CISSP® Common Body of Knowledge Review:

Access Control Domain

Version: 5.10

Learning Objective

Access Control

Access Control domain covers mechanisms by which a system grants or revokes the right to access data or perform an action on an information system.

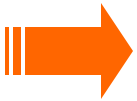
- File permissions, such as “create”, “read”, “edit”, or “delete” on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data right, such as the right to retrieve or update information in a database.

CISSP candidates should fully understand access control concepts, methodologies and their implementation within centralized and decentralized environments across an organization’s computing environment.

Reference: *CISSP CIB*, January 2012 (Rev. 5)

Topics

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

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

Reference: *Access Control: Principles and Practices*, Ravi Sandhu and Pierangela Samarati, IEEE Communications Magazine, September 1994.

Information Protection Environment

- The environment for access control includes the following:
  - Information systems.
  - Facilities (e.g. Physical security countermeasures).
  - Support systems (e.g. Systems that runs the critical infrastructure: HVAC, Utility, Water, etc.)
  - Personnel (e.g. users, operators, customers, or business partners, etc.)

Reference: *Official (ISC)² Guide To The CISSP CBK*, H. Tipton and K. Henry, (ISC)² Press, Auerbach Publications.

Security Consideration in System Life Cycle (SLC) ...(1/2)

1. Initiation Phase (IEEE 1220: Concept Stage)
   - Survey & understand the policies, standards, and guidelines.
   - Identify information assets (tangible & intangible).
   - Define information security categorization & protection level.
   - Define rules of behavior & security CONOPS.
2. Acquisition / Development Phase (IEEE 1220: Development Stage)
   - Conduct business impact analysis (BIA) (a.k.a. risk assessment).
   - Define security requirements and select security controls.
   - Perform cost/benefit analysis (CBA).
   - Security planning (based on risks & CBA).
   - Practice Information Systems Security Engineering (ISSE) Process to develop security controls.
   - Develop security test & evaluation (ST&E) plan for verification & validation of security controls.

Reference: NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*.

Security Consideration in System Life Cycle (SLC) ...(2/2)

3. Implementation Phase (IEEE 1220: Production Stage)
   - Implement security controls in accordance with baseline system design and update system security plan (SSP).
   - Perform Security Certification & Accreditation of target system.
4. Operations / Maintenance Phase (IEEE 1220: Support Stage)
   - Configuration management & perform change control.
   - Continuous monitoring – perform periodic security assessment.
5. Disposition Phase (IEEE 1220: Disposal Stage)
   - Preserve information. archive and store electronic information
   - Sanitize media. Ensure the electronic data stored in the disposed media are deleted, erased, and over-written
   - Dispose hardware. Ensure all electronic data resident in hardware are deleted, erased, and over-written (i.e. EPROM, BIOS, etc.

Reference: NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*.

Information Classification

- Identifies and characterizes the critical information assets (i.e. sensitivity)
- Explains the level of safeguard (protection level) or how the information assets should be handled (sensitivity and confidentiality).

Commercial

- Public.
- Private / Sensitive.
- Confidential / Proprietary.

Military and Civil Gov.

- Unclassified.
- Sensitive But Unclassified (SBU).
- Confidential.
- Secret.
- Top Secret.

Information Classification – Process

1. Determine data classification project objectives.
2. Establish organizational support.
3. Develop data classification policy.
4. Develop data classification standard.
5. Develop data classification process flow and procedure.
6. Develop tools to support processes.
7. Identify application owners.
8. Identify data owners and date owner delegates.
9. Distribute standard templates.
10. Classify information and applications.
11. Develop auditing procedures.
12. Load information into central repository.
13. Train users.
14. Periodically review and update data classifications.

Reference: *Official (ISC)^2 Guide To The CISSP CBK*, H. Tipton and K. Henry, (ISC)^2 Press, Auerbach Publications.

Information Classification – Example Policy (E.O. ~~12958~~/~~13292~~/13526)

- Classification Levels:
  - Top Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
  - Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
  - Confidential shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Information Classification – Example Policy (E.O. ~~12958/13292~~/13526)

E.O. 13526, *Classified National Security Information*, Dec. 29, 2009

- Classification Authority:
  1) The President, Vice President
  2) Agency heads and officials designated by the President in the Federal Register; or
  3) Subordinate USG officials who have a demonstrable and continuing need to exercise classification authority.

  – Each delegation of original classification authority shall be in writing and the authority shall not be re-delegated except as provided in this order. Each delegation shall identify the official by name or position title.

Information Classification – Example Standard (E.O. ~~12958/13292~~/13526)

- Classified Categories:
  - military plans, weapons systems, or operations;
  - foreign government information;
  - intelligence activities (including special activities), intelligence sources or methods, or cryptology;
  - foreign relations or foreign activities of the United States, including confidential sources;
  - scientific, technological, or economic matters relating to the national security;
  - United States Government programs for safeguarding nuclear materials or facilities;
  - vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
  - the development, production, or use of weapons of mass destruction.

Information Classification – Example Guideline

DoD 5200.01, *Information Security Program*, Feb. 24, 2012 prescribes rules for implementation of E.O. 13526 within DoD.

- Volume 1: Overview, Classification, and Declassification
- Volume 2: Marking of Classified Information
- Volume 3: Protection of Classified Information
- Volume 4: Controlled Unclassified Information (CUI)

Reference: DoD Publications (http://www.dtic.mil/whs/directives/corres/pub1.html)

Categories of Security Controls

- Management (Administrative) Controls.
  - Policies, Standards, Processes, Procedures, & Guidelines
    - Administrative Entities: Executive-Level, Mid.-Level Management
- Operational (and Physical) Controls.
  - Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
    - Service Providers: IA, Program Security, Personnel Security, Document Controls (or CM), HR, Finance, etc
  - Physical Security (Facility or Infrastructure Protection)
    - Locks, Doors, Walls, Fence, Curtain, etc.
    - Service Providers: FSO, Guards, Dogs
- Technical (Logical) Controls.
  - Access Controls , Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - Service Providers: Enterprise Architect, Security Engineer, CERT, NOSC, Helpdesk.

Types of Security Controls

- Directive Controls. Policy and standard that advise employees of the expected behavior for protecting an organization's information asset from unauthorized access.
- Preventive Controls. Physical, administrative, and technical measures intended to prevent unauthorized access to organization's information asset.
- Detective Controls. Practices, processes, and tools that identify and possibly react to unauthorized access to information asset.
- Corrective Controls. Physical, administrative, and technical countermeasures designed to react to security incident(s) in order to reduce or eliminate the opportunity for the unwanted event to recur.
- Recovery Controls. The act to restore access controls to protect organization's information asset.

Reference: *CISM Review Manual – 2007*, ISACA.

Example Implementations of Access Controls

	Directive	Preventive	Detective	Corrective	Recovery
Management (Administrative)	• Policy • Guidelines	• User registration • User agreement • NdA • Separation of duties • Warning banner	• Review access logs • Job rotation • Investigation • Security awareness training	• Penalty • Administrative leave • Controlled termination processes	• Business continuity planning (BCP) • Disaster recovery planning (DRP)
Physical/ Operational	• Procedure	• Physical barriers • Locks • Badge system • Security Guard • Mantrap doors • Effective hiring practice • Awareness training,	• Monitor access • Motion detectors • CCTV	• User behavioral modification • Modify and update physical barriers	• Reconstruction • Offsite facility

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	• Standards,	• User authentication • Multi-factor authentication • ACLs • Firewalls • IPS • Encryption	• Log access and transactions • Store access logs • SNMP • IDS	• Isolate, terminate connections • Modify and update access privileges	• Backups • Recover system functions, • Rebuild,

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

Questions:

- What are the two security implementation principles for access control?
  -
  -
- What are the four access control environments?
  -
  -
  -
  -

Answers:

- What are the two security implementation principles for access control?
  - Least privilege
  - Separation of duties

- What are the four access control environments?
  - Information systems
  - Facilities
  - Support systems
  - Personnel

Questions:

- In the process of establishing a data classification program, why it is important to develop the policy, standard, process, and procedure?
  - Policy defines…
  - Standard delineates...
  - Process explains ...
  - Procedure provides...

