Module 1
Security Fundamentals

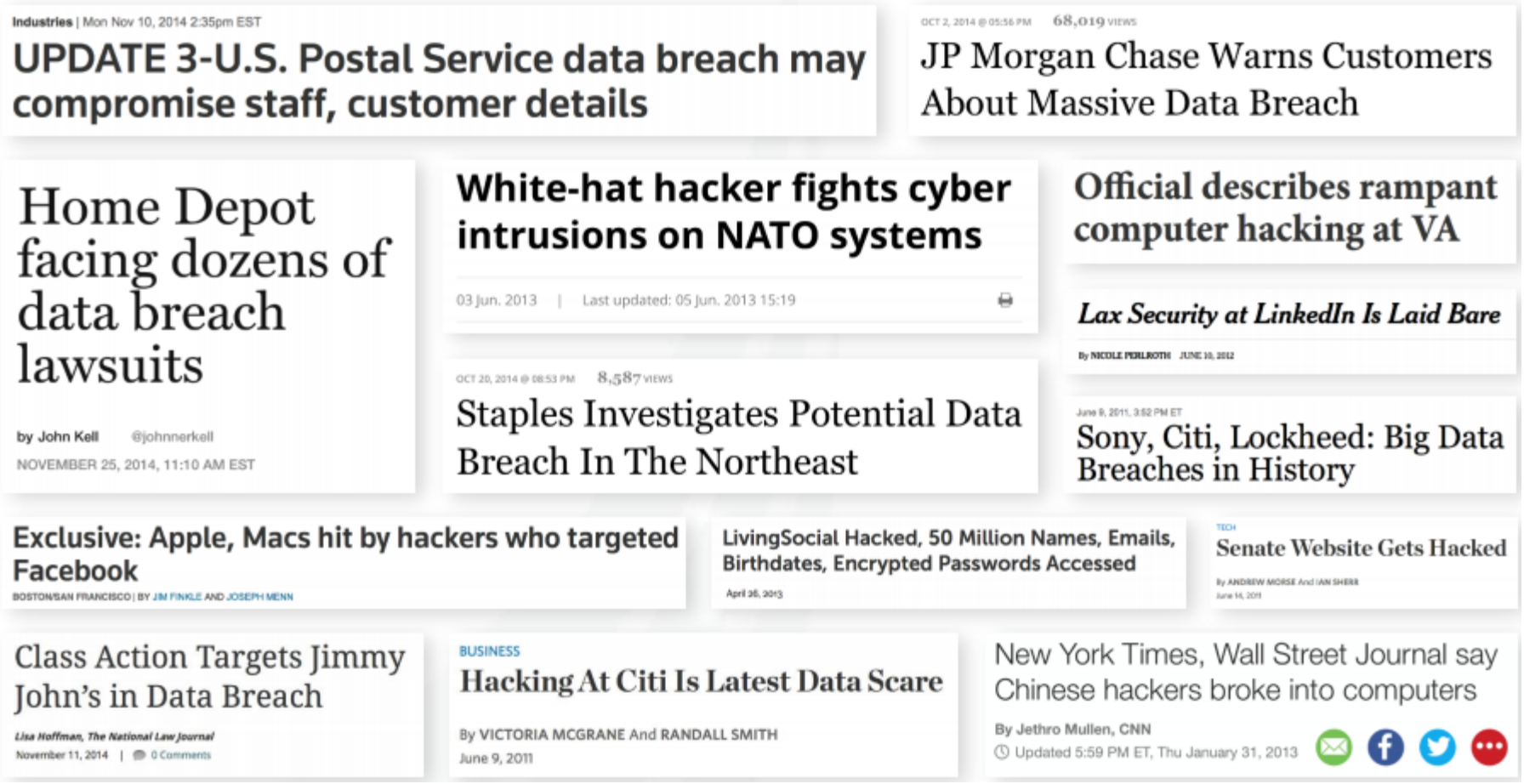
Submodule 1: Security Concepts and Principles

Submodule Learning Outcomes:

Accurately explain basic cybersecurity related concepts.

