

CISSP® Common Body of Knowledge Review: Access Control Domain

Version: 5.10



CISSP Common Body of Knowledge Review by Alfred Ouyang is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Course details

- Oral exam
- www.opensecuritytraining.info

Reference:

- *CISSP All-in-One Exam Guide*, 4th Ed., S. Harris, McGraw-Hill
- *Official (ISC)² Guide To The CISSP CBK*, H. Tipton and K. Henry, (ISC)² Press, Auerbach Publications
- William Stallings, Lawrie Brown - Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Wydanie IV. Tom 1 i 2, Helion 2019

• Contact information

Bogdan Księżopolski

www: ksiezopolski.pl

e-mail: bogan.ksiezopolski@acm.org

CISSP

- **Certified Information Systems Security Professional**
- CISSP CBK Review consists of 10 interdependent knowledge domains:
- Information Security and Risk Management Domain
- Security Architecture and Design Domain
- Telecommunications and Network Security Domain
- Operations Security Domain
- Cryptography Domain
- Physical Security Domain
- Software Development Security Domain
- Access Control Domain
- Business Continuity and Disaster Recovery Planning Domain
- Legal, Regulations, Compliance, and Investigation Domain

Access Control



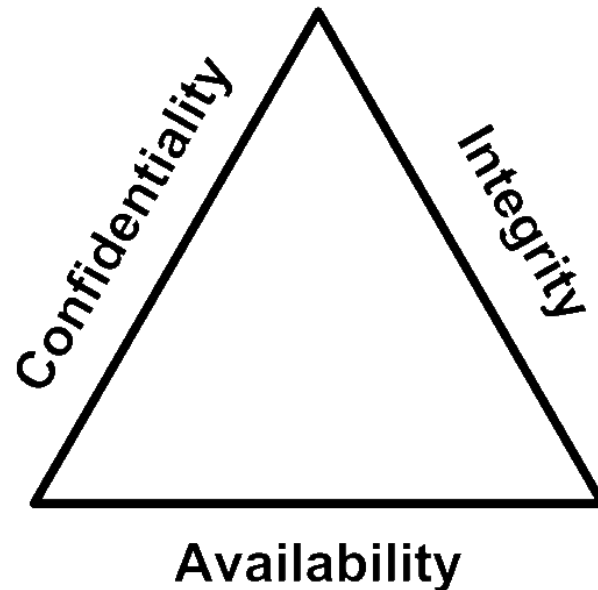
Definition & Principles

- Threats
- Types of Access Control
 - Identification, Authentication, Authorization, and Accountability
- Access Control Models
 - Security Models
 - Centralized & Decentralized/Distributed
- Monitor & Management
 - IPS & IDS
 - Security Assessment & Evaluation

Concepts of Confidentiality, Integrity, and Availability

Concepts of Confidentiality, Integrity, and Availability

- The primary goals and objectives of security are contained within the **CIA Triad**, which is the name given to the three primary security principles:
- Confidentiality
- Integrity
- Availability



Confidentiality

- If a security mechanism offers confidentiality, it offers a high level of assurance that data, objects, or resources are restricted from **unauthorized subjects**.
- Data must be protected from unauthorized access, use, or disclosure while in **storage, in process, and in transit**.
- **Attacks**: capturing network traffic and stealing password files as well as social engineering, port scanning, shoulder surfing, eavesdropping, sniffing,....
- **Countermeasures**: encryption, strict access control, rigorous authentication procedures, data classification, extensive personnel training,

Other „flavour” of confidentiality

- **Secrecy** - Secrecy is the act of keeping something a secret or preventing the disclosure of information.
- **Privacy** - Privacy refers to keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.

Integrity

- If a security mechanism offers integrity, it offers a high level of assurance that the data, objects, and resources are unaltered from their **original protected state**.
- Alterations should not occur while the object is in **storage, in transit, or in process**.

Integrity can be examined from three perspectives

- Preventing **unauthorized** subjects from making **modifications**
- Preventing **authorized** subjects from making unauthorized modifications, such as **mistakes**
- Maintaining the internal and external **consistency of objects** so that their data is a correct and true reflection of the real world and any relationship with any child, peer, or parent object is valid, consistent, and verifiable

Integrity

- **Attacks:** viruses, malicious modification, intentional replacement, system backdoors, human error, accidentally deleting files; entering invalid data; altering configurations, including errors in commands.
- **Countermeasures:** strict access control, rigorous authentication procedures, intrusion detection systems, object/data encryption, hash total verifications, extensive personnel training.

Availability

- **Availability** - authorized subjects are granted timely and uninterrupted access to objects. Availability includes efficient uninterrupted access to objects and prevention of denial-of-service (DoS) attacks.
- **Other aspects** of availability: usability, accessibility, and timeliness.
- **Attacks**: These include device failure, software errors, and environmental issues (heat, flooding, power loss), DoS attacks, object destruction, communication interruptionsm, ...

Availability - Countermeasures

- Designing intermediary delivery systems properly, using access controls effectively, monitoring performance and network traffic, using firewalls and routers to prevent DoS attacks, implementing redundancy for critical systems, and maintaining and testing backup systems.
- Most security policies, as well as business continuity planning (BCP), focus on the use of fault tolerance features at the various levels of access/ storage/ security (that is, disk, server, or site) with the goal of eliminating single points of failure to maintain availability of critical systems.

Nonrepudiation

- **Nonrepudiation** ensures that the subject of an activity or event cannot deny that the event occurred. Nonrepudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event.
- **Full Nonrepudiation** can be established using digital certificates,

Access Control

Access Control

- Access is the flow of information between a subject (e.g., user, program, process, or device, etc.) and an object (e.g., file, database, program, process, or device, etc.)
- Access controls are a collection of mechanisms that work together to protect the information assets of the enterprise from unauthorized access.
- Access controls enable management to:
 - Specify which user can access the resources contained within the information system
 - Specify what resources they can access
 - Specify what operations they can perform
 - Provide individual accountability

Reference:

- *CISSP All-in-One Exam Guide*, 4th Ed., S. Harris, McGraw-Hill
- *Official (ISC)² Guide To The CISSP CBK*, H. Tipton and K. Henry, (ISC)² Press, Auerbach Publications

Security Implementation Principles for Access Control

- Least privilege is a policy that limits both the system's user and processes to access only those resources necessary to perform assigned functions.
 - Limit users and processes to access only resources necessary to perform assigned functions
- Separation of duties means that a process is designed so that separate steps must be performed by different people (i.e. force collusion).
 - Define elements of a process or work function
 - Divide elements among different functions

Categories of Security Controls

- Management (Administrative) Controls.
 - Policies, Standards, Processes, Procedures, & Guidelines
- Operational (and Physical) Controls.
 - Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
 - Physical Security (Facility or Infrastructure Protection)
 - Locks, Doors, Walls, Fence, Curtain, etc.
 - Service Providers: Guards, Dogs
- Technical (Logical) Controls.
 - Access Controls , Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.

Control Types

1. Directive - Policy and standard that advise employees
2. Preventive – Controls that avoid incident
3. Detective – Controls that identify incident
4. Corrective – Controls that remedy incident
5. Recovery – Controls that restores baseline from incident

Example Implementations of Access Controls

	Directive	Preventive	Detective	Corrective	Recovery
Management (Administrative)	<ul style="list-style-type: none"> • Policy • Guidelines 	<ul style="list-style-type: none"> • User registration • User agreement • Separation of duties • Warning banner 	<ul style="list-style-type: none"> • Review access logs • Job rotation • Investigation • Security awareness training 	<ul style="list-style-type: none"> • Penalty • Controlled termination processes 	<ul style="list-style-type: none"> • Business continuity planning (BCP) • Disaster recovery planning (DRP)
Physical/ Operational	<ul style="list-style-type: none"> • Procedure 	<ul style="list-style-type: none"> • Physical barriers • Locks • Badge system • Security Guard • Mantrap doors • Effective hiring practice • Awareness training, 	<ul style="list-style-type: none"> • Monitor access • Motion detectors • CCTV 	<ul style="list-style-type: none"> • User behavioral modification • Modify and update physical barriers 	<ul style="list-style-type: none"> • Reconstruction

Reference:

- *CISSP All-in-One Exam Guide*, 4th Ed., S. Harris, McGraw-Hill
- *Official (ISC)² Guide To The CISSP CBK*, H. Tipton and K. Henry, (ISC)² Press, Auerbach Publications

Example Implementations of Access Controls

	Directive	Preventive	Detective	Corrective	Recovery
Technical	<ul style="list-style-type: none">Standards,	<ul style="list-style-type: none">User authenticationMulti-factor authenticationACLsFirewallsIPSEncryption	<ul style="list-style-type: none">Log access and transactionsStore access logsSNMPIDS	<ul style="list-style-type: none">Isolate, terminate connectionsModify and update access privileges	<ul style="list-style-type: none">BackupsRecover system functions,

Reference:

- *CISSP All-in-One Exam Guide*, 4th Ed., S. Harris, McGraw-Hill
- *Official (ISC)² Guide To The CISSP CBK*, H. Tipton and K. Henry, (ISC)² Press, Auerbach Publications

Access Control

- Definition & Principles



Threats

- Types of Access Control
 - Identification, Authentication, Authorization, and Accountability
- Access Control Models
 - Security Models
 - Centralized & Decentralized/Distributed
- Monitor & Management
 - IPS & IDS
 - Security Assessment & Evaluation

Example Threat List Related To Access Control

- Computing threats:
 - Denial of services (DoS) threats
 - Ping-of-death
 - Smurfing
 - SYN flood
 - Distributed DoS (DDoS)
 - Unauthorized software
 - Malicious code
 - Mobile code
 - Software defects
 - Buffer overflows
 - Covert channel
- Physical threats:
 - Unauthorized physical access
 - Dumpster diving
 - Shoulder surfing
 - Eavesdropping
 - Electronic emanations
- Personnel/Social engineering threats:
 - Disgruntle/ careless employees
 - Targeted data mining/ “browsing”
 - Spying
 - Impersonation

DoS Threats – Ping-of-Death

- Ping-of-Death
 - **Attack:** The originator sends an ICMP Echo Request (or ping) with very large packet length (e.g. 65,535 bytes) to the target machine. The physical and data-link layers will typically break the packet into small frames. The target machine will attempt to re-assemble the data frames in order to return an ICMP Echo Reply. The process of reassemble large packet may cause buffer overflow of the target machine.
 - **Countermeasure:**
 - Apply patches for buffer overflow
 - Configure host-based firewall to block ICMP Echo Request (ping)