Answers:

- In the process of establishing a data classification program, why it is important to develop the policy, standard, process, and procedure?
  - Policy defines the management's goals and objectives (i.e., requirements) to classify the information assets. Identifies the roles and assign responsibilities.
  - Standard delineates the data types and defines the protection levels required.
  - Process explains the mandatory activities, actions, and rules for data classification.
  - Procedure provides the step-by-step instruction on how to identify and classify data.

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
    - Trapdoor
- 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 (a.k.a. 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 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.

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

- Macro Viruses
- Trojans and Worms
- Instant Messaging Attacks
- Internet Browser Attacks
- Malicious Java Applets
- Malicious Active X Controls
- Email Attacks

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.
  - Programmer implementing parameter checks and enforce data rules.

Software Defects – Memory Protection Threats

- Memory protection is enforcement of access control and privilege level to prevent unauthorized access to OS memory.
- Countermeasures:
  - Ensure all system-wide data structures and memory pools used by kernel-mode system components can only be accessed while in kernel mode.
  - Separate software processes, protect private address space from other processes.
  - Hardware-controlled memory protection
  - Use Access Control List (ACL) to protect shared memory objects.

Software Defects – Covert Channel Threats*

- Covert channel is an un-controlled information flow (or unauthorized information transfer) through hidden communication path(s).
  - Storage channel
  - Timing channel
- Countermeasure steps:
  - Identify potential covert channel(s)
  - Verify and validate existence of covert channel(s)
  - Close the covert channel by install patch or packet-filtering security mechanism.

*** Note**: The “classic” definition of covert channel is in the context of TCSEC (i.e., storage & timing channels).

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

Topics

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

Control Types & Examples

- Administrative (or Directive Controls)
  - Regulations, Policies, Standards, Guidelines, Processes & Procedures

- Physical and Technical Controls
  - Preventive – Controls that avoid incident
  - Detective – Controls that identify incident
  - Corrective – Controls that remedy incident
  - Recovery – Controls that restores baseline from incident

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).

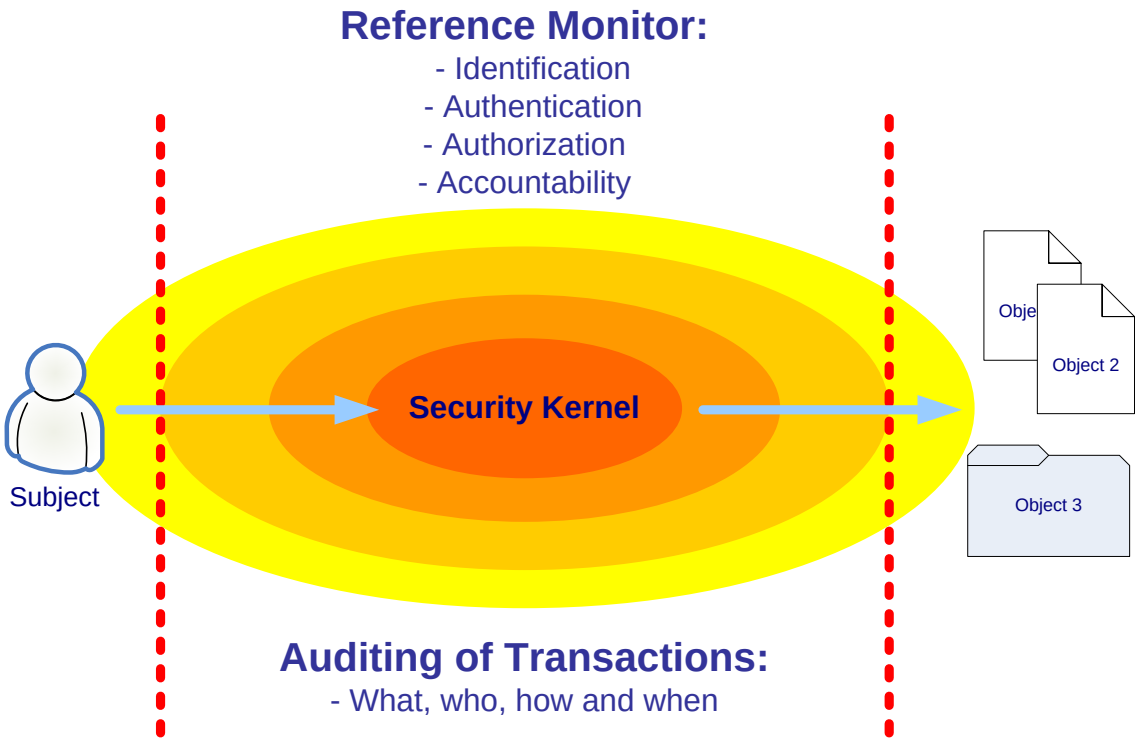
Identification & Authentication

- 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.

Authentication, Authorization & Accountability (AAA)

- Access control is not complete without coupled with auditing for accountability.
- Reference monitor provides the mechanism for access control. (i.e., AAA)



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.>

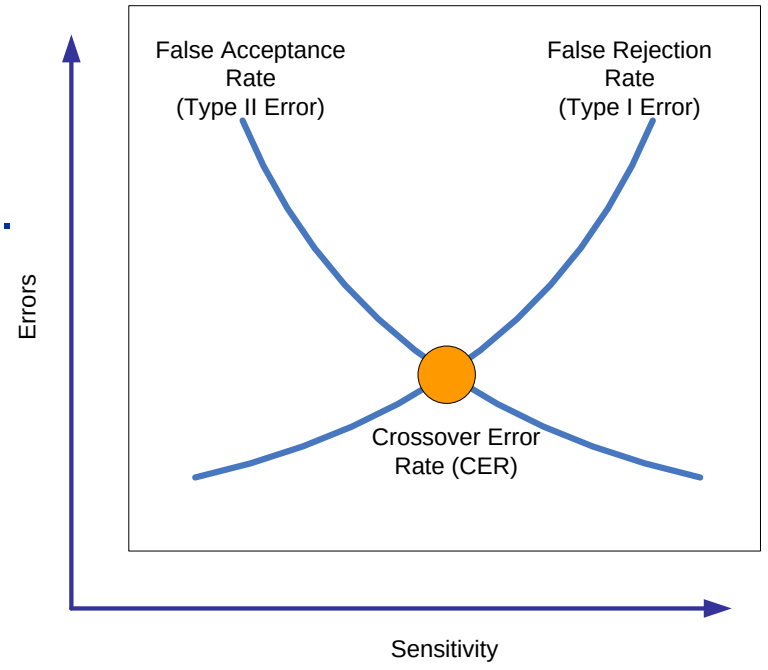
Something the Subject HAS

- One-Time Password (OTP)
  - Something generated from a RNG device that generates an OTP
- Synchronous Token
  - Counter-based token (e.g. RSA token)
  - Clock-based token (e.g. Kerberos token)
- Asynchronous Token
  - Challenge-response devices (e.g. token cards, grid cards)
  - 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.



Questions:

- What are the three types of access control?
  -
  -
  -
- What are the six categories of controls?
  -
  -
  -
  -
  -
  -

Answers:

- What are the three types of access control?
  - Administrative (Management)
  - Technical (Logical)
  - Physical (Operational)

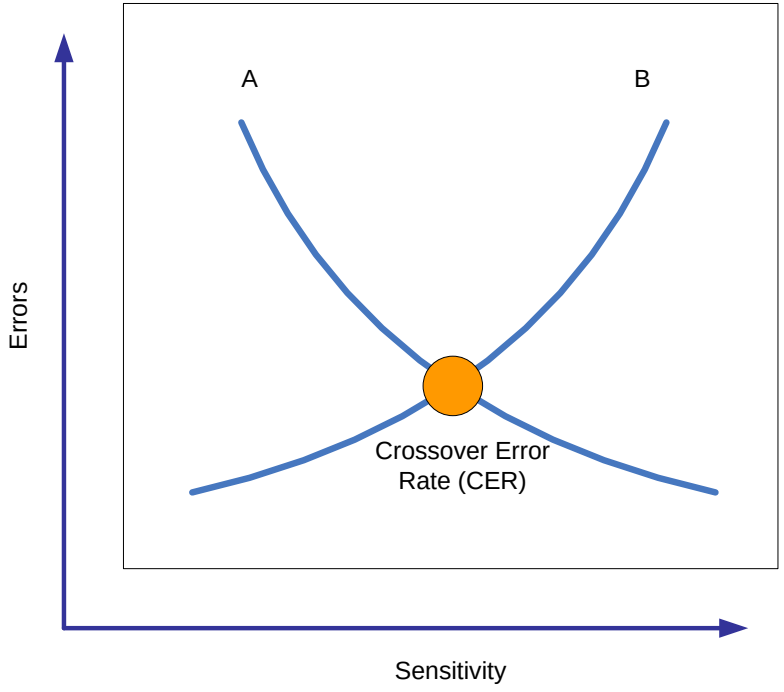
- What are the five categories of controls?
  - Preventive
  - Detective
  - Corrective
  - Recovery
  - Directive