Clearly define principles of cybersecurity.

Explain security models with precision.


Industries | Mon Nov 10, 2014 2:35pm EST
UPDATE 3-U.S. Postal Service data breach may compromise staff, customer details
OCT 2, 2014 @ 05:56 PM 68,019 VIEWS
JP Morgan Chase Warns Customers About Massive Data Breach
Home Depot facing dozens of data breach lawsuits
by John Kell @johnnerkell
NOVEMBER 25, 2014, 11:10 AM EST
White-hat hacker fights cyber intrusions on NATO systems
03 Jun. 2013 | Last updated: 05 Jun. 2013 15:19
Official describes rampant computer hacking at VA
Lax Security at LinkedIn Is Laid Bare
By NICOLE PERLROTH JUNE 10, 2012
OCT 20, 2014 @ 08:53 PM 8,587 VIEWS
Staples Investigates Potential Data Breach In The Northeast
June 9, 2011, 3:52 PM ET
Sony, Citi, Lockheed: Big Data Breaches in History
Exclusive: Apple, Macs hit by hackers who targeted Facebook
BOSTON/SAN FRANCISCO | BY JIM FINKLE AND JOSEPH MENN
LivingSocial Hacked, 50 Million Names, Emails, Birthdates, Encrypted Passwords Accessed
April 26, 2013
TECH
Senate Website Gets Hacked
By ANDREW MORSE And IAN SHERR
Class Action Targets Jimmy John's in Data Breach
Lisa Hoffman, The National Law Journal
November 11, 2014 | 0 Comments
BUSINESS
Hacking At Citi Is Latest Data Scare
By VICTORIA MCGRANE And RANDALL SMITH
June 9, 2011
New York Times, Wall Street Journal say Chinese hackers broke into computers
By Jethro Mullen, CNN
Updated 5:59 PM ET, Thu January 31, 2013

Vulnerability & Risk

- Vulnerability: weakness or fault that can lead to an exposure
- Exposure: a successful attack
- Risk: the possibility of damage happening and the ramification of such damage should it occur.
  - It captures the likelihood that a vulnerability materializes into an exposure

Threats

- Threat: an object, person, or other entity that represents a constant danger to an asset.

- Threats are everywhere:
  - SANS 2016 State of ICS Security Surveys: 73% of organizations reported perceived high or moderate levels of threats to control systems;

  - SANS 2016 Survey on Security and Risk in the Financial Sector: the top attack vectors include Ransomeware (55%), Spearphishing or whaling (50%), and APTs (32%);

Components of a Threat

- Threat agent/actor: a specific object, person who poses danger of carrying out an attack.
  - For instance, DDoS attacks are a threat. The hacker who carries out that attack is a threat agent.

- Threat target: anything of value to the threat agent/ actor.
  - A piece of hardware, or your identity

- Threat vector: a path or a tool that a threat agent uses to attack the target, it captures how the attack is carried out.
  - Malicious email attachment is a threat vector

Threats to Information Security

Categories of Threats	Examples
Acts of human error or failure	Employee mistakes
Compromises to intellectual property	Piracy
Deliberate acts of espionage or trespass	Unauthorized access to data
Deliberate acts of information extortion	Blackmail of information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Malware
Forces of nature	Fire, hurricane
Deviations in quality of service from service providers	Power outage
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs
Technological obsolescence	Outdate technologies

Acts of Human Error or Failure

- Performed without malicious intent but because of:
  - Inexperience
  - Carelessness
  - Insufficient training
- An organization's employees probably pose the biggest threat to its data/information
- Errors/mistakes may include:
  - Enter wrong data
  - Accidental deletion or update of data
  - Not properly protected data storage
  - Revelation of classified data
- Insider threat

Deviations in Quality of Services

- Products and services that are needed to support regular business operations may become unavailable;
- Other systems you depend on may become unavailable;
- Critical services such as Internet, Telecommunication, and power may become unavailable or irregular;
- Internet service issues may include:
  - Internet Service Provider (ISP) failures can compromise the availability of data/ information;
  - Outsourced Web hosting provider assumes responsibility for all Internet services as well as hardware and Website operating system software.