DoS Threats – Smurf Attack

- Smurfing (ICMP storm or ping flooding).
 - **Attack:** The attacker sends a large stream of ping packets with spoofed source IP address to a broadcast address. The intermediaries receives the ping and returns the ICMP Echo Reply back using the spoofed IP address (which is the address of the target machine).
 - **Countermeasure:**
 - Disable IP-directed broadcasts on routers (using ACL)
 - Configure host-based firewall or server OS to block ICMP Echo Request (ping)

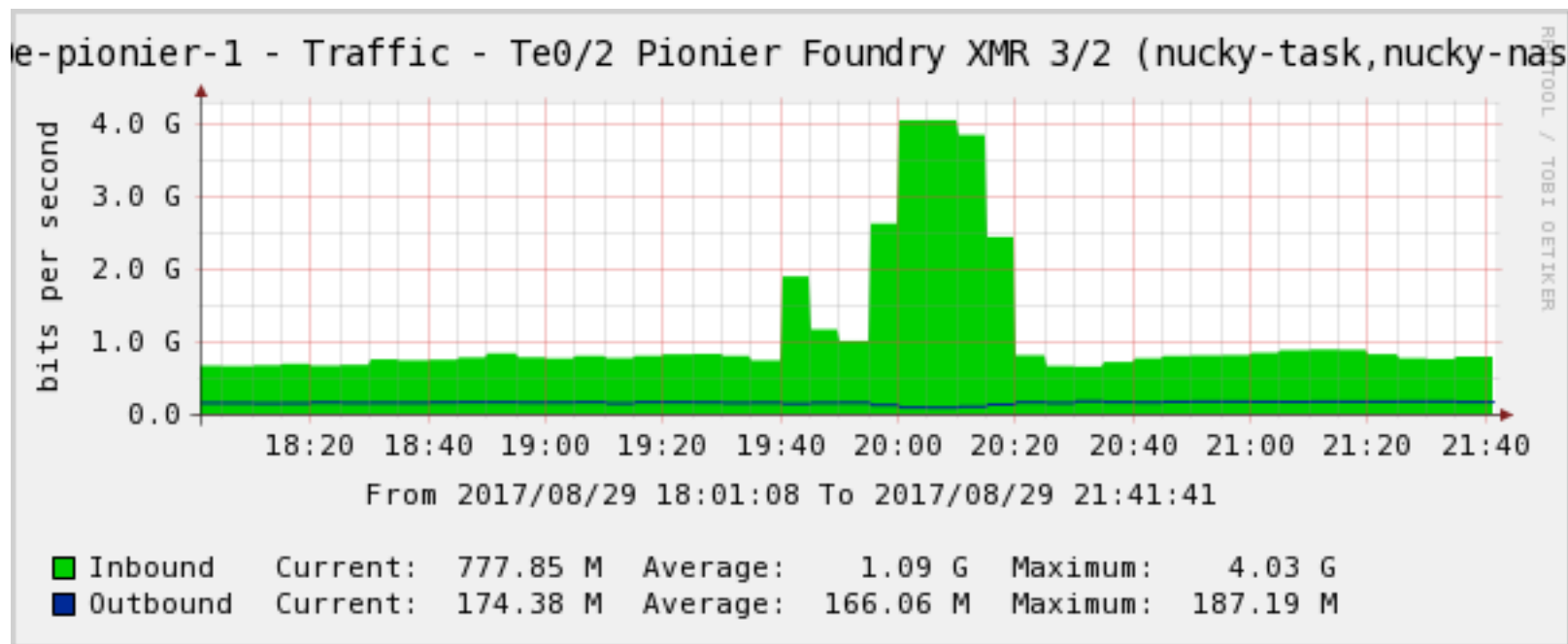
DoS Threats – SYN Flooding

- SYN Flooding
 - **Attack:** Client system sending a SYN (synchronization) message with spoofed source address to server. Server respond by returning a SYN/ACK message. However, since the return source address is spoofed so the server will never get to complete the TCP session. Since TCP is a stateful protocol, so the server stores this “half-open” session. If the server receives false packets faster than the legitimate packets then DoS may occur, or server may exhaust memory or crash for buffer overflow.
 - **Countermeasure:**
 - For attacks originated from outside: Apply “Bogon” and private IP inbound ACL (reserved private address) to edge (perimeter) router’s external interface.
 - For attacks originated from inside: Permit packets originated from known interior IP address to outbound ACL on edge router’s internal interface.

DoS Threats – Distributed DoS

- Distributed Denial-of-Service (DDoS) requires the attacker to have many compromised hosts, which overload a targeted server with network packets.
 - **Attack:** The attacker installs malicious software into target machine. The infected target machine then becomes the “bots” (/“zombies”) that infects more machines. The infected machines begins to perform distributed attacks at a pre-program time (time bomb) or the a initiation command issued through covert channel. “Bots” (/“zombies”) can initiate legitimate TCP session or launch SYN flooding, Smurfing, or Ping-of-death attacks to prevent the target machine(s) from providing legitimate services.
 - **Countermeasure:**
 - Harden servers or install H-IDS to prevent them become “bots” (/ “zombies”).
 - Setup N-IPS at the edge (perimeter) network.
 - Active monitoring of H-IDS, N-IDS, N-IPS, and Syslogs for anomalies.

DDoS - example



Example Threat List Related To Access Control

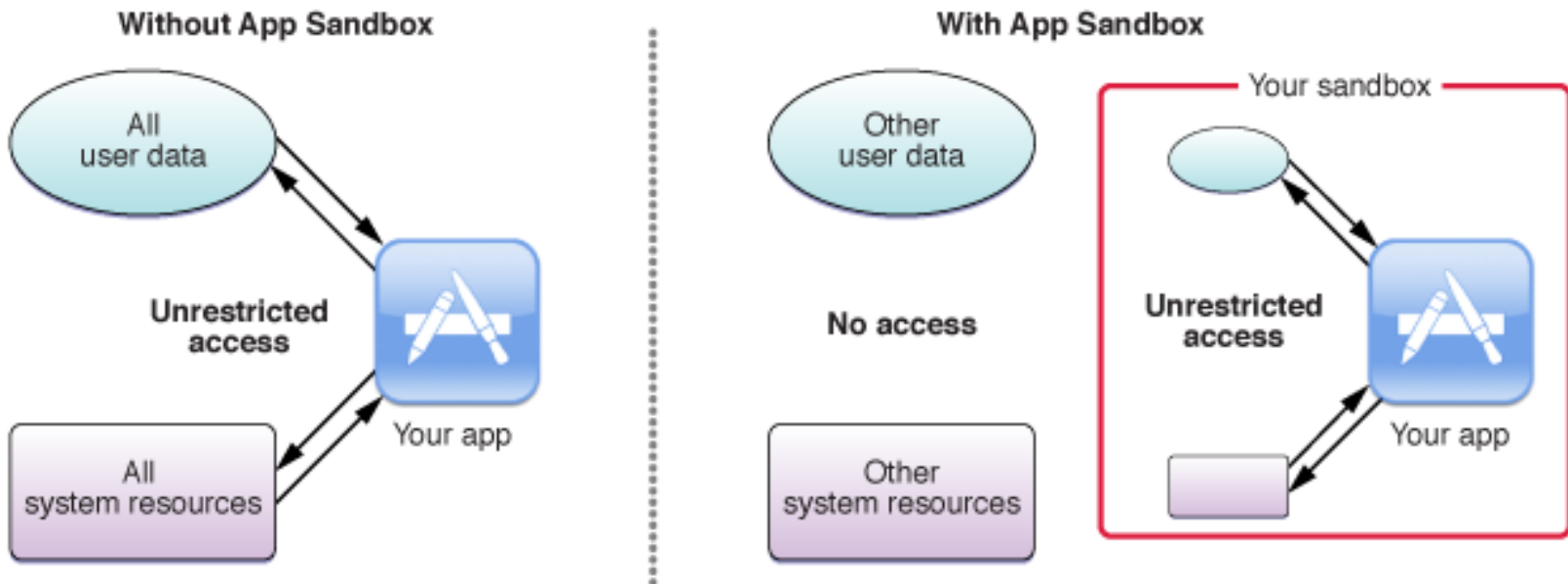
- Computing threats:
 - Denial of services (DoS) threats
 - Ping-of-death
 - Smurfing
 - SYN flood
 - Distributed DoS (DDoS)
 - Unauthorized software
 - Malicious code
 - Mobile code
 - Software defects
 - Buffer overflows
 - Covert channel
- Physical threats:
 - Unauthorized physical access
 - Dumpster diving
 - Shoulder surfing
 - Eavesdropping
 - Electronic emanations
- Personnel/Social engineering threats:
 - Disgruntle/ careless employees
 - Targeted data mining/ “browsing”
 - Spying
 - Impersonation

Unauthorized Software – Malicious Code Threats

- Viruses – programs attaches itself to executable code and is executed when the software program begins to run or an infected file is opened.
- Worms – programs that reproduce by copying themselves through computers on a network.
- Trojan horse – code fragment that hides inside a program and performs a disguised functions.
- Logic bomb – a type of Trojan horse that release some type of malicious code when a particular event occurs.

Unauthorized Software – Malicious Mobile Code Threats

- Instant Messaging Attacks
- Internet Browser Attacks
- Malicious Java Applets
- Malicious Active X Controls
- Email Attacks