Questions:

- What are the three types of authentication factors?
  -
  -
  -

- For biometrics authentication…
- What is A?
  -

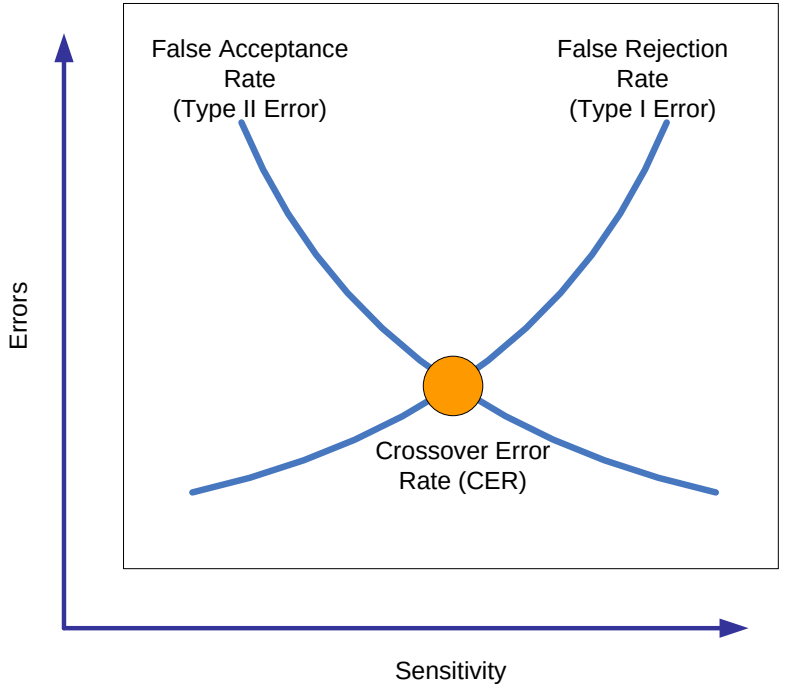
- What is B?
  -



Answers:

- What are the three types of authentication factors?
  - Something the subject knows
  - Something the subject has
  - Something the subject is

- For biometrics authentication…
- What is A?
  - False Acceptance Rate (Type II Error)
- What is B?
  - False Rejection Rate (Type I Error)



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 Revisited…

- 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, and Clark-Wilson
  - Rule-set based Access Model:
    - Role-based Access Control (RBAC)

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 Control Matrix – Using Graham-Denning

- Graham-Denning is an information access control model operates on a set of subjects, objects, rights and an access capability matrix.
  - How to securely create an object/subject.
  - How to securely delete an object/subject.
  - How to securely provide the read access right.
  - How to securely provide the grant access right.
  - How to securely provide the delete access right.
  - How to securely provide the transfer access right.

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
  - Windows has 14 access permission settings for SID & UID!
    - Full Control,
    - Traverse Folder / Execute File, List Folder / Read Data,
    - Read Attributes, Read Extended Attributes,
    - Create Files / Write Data, Create Folders / Append Data,
    - Write Attributes, Write Extended Attributes,
    - Delete Subfolders and Files, Delete,
    - Read Permissions, Change Permissions, Take Ownership

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--

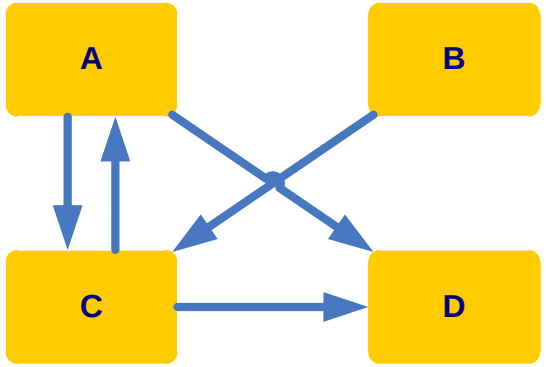
Information Flow Model

Information Flow Model illustrates the direction of data flow between objects

- Based on object security levels
- Information flow is constrained in accordance with object's security attributes
- Covert channel analysis is simplified

Note: Covert channel is moving of information to and from unauthorized transport

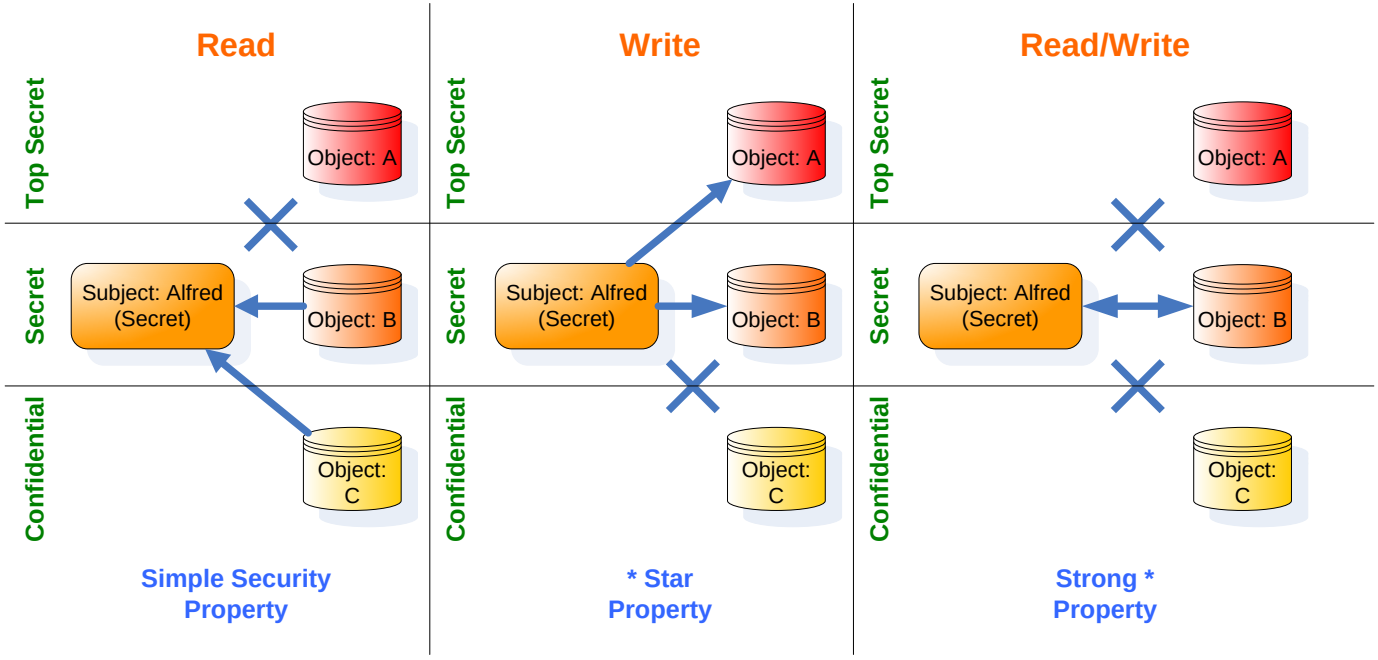
	A	B	C	D
A	N/A		X	X
B		N/A	X	
C	X		N/A	X
D				N/A



Bell-LaPadula Security Model

Bell-LaPadula confidentiality policy:

