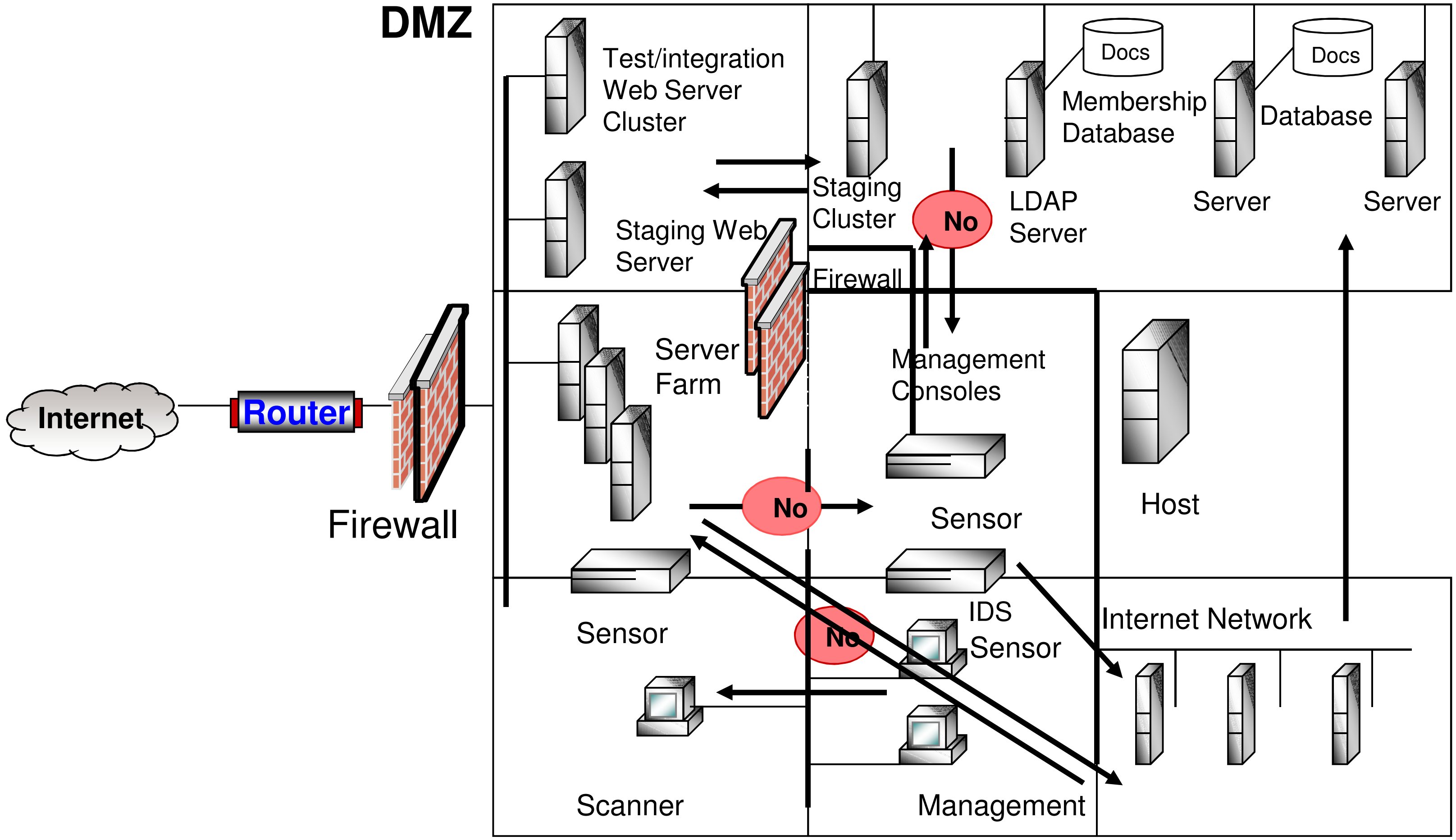
- If the “leaf is a user, we can store all sorts of things about this user:
  - Name
  - Location
  - Phone numbers
  - E-mail addresses
  - Digital certificates
  - Application or data access

Directory Tree



Technical Control – Network Design

Network Architecture

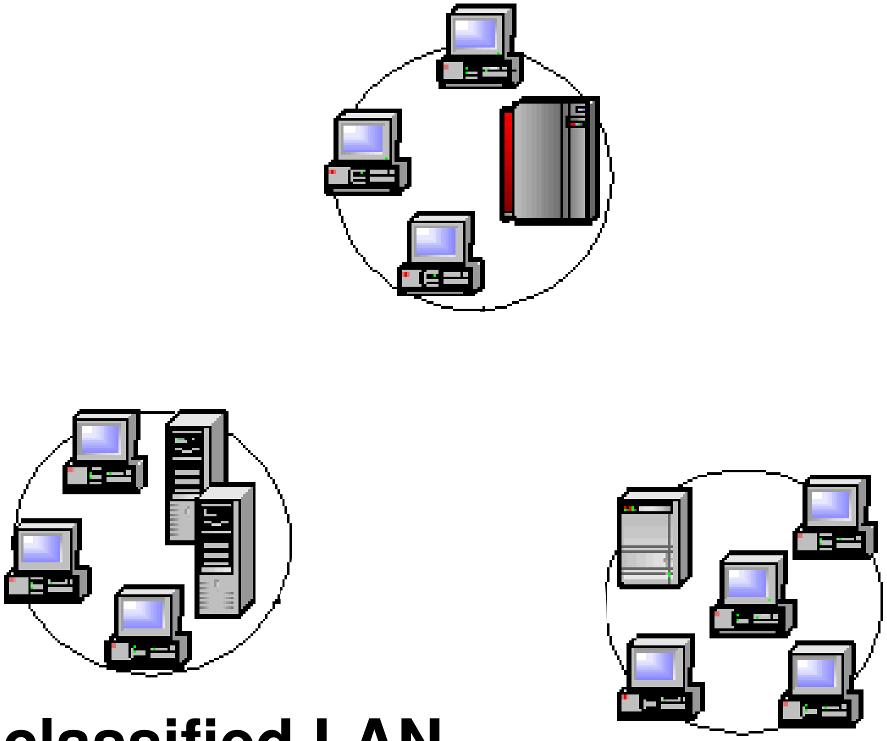


Access Controls – Physical Layer

Physical Controls

- Network Segregation
- Perimeter Security
- Computer Controls
- Work Area Separation
- Cabling

Physical Control – Network Segregation



Secret LAN

Unclassified LAN

Top Secret LAN

Bringing Things Together

- Access controls are the first line of defense
- They dictate how subjects access objects and resources
- Their main goal is to protect resources from unauthorized access
- The models are DAC, MAC, RBAC, and RuBAC
- The administration of the model can be centralized or decentralized
- The controls can be administrative, physical, or technical
- The controls can supply preventative, detective, and corrective services