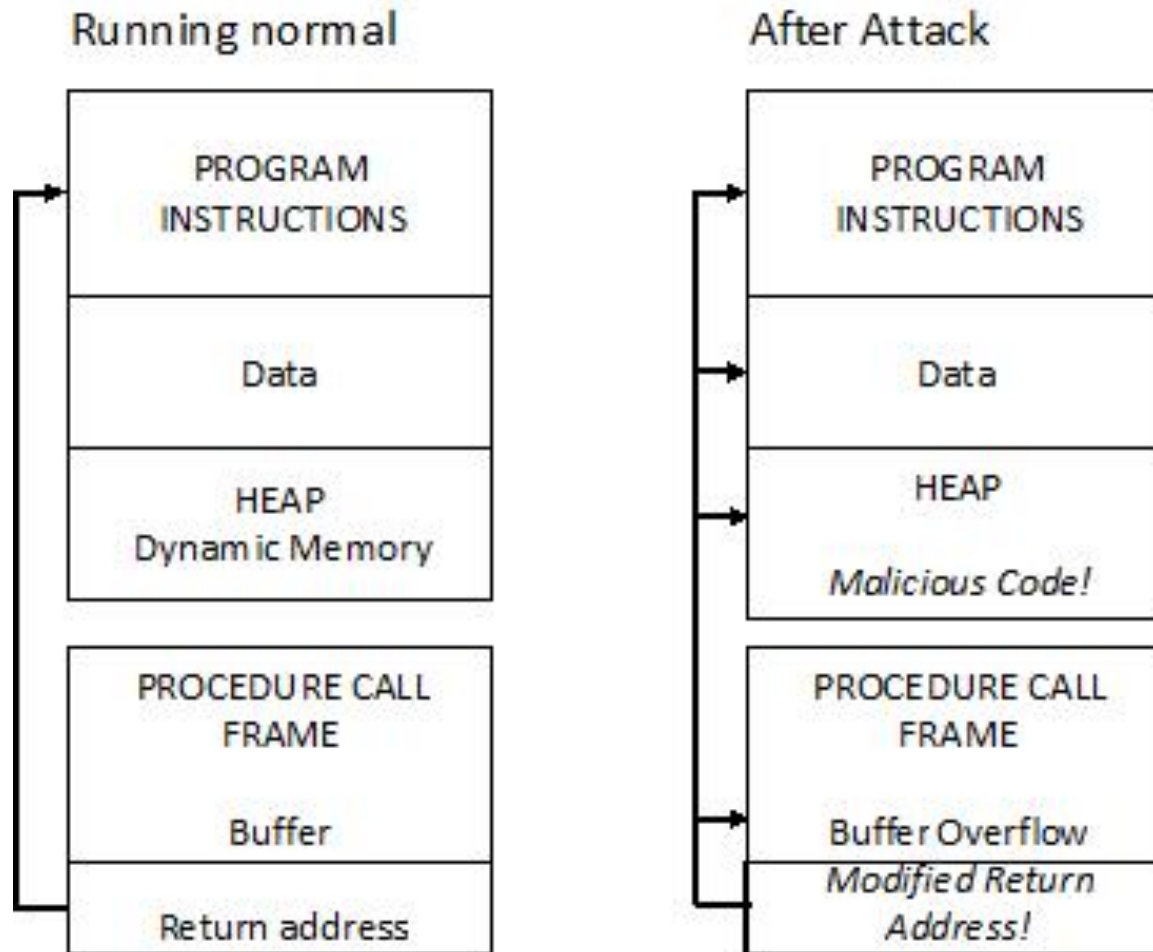
Example Threat List Related To Access Control

- Computing threats:
 - Denial of services (DoS) threats
 - Ping-of-death
 - Smurfing
 - SYN flood
 - Distributed DoS (DDoS)
 - Unauthorized software
 - Malicious code
 - Mobile code
 - **Software defects**
 - Buffer overflows
 - Covert channel
- Physical threats:
 - Unauthorized physical access
 - Dumpster diving
 - Shoulder surfing
 - Eavesdropping
 - Electronic emanations
- Personnel/Social engineering threats:
 - Disgruntle/ careless employees
 - Targeted data mining/ “browsing”
 - Spying
 - Impersonation

Software Defects: Buffer Overflow Threats

- One of the oldest and most common problems to software.
- A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.
- Vulnerability is caused by lack of parameter checking or enforcement for accuracy and consistency by the software application or OS.
- Countermeasure:
 - Practice good SDLC process (code inspection & walkthrough).
 - Apply patches for OS & applications.
 - If available, implement hardware states and controls for memory protection. Buffer management for OS.

Software Defects: Buffer Overflow Threats



Attacker plants code that overflows buffer and corrupts the return address. Instead of returning to the appropriate calling procedure, the modified return address returns control to malicious code, located elsewhere in process memory.

Software Defects – Covert Channel Threats

- Covert channel is an un-controlled information flow (or unauthorized information transfer) through hidden communication path(s).
 - Timing channel (the attacker can observe how long an example process takes or what are the delays between different actions (ex. http requests, ssh requests) and based on this can resolve the information (0 v 1))
 - Storage channel (ICMP error may contain extra information about the identity of the target operating system)
- Countermeasure steps:
 - Identify potential covert channel(s)
 - Close the covert channel by install patch or packet-filtering security mechanism.

Reference: NCSC-TG-30, *A Guide To Understanding Covert Channel Analysis of Trusted System*

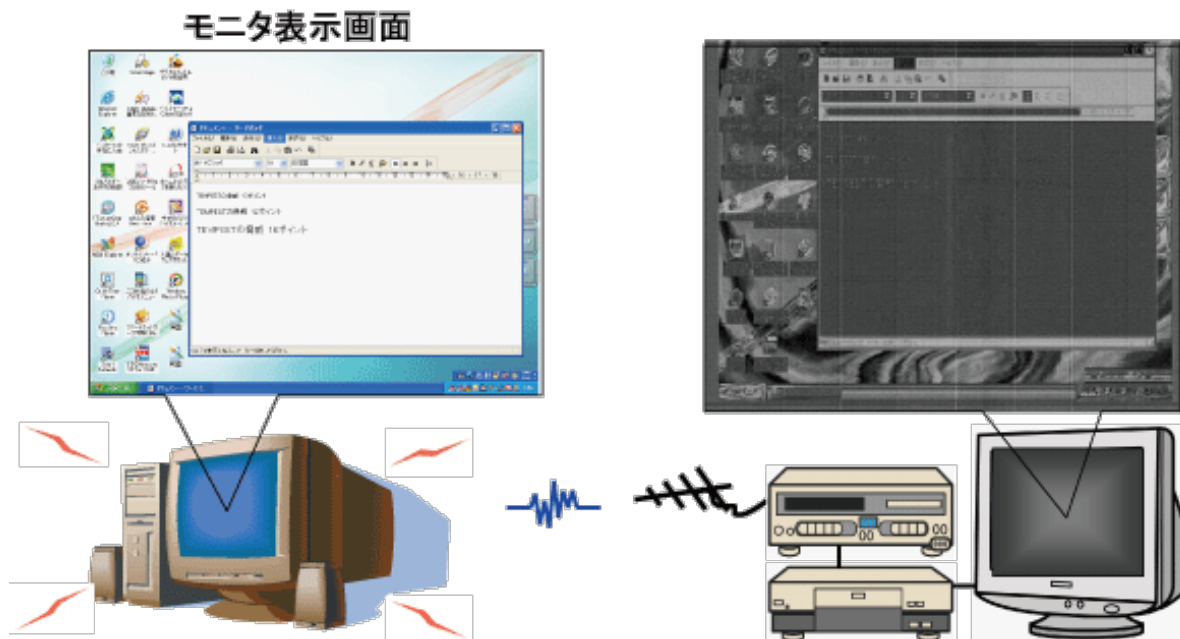
Example Threat List Related To Access Control

- Computing threats:
 - Denial of services (DoS) threats
 - Ping-of-death
 - Smurfing
 - SYN flood
 - Distributed DoS (DDoS)
 - Unauthorized software
 - Malicious code
 - Mobile code
 - Software defects
 - Buffer overflows
 - Covert channel
- Physical threats:
 - Unauthorized physical access
 - Dumpster diving
 - Shoulder surfing
 - Eavesdropping
 - Electronic emanations
- Personnel/Social engineering threats:
 - Disgruntle/ careless employees
 - Targeted data mining/ “browsing”
 - Spying
 - Impersonation

Physical threats:

- Physical threats:
 - Unauthorized physical access
 - Dumpster diving
 - Shoulder surfing
 - Eavesdropping
 - Electronic emanations (NSA TEMPEST Attack can remotely view your computer and cell phone screen using radio waves)

!



Personnel/Social engineering threats:

- Personnel/Social engineering threats:
 - Disgruntle/ careless employees
 - Targeted data mining/ “browsing”
 - Spying
 - Impersonation