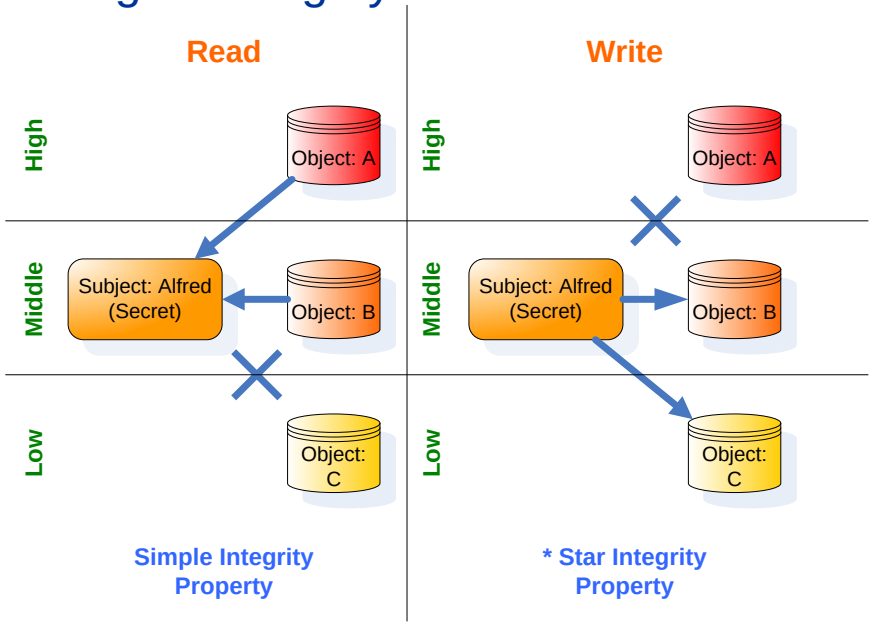
- Simple security property
  - Subject cannot read object of higher sensitivity.
- Star property (* property)
  - Subject cannot write to object of lower sensitivity.
- Strong Star property (Strong * property)
  - Subject cannot read/write to object of higher/lower sensitivity.



Biba Security Model

Biba security policy:

- Simple integrity condition
  - Subject cannot read objects of lesser integrity.
- Integrity star * property
  - Subject cannot write to objects of higher integrity.
- Invocation property
  - Subject cannot send messages (logical request for service) to object of higher integrity.

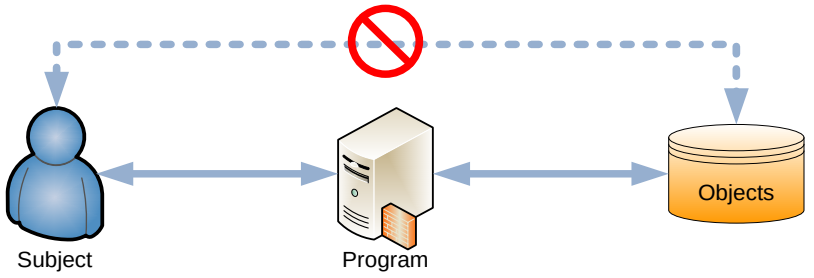


Clark-Wilson Security Model

Clark-Wilson is a state-machine security model addresses information flow and the integrity goals of:

- Preventing unauthorized subjects from modifying objects
- Preventing authorized subjects from making improper modification of objects
- Maintaining internal and external consistency

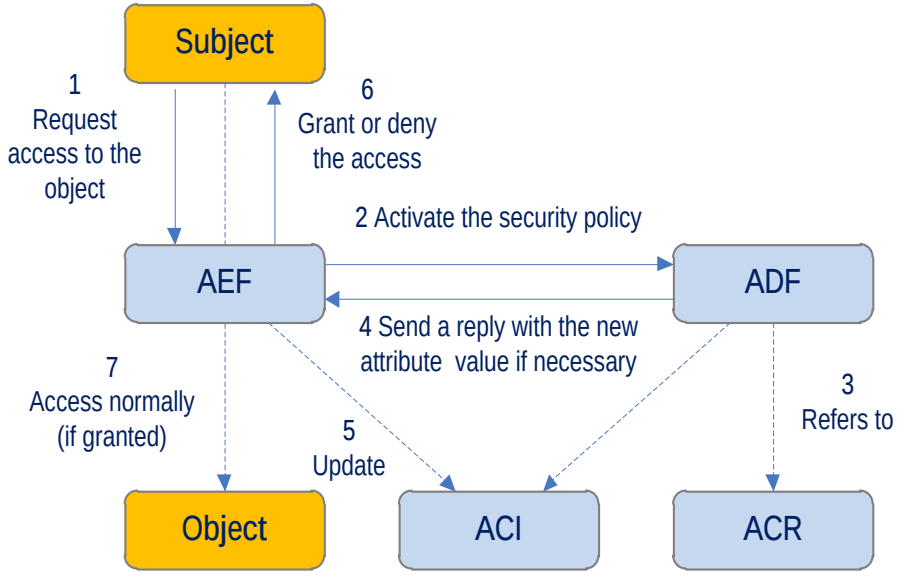
- Well-formed transaction
  - Preserve/ensure internal consistency
  - Subject can manipulate objects (i.e. data) only in ways that ensure internal consistency.
- Access Triple: Subject-Program-Object
  - Subject-to-Program and Program-to-Object.
  - Separation-of-Duties



Reference: D. Clark, D. Wilson, *A Comparison of Commercial and Military Computer Security Policies*, IEEE Symposium on Security and Privacy, 1987

Rule-set Based Access Control Model

- Access is based on a set of rules that determines capabilities.
- The model consists of:
  - Access enforcement function (AEF)
  - Access decision function (ADF)
  - Access control rules (ACR)
  - Access control information (ACI)



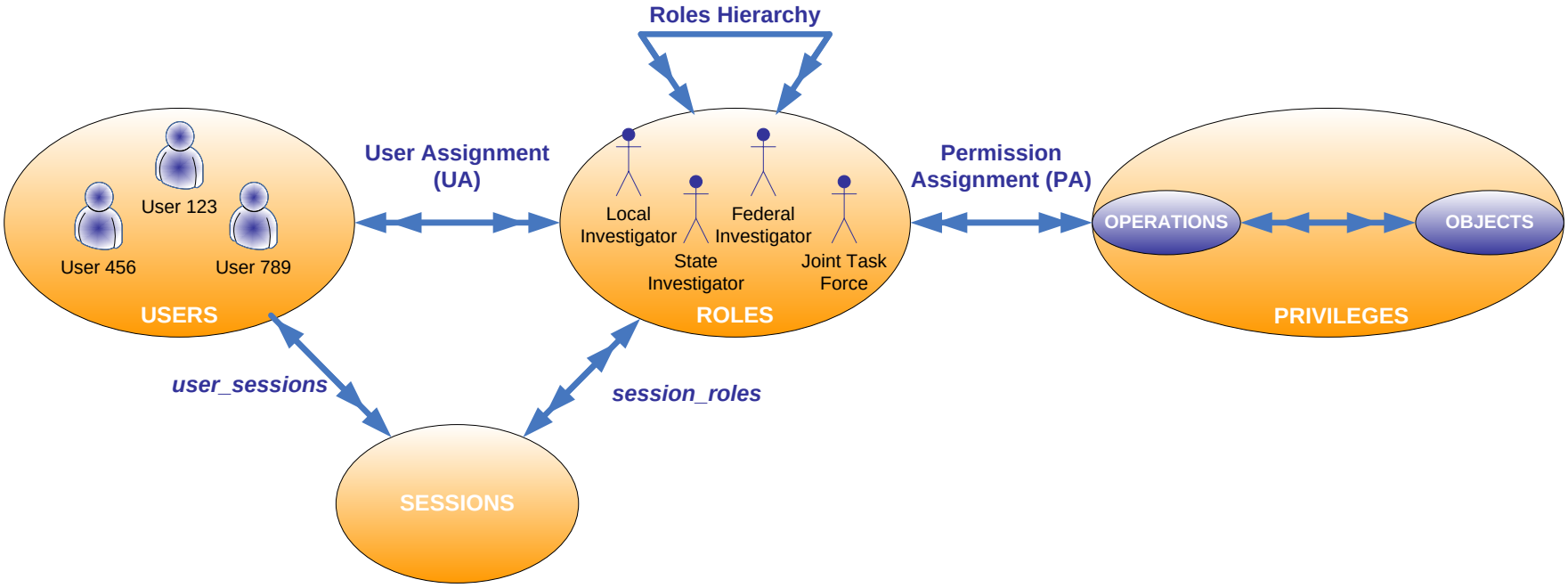
Reference: M.D. Abrams, K.W. Eggers, L.J. LaPadula, I.M. Olson, *Generalized Framework for Access Control: An Informal Description*,, October, 1990.