In-Class Case Study

Read the given description of CryptoLocker, identify/illustrate the security related concepts we have discussed.

Risk Management

- Risk management is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.
- Risk assessment is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.
- Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats.

Risk Analysis

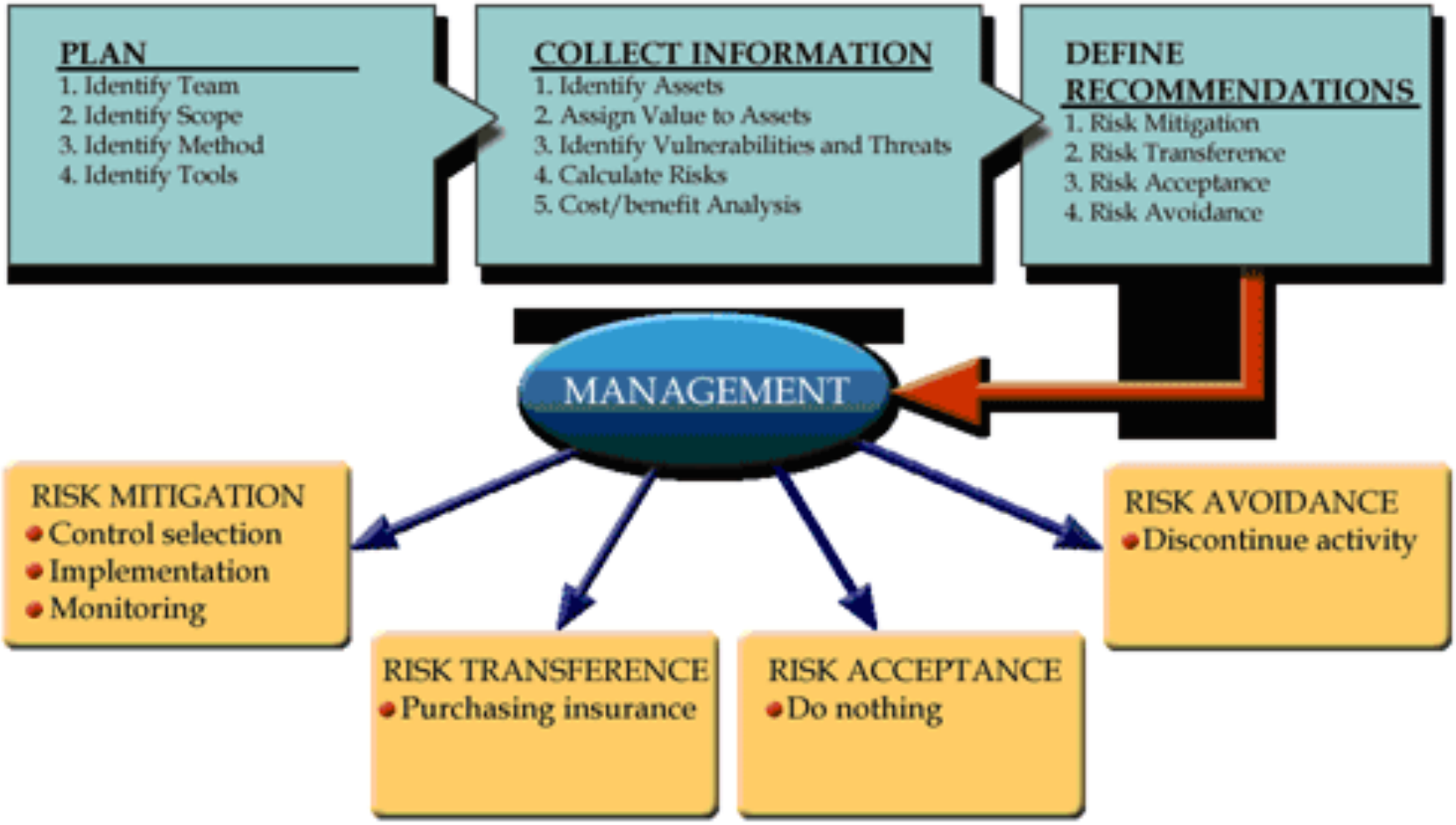
- Risk analysis helps companies prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in sensible manners.
- It has four main goals:
  - Identify assets and their value to the organization
  - Identify vulnerabilities and threats
  - Quantify the probability and business impact of these potential threats
  - Provide an economic balance between the impact of the threat and the cost of the countermeasure

How to Handle Risks?