Access Control

- Definition & Principles

- Threats



Types of Access Control

- Identification, Authentication, Authorization, and Accountability

- Access Control Models

- Security Models
- Centralized & Decentralized/Distributed

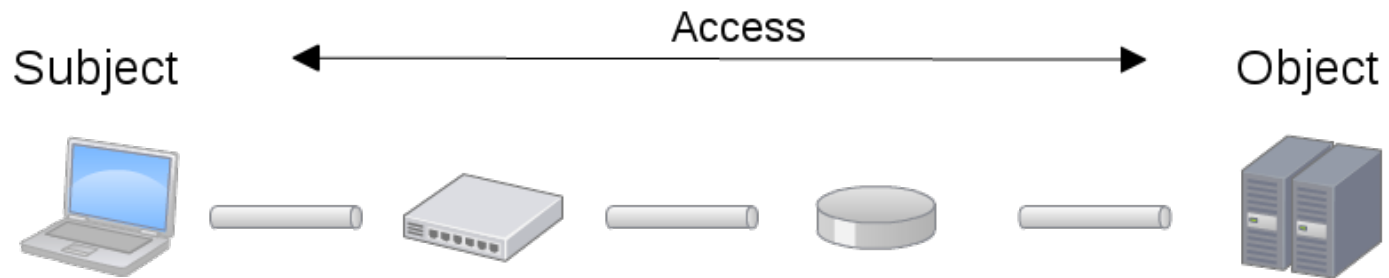
- Monitor & Management

- IPS & IDS
- Security Assessment & Evaluation

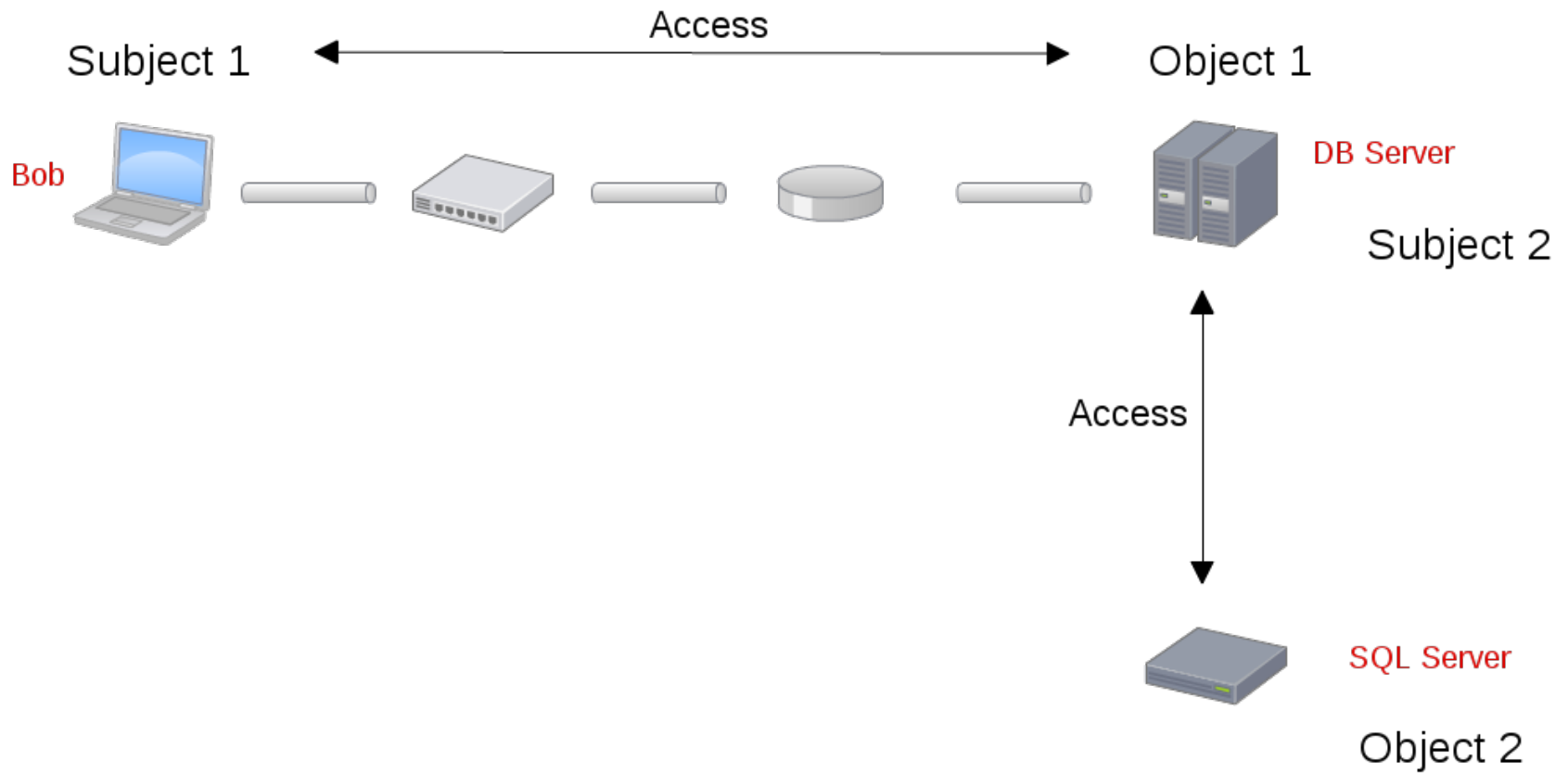
Subject vs. Object (TCB – Orange Book)

- Subject – requests service.
 - User, program, process, or device, etc.
 - Can be labeled to have an access sensitivity level (e.g. Unclassified, Secret, Top Secret).
- Object – provide the requested service.
 - File, database, program, process, device, etc.
 - Can be labeled to have an access sensitivity level (e.g. Unclassified, Secret, Top Secret).

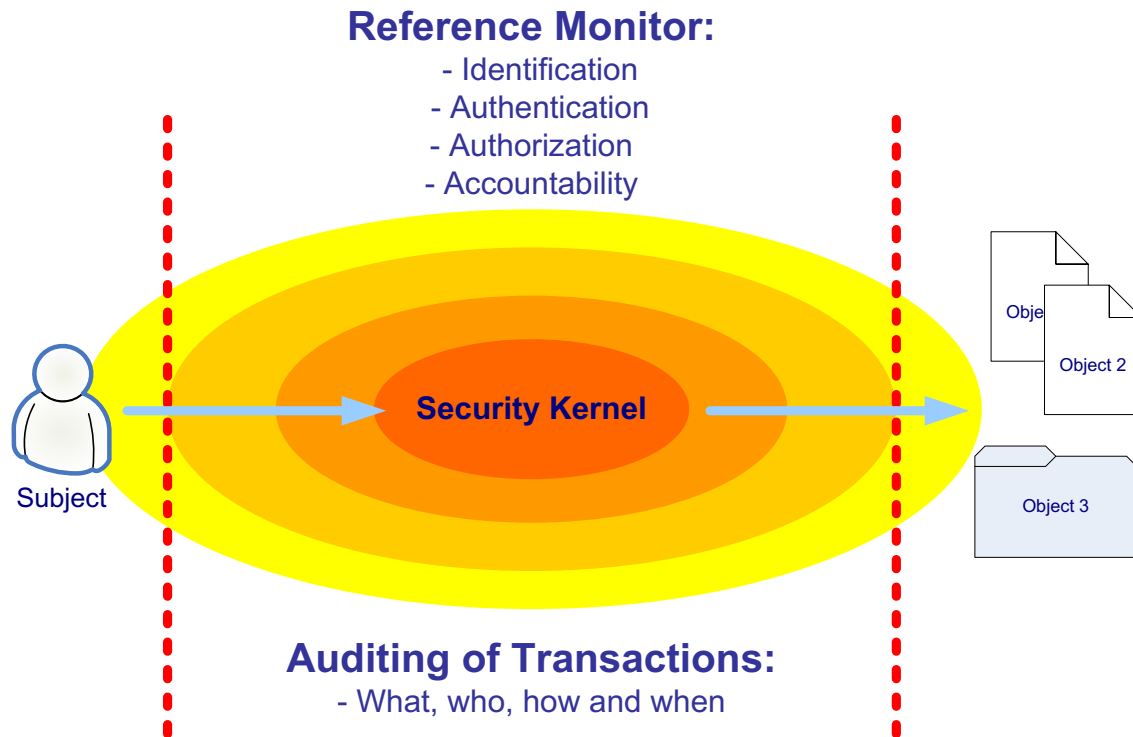
Access Control



Access Control



Authentication, Authorization & Accountability (AAA)



identification, authentication, authorization, auditing, accountability

- **Identification** - is the process by which a subject professes an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, authorization, and accountability (AAA).
- **Authentication** – is the process of verifying or testing that the claimed identity is valid is authentication. Authentication requires from the subject additional information that must exactly correspond to the identity indicated.

Authorization , Auditing , Accountability

- **Authorization** - once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity.
- **Auditing** - Auditing, or monitoring, is the programmatic means by which a subject's actions are tracked and recorded for the purpose of holding the subject accountable for their actions while authenticated/unauthorized/abnormal activities on a system.
- **Accountability** - relies on the capability to prove a subject's identity and track their activities.

Bob reading the file

- Bob wants to have access to the file
- We need to know who Bob is?
- Component 1: He has to provide his identity and has to prove that this is true (Authentication)
- Component 2: We need to control the traffic to the server
- Component 3: We should have the access to the file (eg. Read, Write, Execute, Full access - permissions) (Authorization)
- Component 4: Track the user actions in the network or server (Accountability)



Identification & Authentication

- Types of identity:
 - User ID, Account Number, User Name, etc.
 - Unique, standard naming convention, non-descriptive of job function, secure & documented issuance process.
- Types of authentication:
 - Something the subject knows – Password, pass phrase, or PIN.
 - Something the subject has – Token, smart card, keys.
 - Something the subject is – Biometrics: fingerprints, voice, facial, or retina patterns, etc.

Something the Subject KNOWS

- Password is a protected word (or string of characters) that authenticates the subject to the system.
- Passphrase is a sequence of characters or words. Passphrase can also be used to generate encryption keys.
- PIN is Personal Identification Number.

Something the Subject **KNOWS**

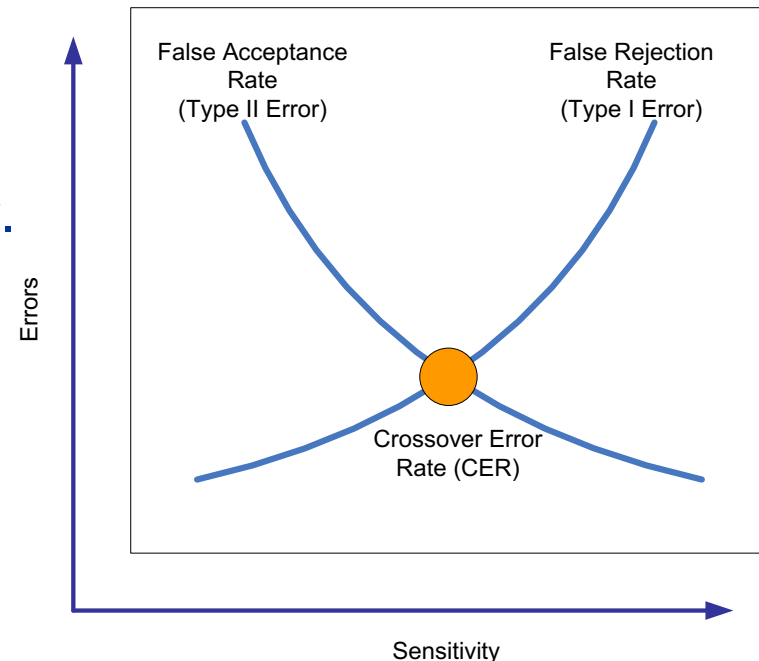
- Password Management
 - Control Access
 - Restrict access to password files
 - Encrypt password files (MD5, SHA)
 - Password Structure
 - Password length
 - Password complexity: a mix of upper/lowercase letters, numbers, special characters
 - Not using common words found in dictionary (use Rainbow Table)
 - Password Maintenance
 - Password aging, e.g., change in <90> days
 - Password can not be reused within <10> password changes
 - <One> change to <every 24 hr.>

Something the Subject HAS


- One-Time Password (OTP)
 - Something generated from a RNG device that generates an OTP
- Synchronous Token (with time)
 - Counter-based token – action increase the number
 - Clock-based token – automatically number increasing (e.g. RSA token)
- Asynchronous Token (without time)
 - Challenge-response devices (e.g. password)
 - Smart card. With memory or processor chips that accepts, stores, and transmit certificates or keys that generate tokens. (e.g. FIPS 201 PIV)

Something the Subject IS

- Biometrics: Fingerprints, Hand geometry, Facial geometry, Retina patterns, Voice patterns, etc.
- Challenges:
 - Crossover error rate (CER) (false acceptance vs. false rejection)
 - Processing speed: Biometrics are complex, one-to-many, many-to-many.
 - User acceptance: Privacy is a big issue.