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.

Role-based Access Control (RBAC)

- Limited hierarchical RBAC-based authorization for web services.
  - User Assignment: Identity-to-roles.
  - Permission Assignment: Roles-to-privileges.



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.

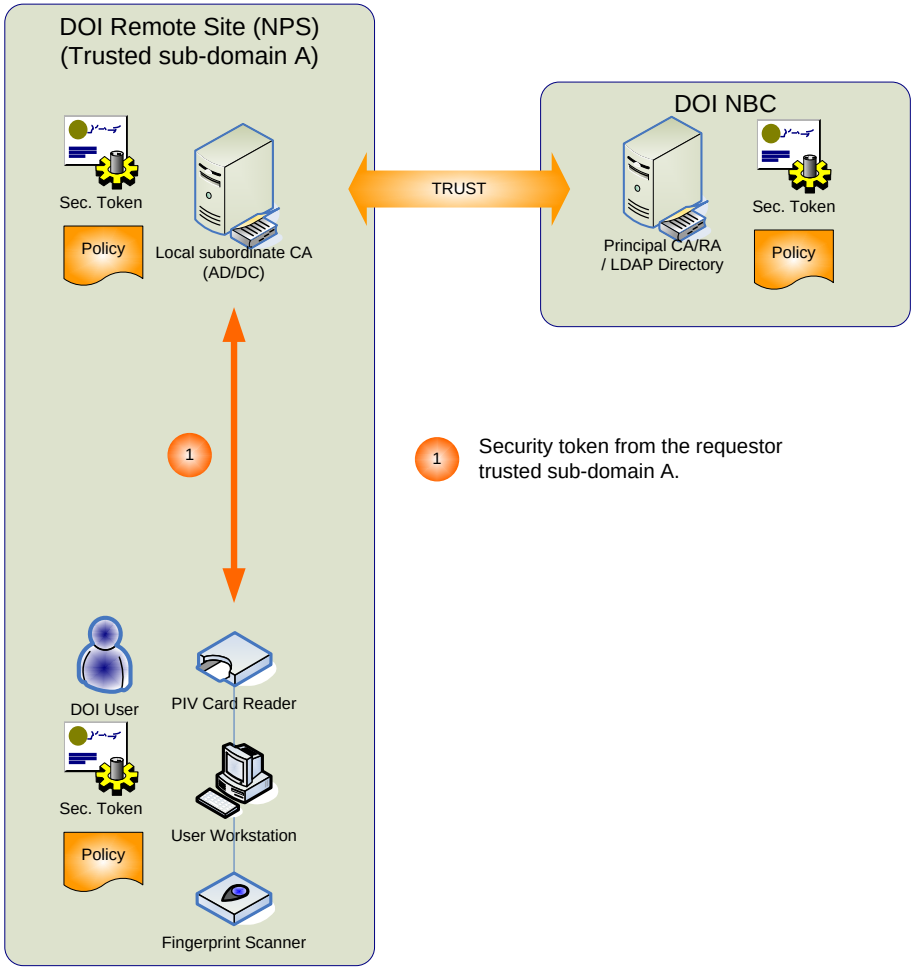
Decentralized Access Control Method

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 singe-, two-, or three-factor authentication method.
- A security token is then issued to the authenticated subject along with access policy.

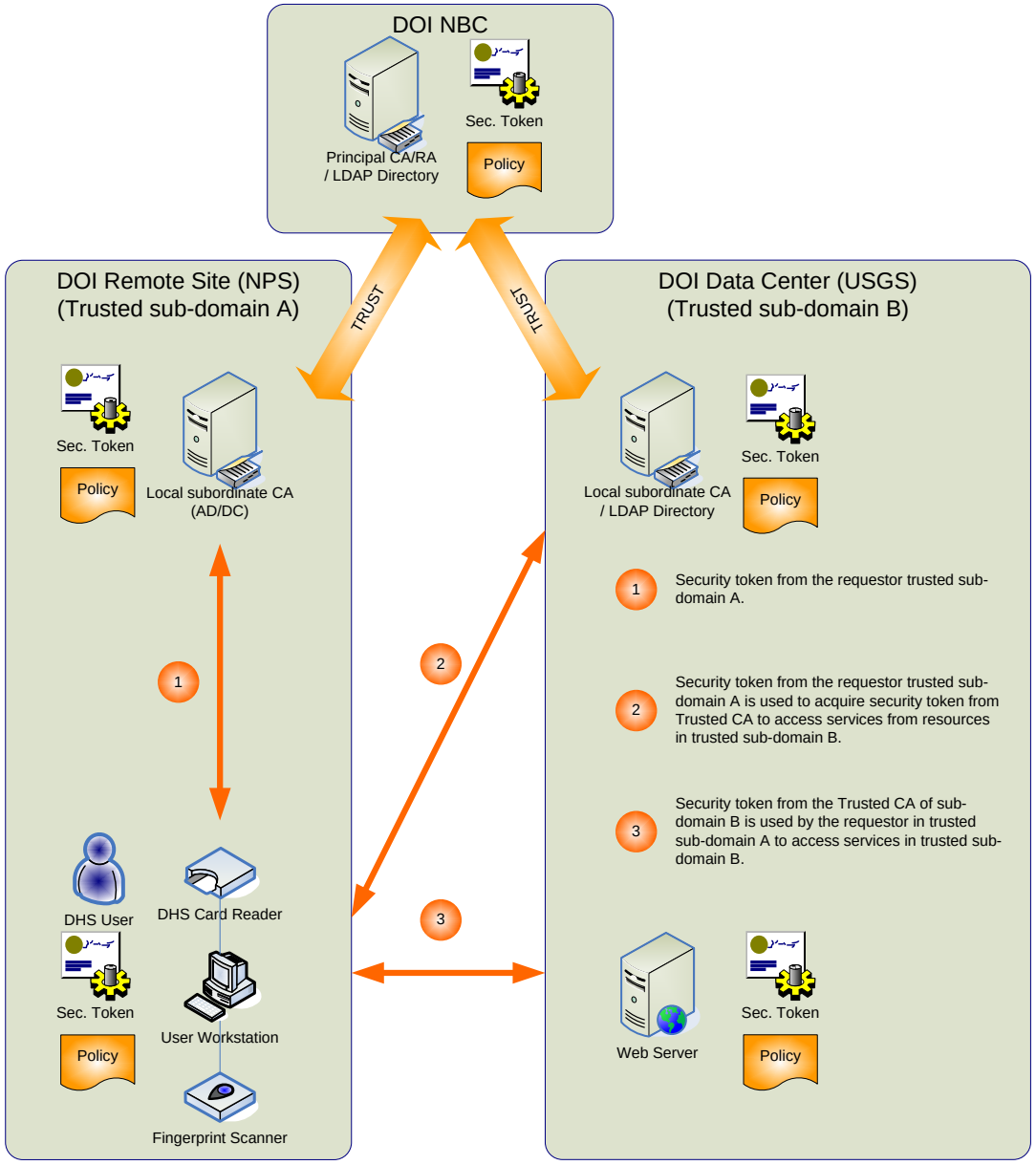


Decentralized Access Control Method

Single Sign-On

Step 2: Distributed Auth.

- The objects (i.e. web browser and web server) exchange certificate tokens and negotiate SSL/TLS session.
- The subjects' authenticated credential is asserted using SAML and validated by the root CA.