Access Control

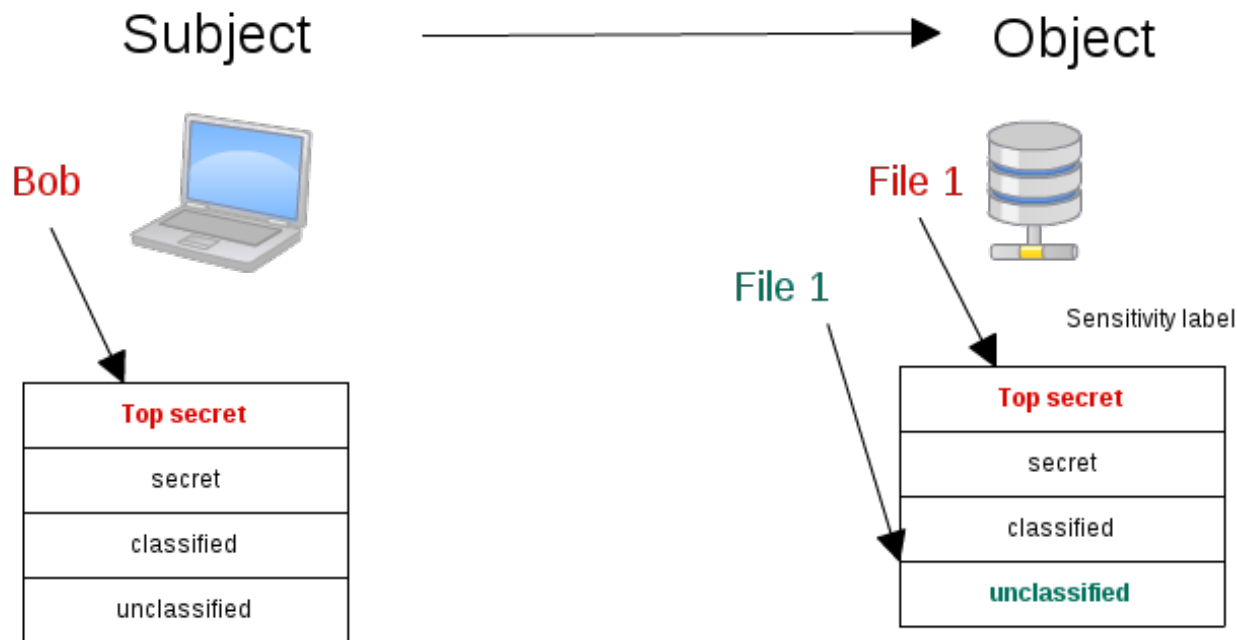
- Definition & Principles
- Threats
- Types of Access Control
 - Identity & Authentication
-  Access Control Models
 - Security Models
 - Centralized & Decentralized/Distributed
- Monitor & Management
 - IPS & IDS
 - Security Assessment & Evaluation

Security Models

- Security objectives for access control: confidentiality and integrity.
- Implementation principles: least-privilege, separation-of-duties.
- Access control governs the information flow.
 - Discretionary access control (DAC) is where the information owner determines the access capabilities of a subject to what object(s).
 - Mandatory access control (MAC) is where a subject's access capabilities have been pre-determined by the security classification of a subject and the sensitivity of an object(s).
- Security models that specifies access control of information operations:
 - HRU Access Capability Matrix, Bell-LaPadula (BLP), Biba
 - Rule-set based Access Model:
 - Role-based Access Control (RBAC)

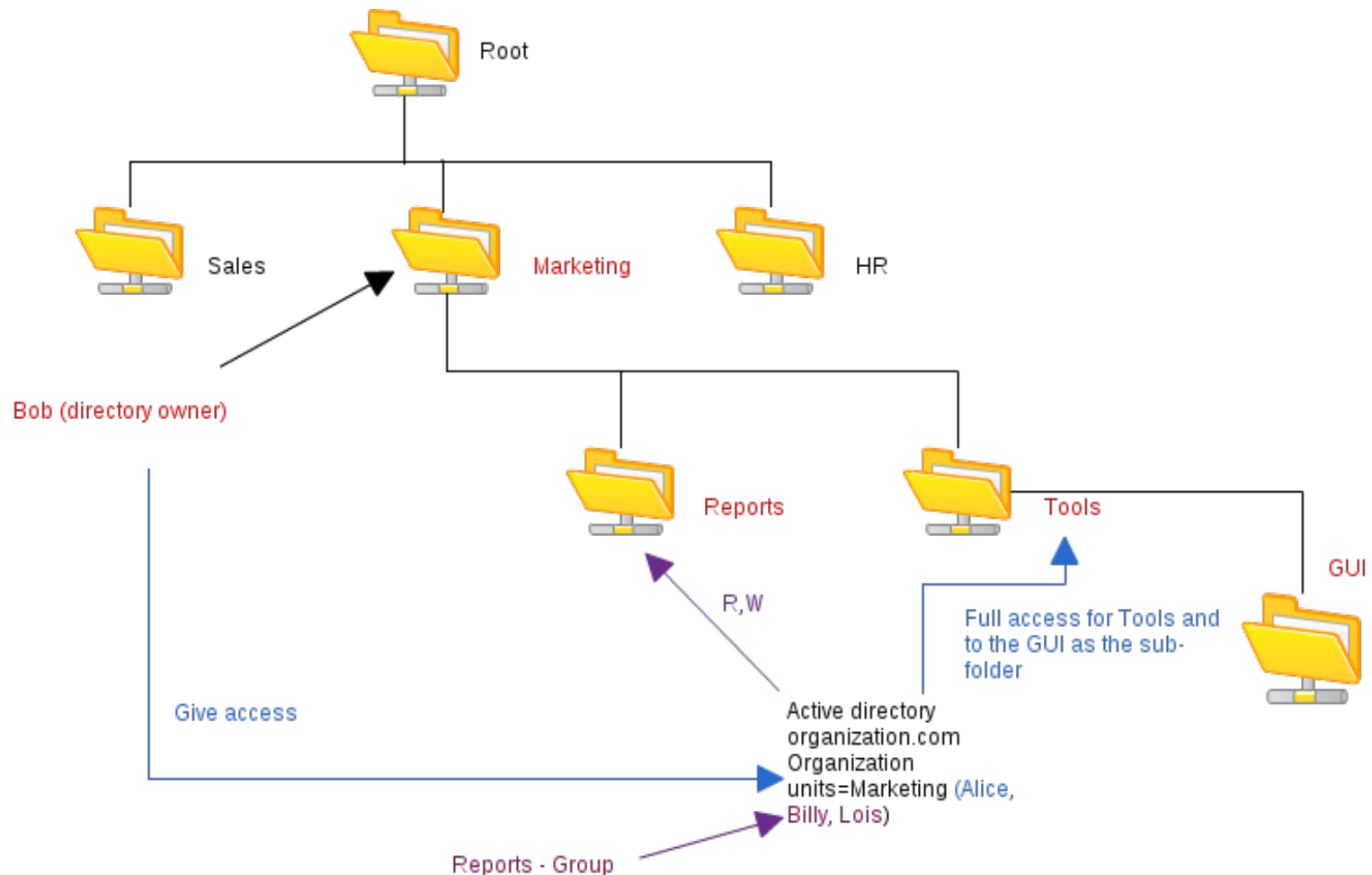
MAC

- Four access levels: Top Secret (TS), Secret (S), Classified (C), Unclassified (U)
- Subject can read any object which is on the same level or below



DAC (Discretionary access control)

- Owner of the data (Director is an owner)
- Identity Based Access Control



Access Control Matrix

- Access control matrix specifies access relations between subject-subject or subject-object.
 - One row per subject.
 - One column per subjects or object.

		Object / Subject						
		A	B	C	D	E	F	G
Subject	1	•				•		
	2		•				•	
	3							
	4							•
	5		•		•			
	6						•	
	7					•		

Access Permission

- List of typical access permission:
 - UNIX has 8 access permission settings for 3 types of users (o,g,w)
 - Combination of Read (r), Write (w), Execute (x)
 - --- All types of access denied
 - --x Execute access is allowed only
 - -w- Write access is allowed only
 - -wx Write and execute access are allowed
 - r-- Read access is allowed only
 - r-x Read and execute access are allowed
 - rw- Read and write access are allowed
 - rwx Everything is allowed

Capability Tables – Harison-Ruzzo-Ullman (HRU)

- Capability table = Access control matrix + Access permissions
- Row = Capability list (Subject's access permission)
- Column = Control list (Objects)

		Object						
		Program A	Program B	Program C	Database D	Database E	File F	File G
Subject	Joe User 1	r-x	---	---	r-x	---	rwX	rwX
	User Role 2	---	---	---	---	---	-wX	-wX
	Process 3	r-x	---	--X	---	rwX	---	---
	Process 4		---	--X	rwX	rwX	---	---
	Program A	rwX	--X	---	rwX	---	---	---

Access Control List (ACL)

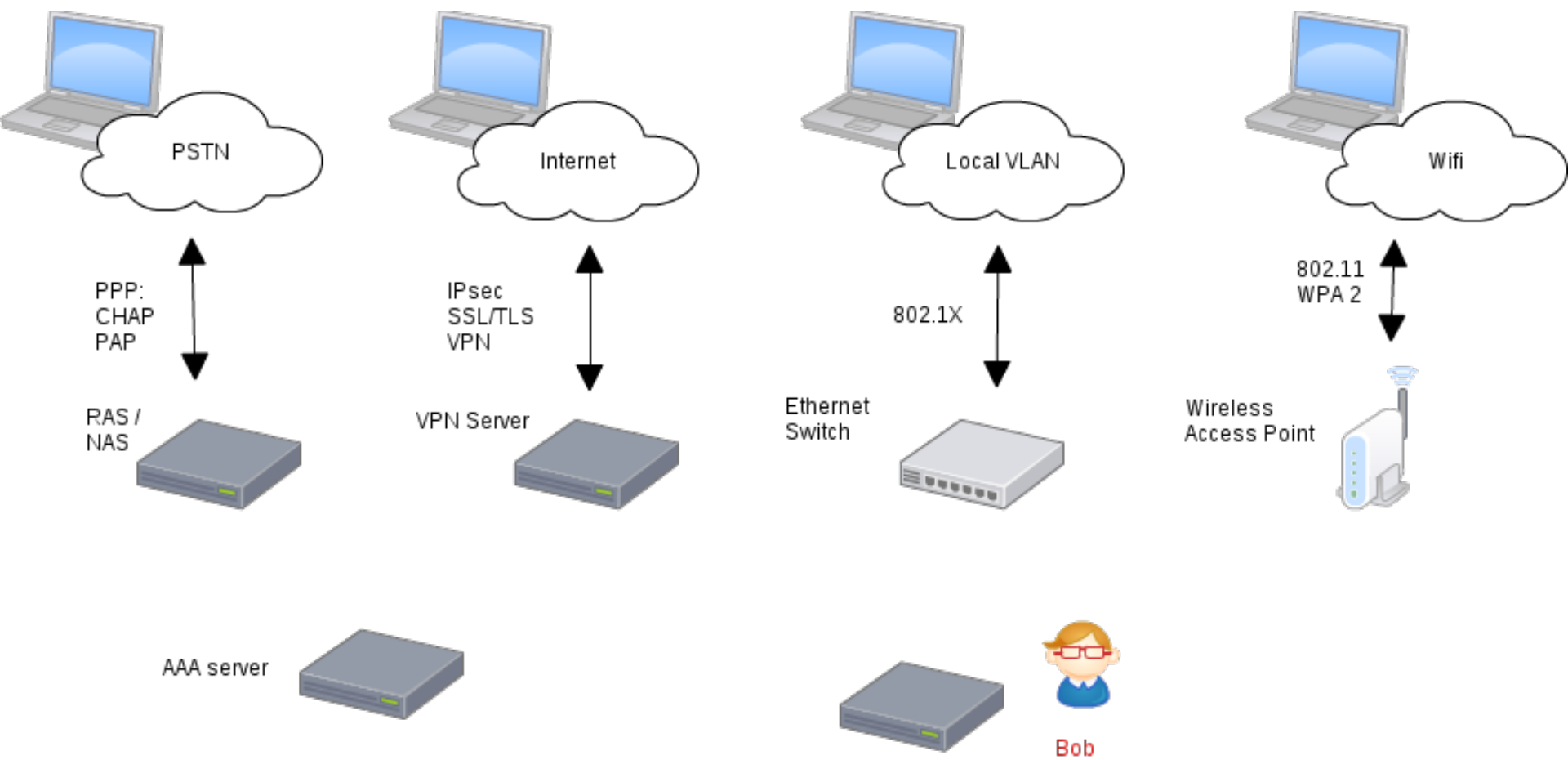
- Access control list (ACL) is most common implementation of DAC.
- Implemented using access control matrices with access permissions, i.e. **capability table**.
 - Define subject's access to and access permissions to object(s).

		Object						
		Program A	Program B	Program C	Database D	Database E	File F	File G
Subject	Joe User 1	r-X	r-X	--X	--X	---	r--	rwX
	Jane User 2	---	r-X	--X	---	---	r--	r--
	John User 3	r-X	---	--X	---	--X	r--	r--

Role-based Access Control (RBAC)

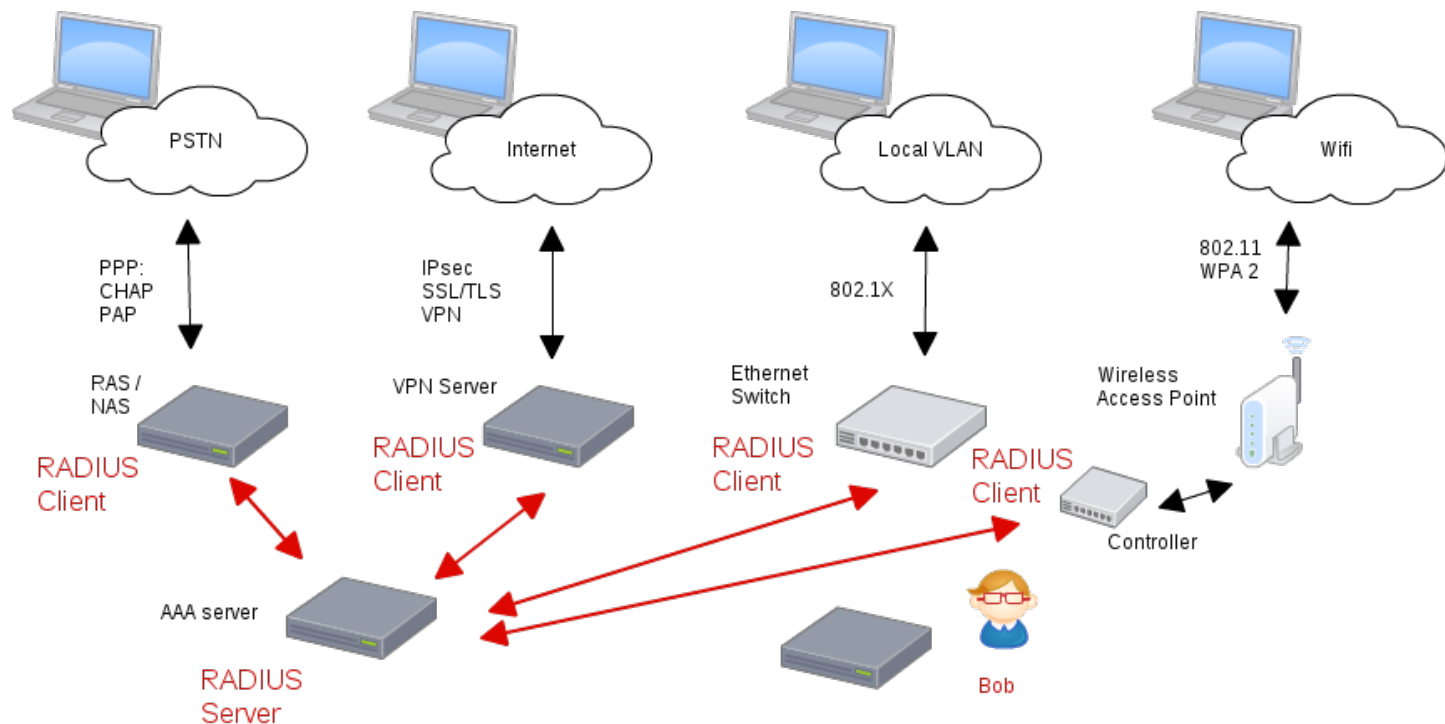
- Access control decisions are based on job function.
- Each role (job function) will have its own access capabilities.
- Access capabilities are inherited by users assigned a job function.
- Determination of role is discretionary and is in compliance with security access control policy.
- Groups of users need similar or identical privileges.
 - Generally associated with DAC.
 - Privileges appropriate to functional roles are assigned
 - Individual users are enrolled in appropriate roles.
 - Privileges are inherited.

Case



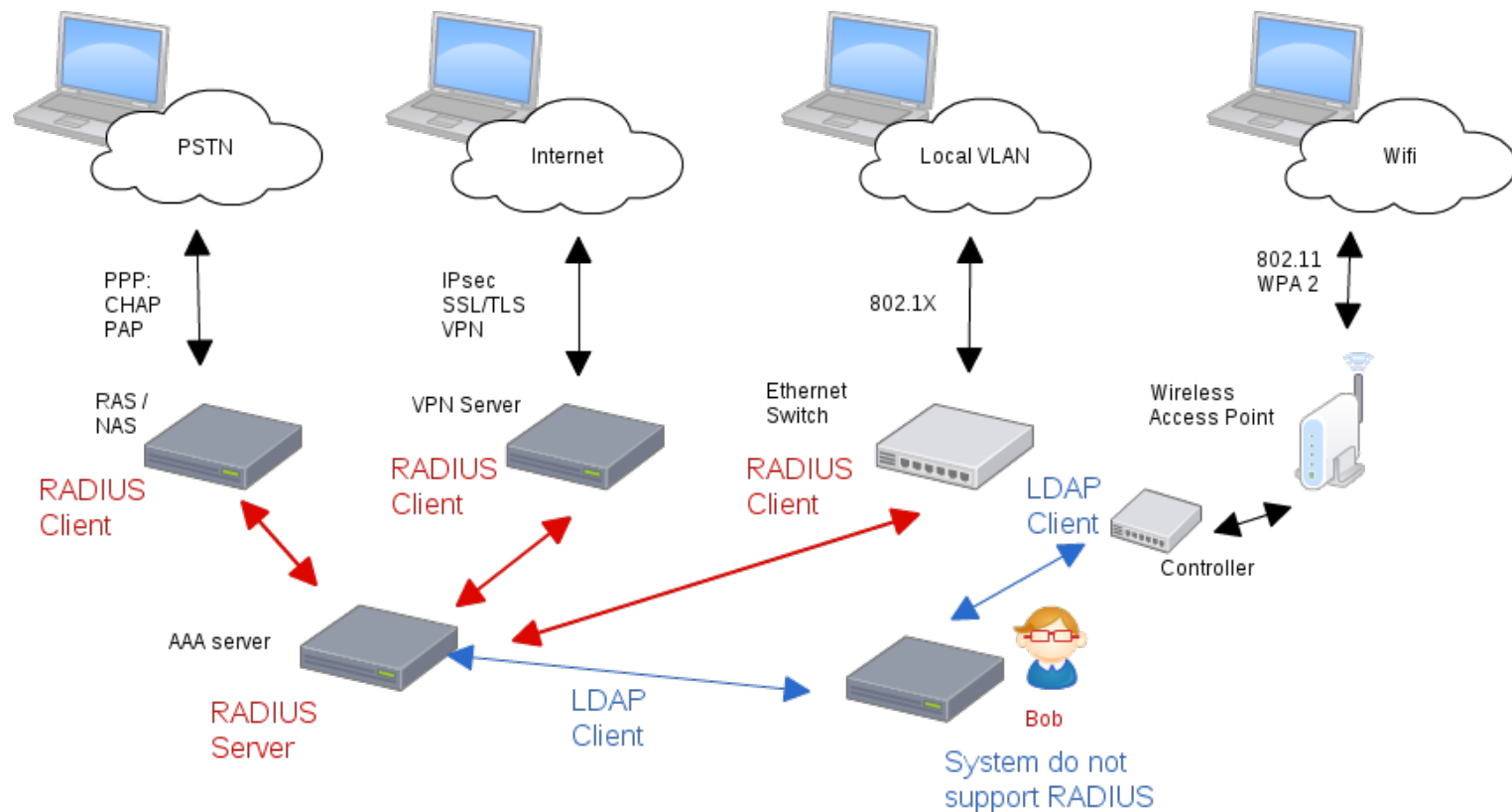
Where the Bob's credential will be stored?

- We can store it locally in any servers separately
- Centralized Access Management
- RADIUS – is defined in RFC 2138 and is an open standard



LDAP

- LDAP: **L**ightweight **D**irectory **A**ccess **P**rotocol
- Entity: Computer, Users, OS
- Microsoft Active Directory supports LDAP



Centralized Access Control Method

AAA (Authentication, Authorization, Accounting) protocols.

- RADIUS (Remote Access Dial-In User Service)
 - Use UDP/IP-based frame protocols: SLIP (Serial Line Internet Protocol) and PPP (Point-to-Point Protocol).
 - In a client/server configuration.
- TACACS (Terminal Access Controller Access Control System)
 - Proprietary (Cisco Systems), TACACS+ a proposed IETF standard.
 - TCP/IP-based, Transaction includes CHAP or PAP.
- Diameter (not an acronym)
 - RFC 3588 for access control of mobile devices.
 - Uses UDP transport in a peer-to-peer configuration.