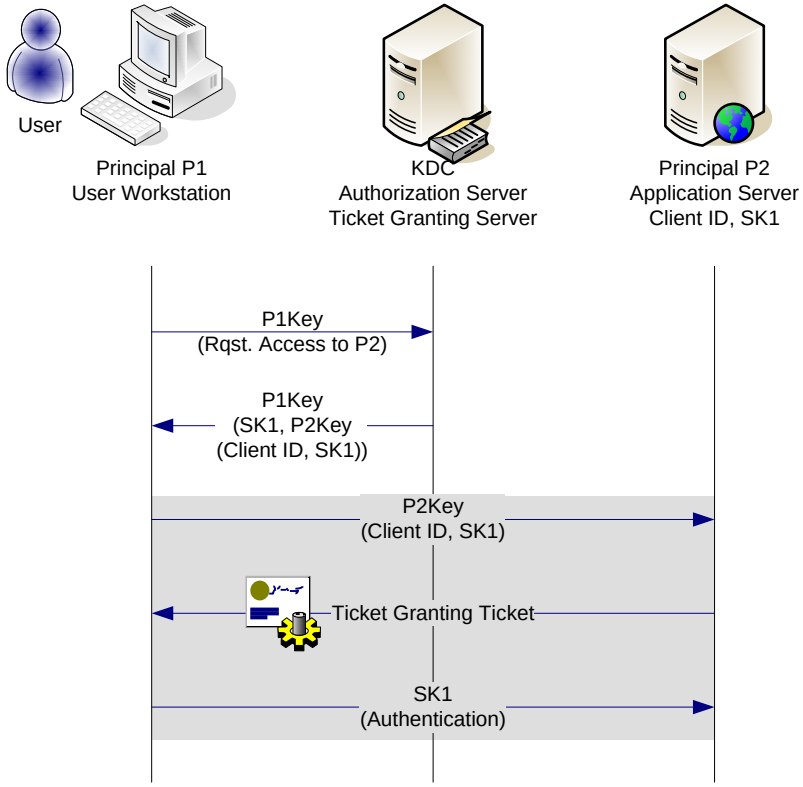
Decentralized Access Control Method

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

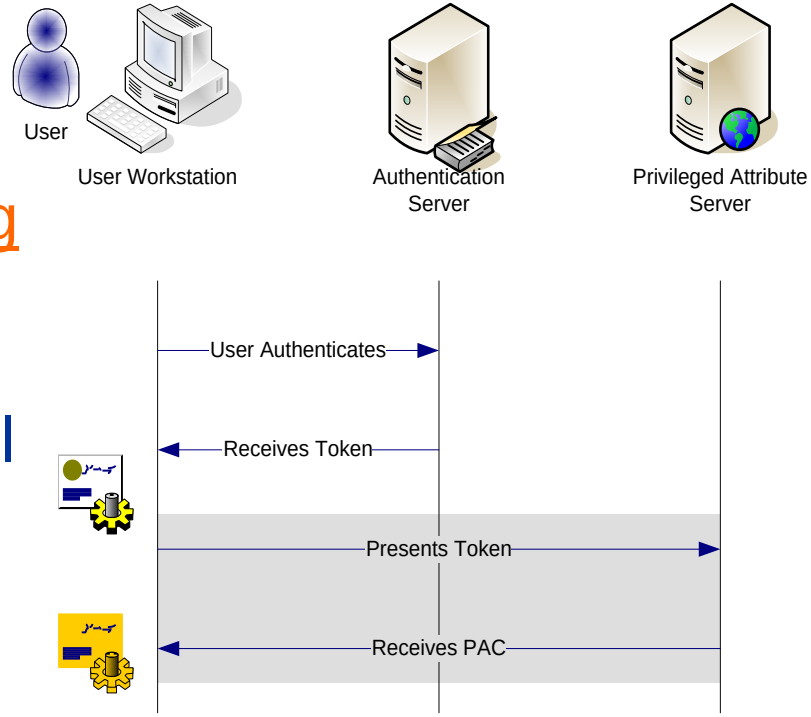
- The Kerberos Key Distribution Center (KDC) server serves two functions:
- An Authentication Server (AS), which authenticates a Principal via a pre-exchanged Secret Key
- A Ticket Granting Server (TGS), which provides a means to securely authenticate a trusted relationship between two Principals.



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.



Questions:

- What are the difference between discretionary access control (DAC) and mandatory access control (MAC)?
  - DAC:
  - MAC:
- Role-based access control is based on ?
  -
- Rule-based access control is based on ?
  -

Answers:

- What are the difference between discretionary access control (DAC) and mandatory access control (MAC)?
  - DAC: Information owner determines who can access and what privilege the subject may has.
  - MAC: Information owner and system determines assess. Clearance of subject = Classification of object.

- Role-based access control is based on ?
  - User's job function.

- Rule-based access control is based on ?
  - Rules created by information owners.

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

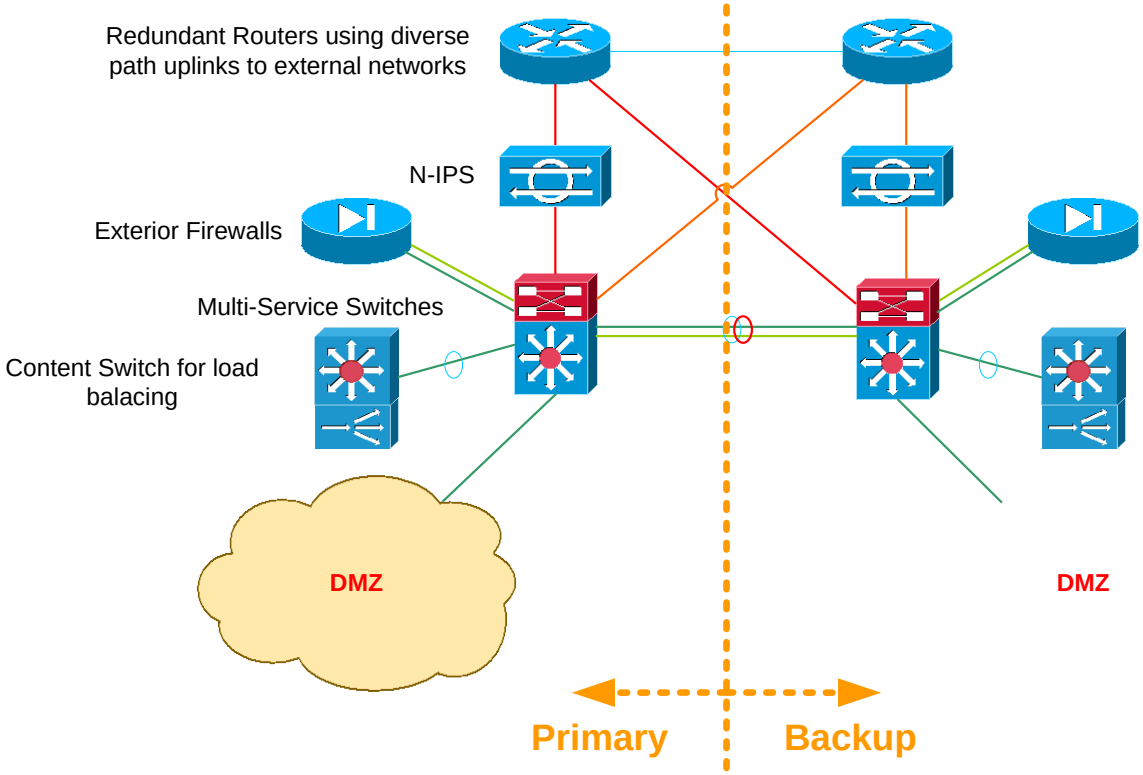
Intrusion Prevention & Detection

- Intrusion Prevention System (IPS)
  - In-line preventive control device.
  - Actively intercept and forward packets.
  - Access control and policy enforcement.
  - Usually a network-based device.
- Intrusion Detection Systems (IDS)
  - Passive monitoring devices.
  - Network-based (N-IDS) and Host-based (H-IDS).
  - Passively monitor and audit transmitted packets.
  - Patter/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.