Decentralized Access Control Method

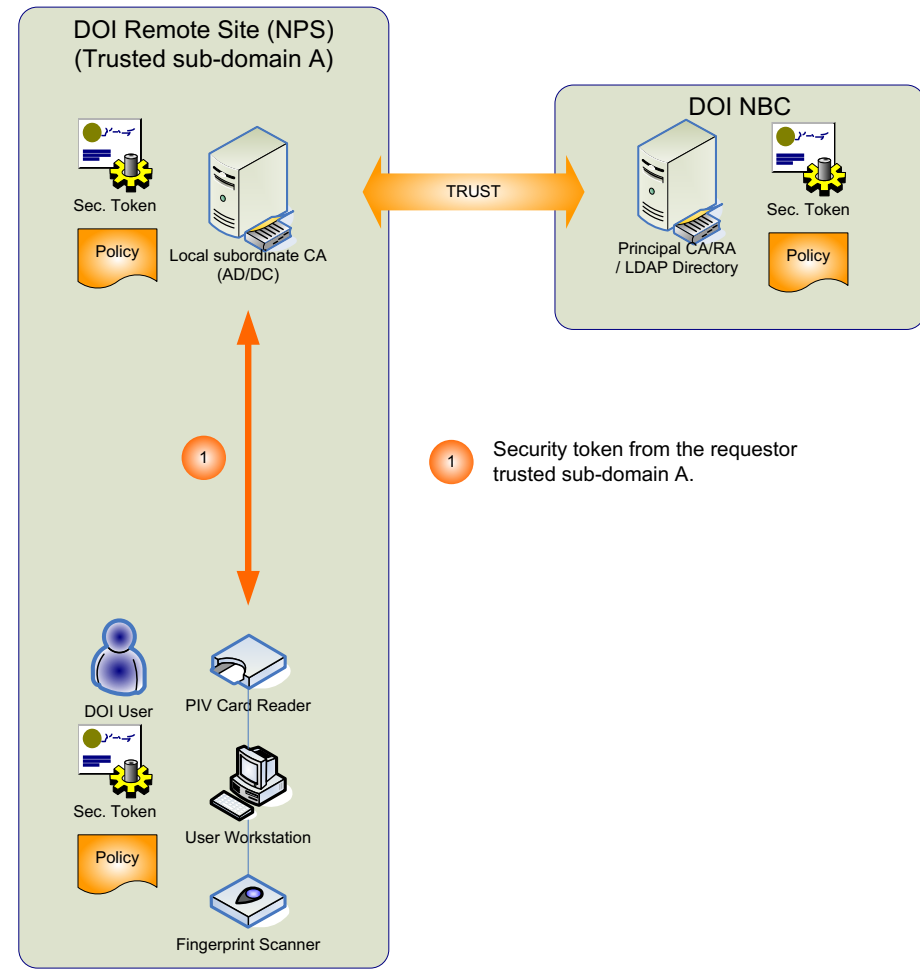
Single Sign-On (SSO):

Key enabler of SSO is

“chain of certificates
and tokens.”

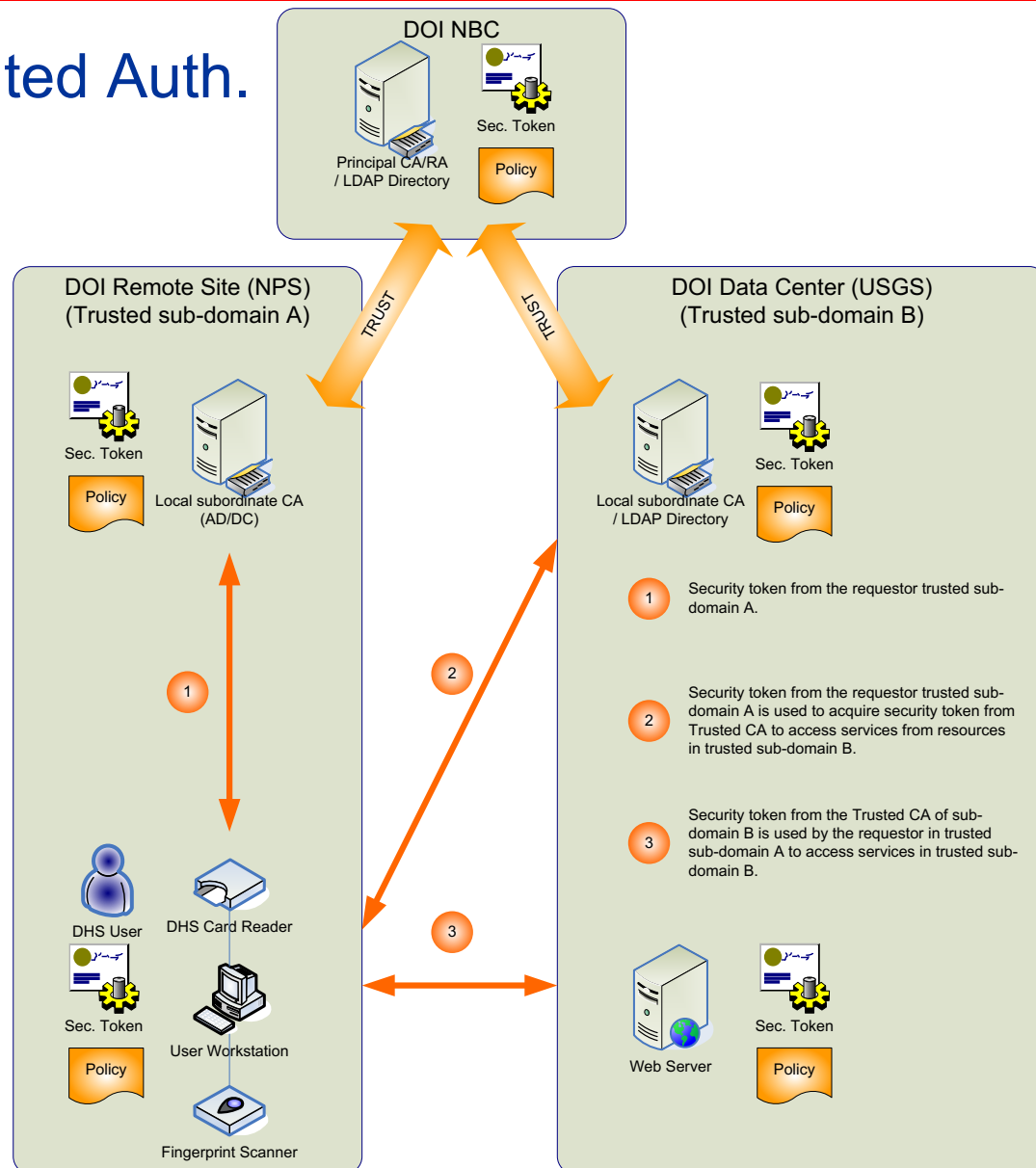
Step 1: Sign-On

- Subject (user) authenticates against a master certification authority (CA) system using single-, two-, or three-factor authentication method.
- A security token is then issued to the authenticated subject along with access policy.



Decentralized Access Control Method

Step 2: Distributed Auth.



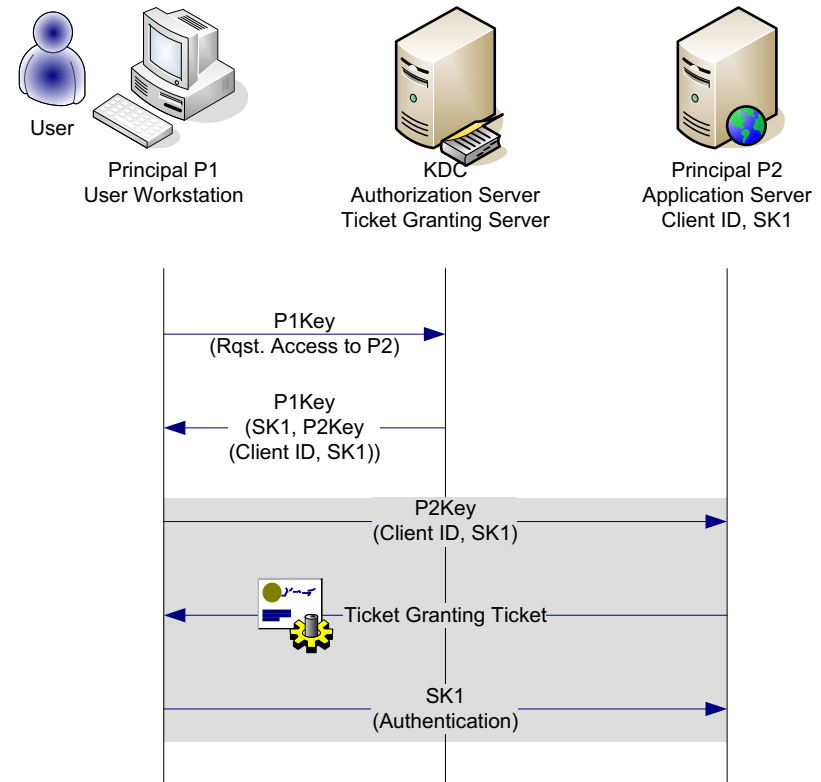
Decentralized Access Control Method

Kerberos is also based on a central authentication authority-Key distribution center (KDC). KDC performs authentication service (AS), and ticket granting service (TGS) functions.

- Kerberos provides:
 - Encryption of data for confidentiality, non-repudiation for integrity.
 - Transparency. The authentication & key distribution process is transparent to subjects
- In many ways, PKI is similar to Kerberos, except Kerberos uses DES cryptographic algorithm for encrypting authentication information and PKI supports various type of crypto. cipher.

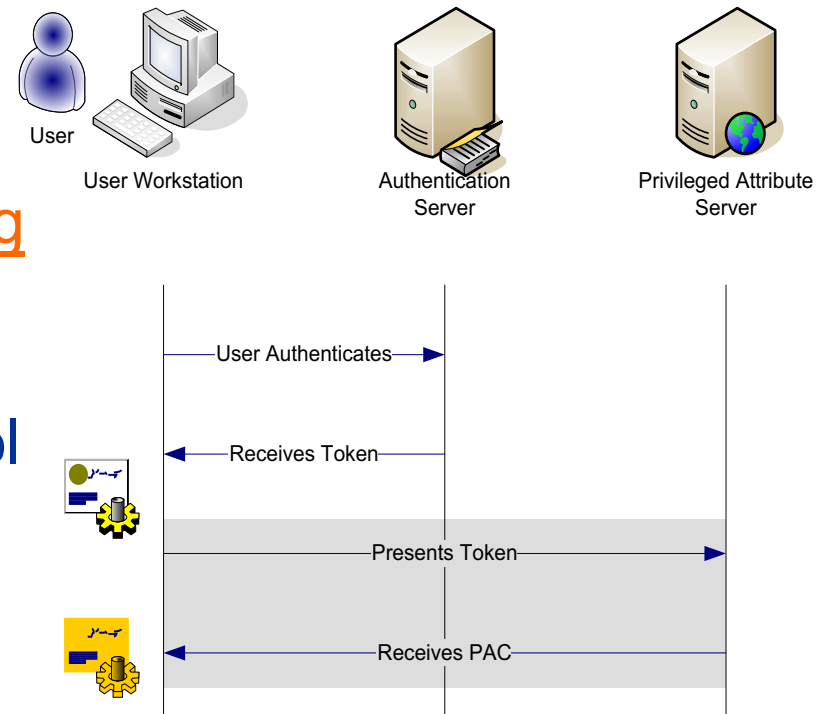
Decentralized Access Control Method

- The Kerberos Key Distribution Center (**KDC**) server serves two functions:
- An Authentication Server (**AS**), which authenticates a Principal via a pre-exchanged Secret Key
- A Ticket Granting Server (**TGS**), which provides a means to securely authenticate a trusted relationship between two Principals.