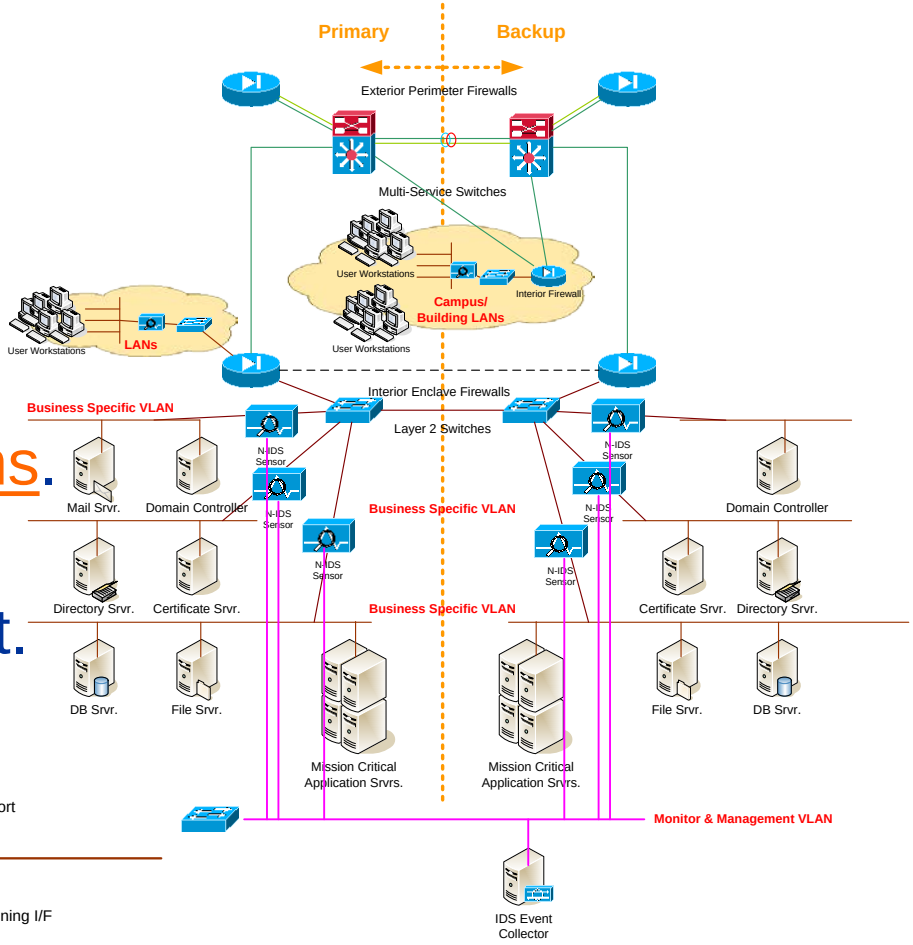
- Ability to block attacks in real time.
- Actively intercept and forward packets.

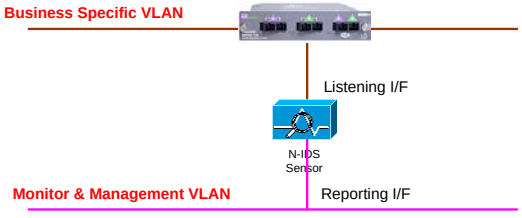


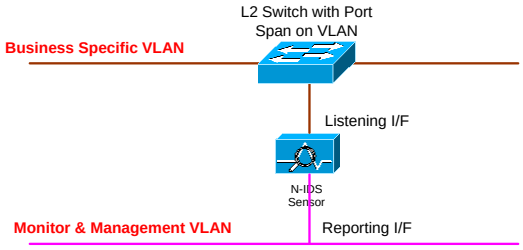
Network-based IDS (N-IDS)

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 know 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).

Audit Trail Monitoring

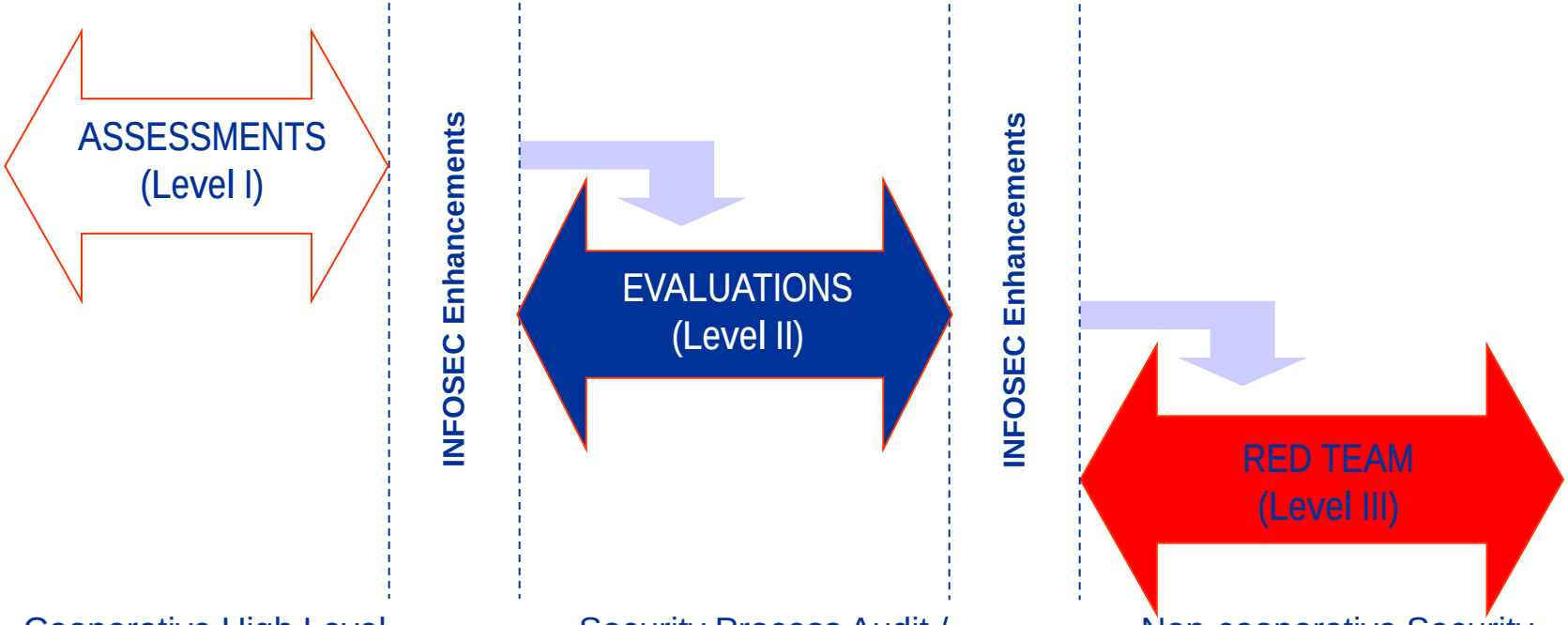
Audit trail is a record of system activities that captures system, network, application & user activities.

- Audit trail can:
  - Alert security officer of suspicious activities.
  - Provide details on non-conformance or illegal activities.
  - Provide information for legal proceedings.
- Audit trail issues:
  - Data volume: need to set clipping level (event filtering) to log event details.
  - Personnel training: to identify non-conformance or illegal activities.
  - Store & archive: need access control to audit logs, and secure storage for archive.

Security Assessment & Evaluation vs. Security Audit

- Security Audit: To verify meeting of defined & specified security requirements.
  - Used mostly in Security Certification & Accreditation Process (CT&E, ST&E).
  - Security audit produces conformance metrics.
- Security/Vulnerability Assessment & Evaluation: To find security vulnerabilities and assess potential exposures.
  - Used mostly in Risk Assessment & Evaluation Process.
  - Vulnerability assessment produces profile of security posture.