Decentralized Access Control Method

- Secure European System for Applications in a Multi-vendor Environment (SESAME)
- Offers SSO with added distributed access controls using public-key cryptography for protect internetworking data.
 - Offers role-based access control (RBAC).
 - Use Privileged Attribute Certificate (PAC) (similar to Kerberos Ticket).
 - SESAME components can be accessible through Kerberos v5 protocol.



Access Control

- Definition & Principles
- Threats
- Types of Access Control
 - Identification, Authentication, Authorization, and Accountability
- Access Control Models
 - Security Models
 - Centralized & Decentralized/Distributed
- ➔ Monitor & Management
 - IPS & IDS

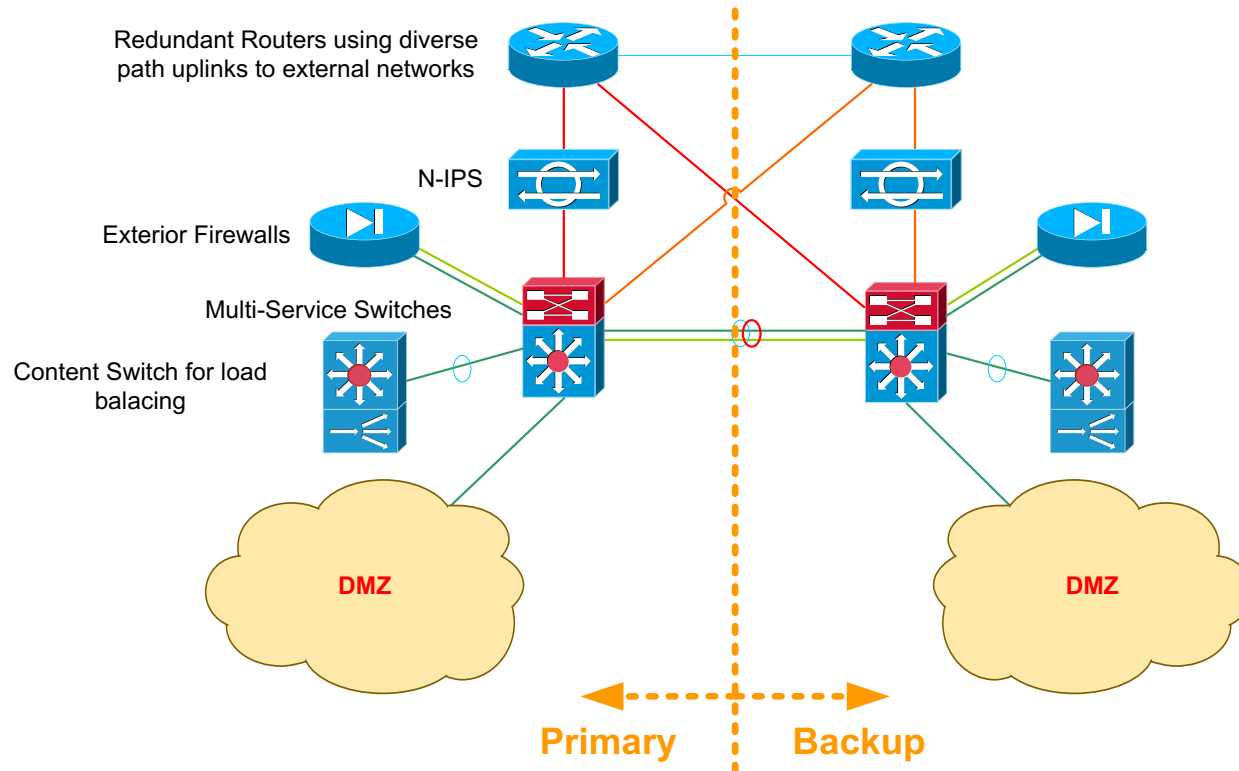
Intrusion Prevention & Detection

- Intrusion Prevention System (IPS)
 - In-line preventive control device (transparent packet forwarding, full control of the packets).
 - Actively intercept and forward packets.
 - Access control and policy enforcement.
 - Usually a network-based device.
- Intrusion Detection Systems (IDS)
 - Passive monitoring devices (examines copies of packages).
 - Network-based (N-IDS) and Host-based (H-IDS).
 - Passively monitor and audit transmitted packets.
 - Pattern/Signature matching or Anomaly-based.
- IDS Analysis Methods & Engine
 - Pattern / Stateful Matching Engine.
 - Anomaly-based Engine.

Network-based IPS (N-IPS)

N-IPS is an in-line security device for preventive controls.

- Ability to block attacks in real time.
- Actively intercept and forward packets.



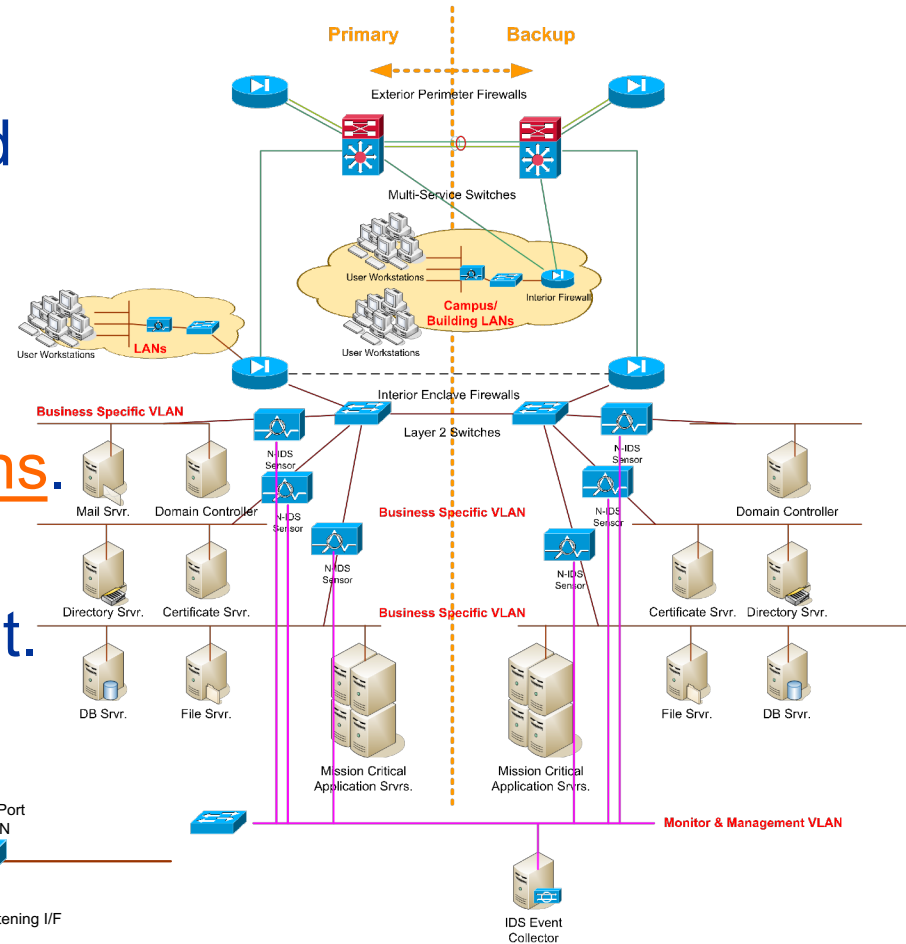
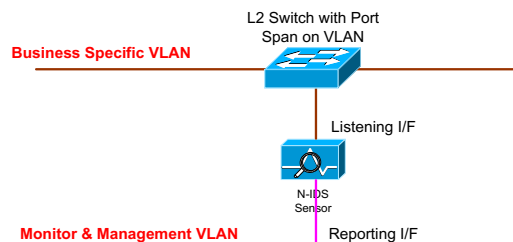
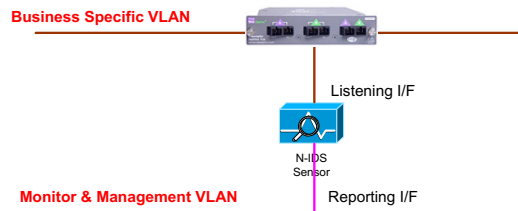
CISCO icons



Network-based IDS (N-IDS)

N-IDS is a passive monitoring device for detective controls.

- Monitors network packets and traffic on transmission links in real time.
- Analyzes protocols & traffic based on signatures & patterns.
- Two interfaces: Monitor (promiscuous) & management.



Host-based IDS (H-IDS)

- H-IDS Program (Agent) on host to detect intrusions
- Analyze event logs, critical system files & other specified log files.
- Compare file signatures (MD-5 or SHA-1) to detect unauthorized changes.
- Monitoring or alert message should be configured to send through dedicated management network interface.

IDS Analysis Methods & Engine – Pattern/Stateful Matching

- Pattern Matching Method
 - Scans incoming packets for specific byte sequences (signatures) stored in a database of known attacks.
 - Identifies known attacks.
 - Require periodic updates to signatures.
- Stateful Matching Method
 - Scan traffic stream rather than individual packets.
 - Identifies known attacks.
 - Detects signatures across multiple packets.
 - Require periodic updates to signatures.

IDS Analysis Methods & Engine – Anomaly-based

- Statistical / Traffic Anomaly-based
 - Develop baseline of “normal” traffic activities and throughput.
 - Can identify unknown attacks and DoS.
 - Must have a clear understanding of “normal” traffic for IDS tuning.
- Protocol Anomaly-based
 - Looks for deviations from RFC standards.
 - Can identify unknown attacks.
 - May not handle complex protocols (SOAP, XML, etc).