Security Assessment & Evaluation – NSA Defined (White, Blue & Red Teams)



- Cooperative High Level Overview
- Information / Mission Critical Analysis (Compliance Audit)
- Inventory Audit of Assets
- Information / Data Flow Analysis

- Security Process Audit / Analysis
- Detailed Inventory Audit of Assets
- Cooperative Security Testing / Audit
  - Non-Intrusive Tests
  - Penetration Tests

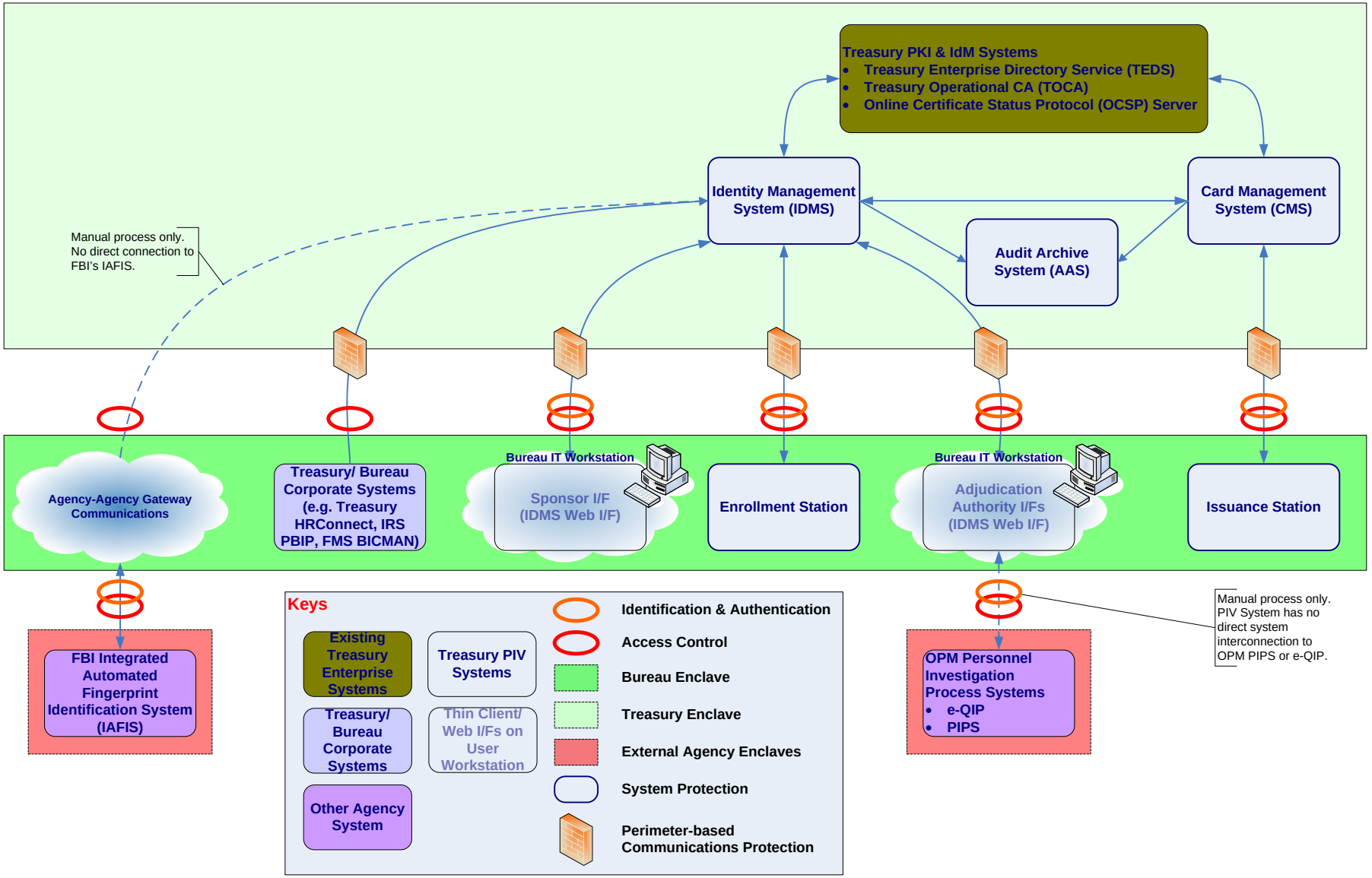
- Non-cooperative Security Testing
  - External Penetration Tests
- Simulation of Appropriate Adversary

Validation Time… ☺

1. Classroom Exercise

2. Review Answers

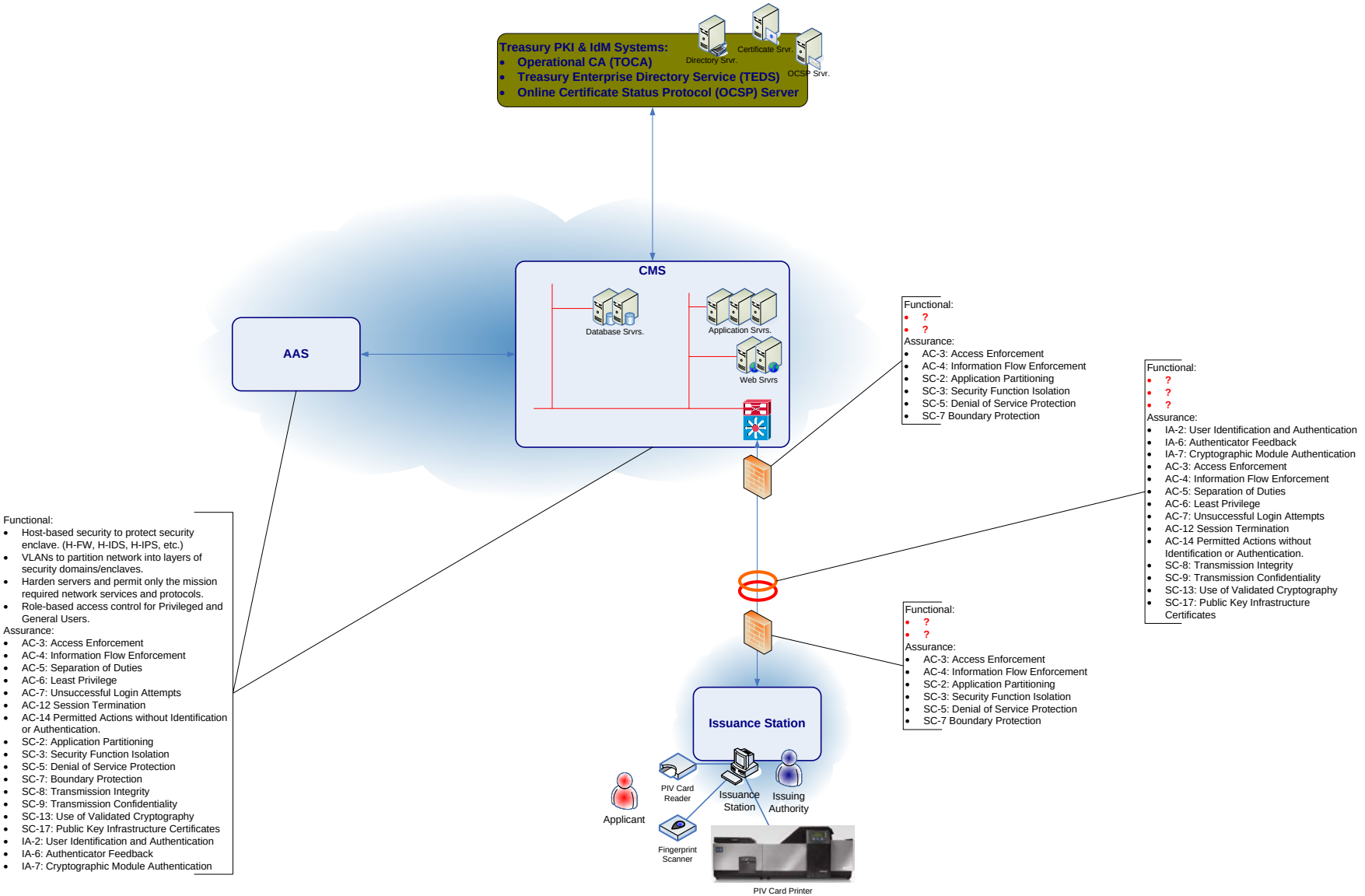
Exercise #1:



Exercise #1: Data Flow

	PIV System Data Flow								
	IDMS	CMS	Enrollment Station	Issuance Station	Sponsorship I/F	Adjudication I/F	Treasury PKI/IdM	Corporate System	AAS
IDMS									
CMS									
Enrollment Station									
Issuance Station									
Sponsorship I/F									
Adjudication I/F									
Treasury PKI/IdM									
Corporate System									
AAS									

Exercise #2: Security Controls



Exercise #2: Security Controls

- Please describe the functional security controls needed for meeting the assurance requirements…

Suggested

ANSWERS

Exercise #1: Data Flow

	PIV System Data Flow								
	IDMS	CMS	Enrollment Station	Issuance Station	Sponsorship I/F	Adjudication I/F	Treasury PKI/IdM	Corporate System	AAS
IDMS		X	X		X	X	X		X
CMS	X			X			X		X
Enrollment Station	X								
Issuance Station		X							
Sponsorship I/F	X								
Adjudication I/F	X								
Treasury PKI/IdM	X	X							
Corporate System	X								
AAS									

Exercise #2: Security Controls