- Total risk = threats X vulnerability X asset value

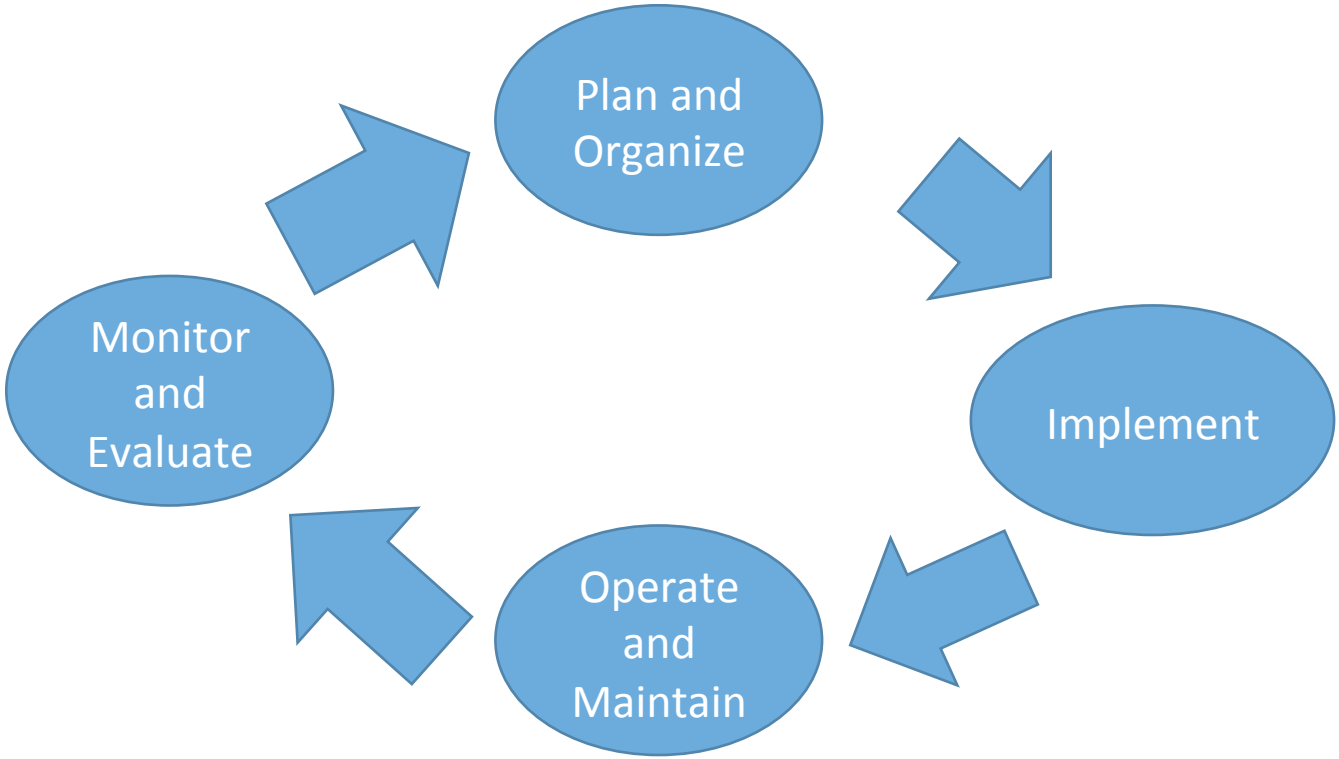
- Residual risk = total risk X controls gap
  = total risk – countermeasures

- To handle residual risks:
  - Transfer it
  - Avoid it
  - Reduce it
  - Accept it


PLAN
1. Identify Team
2. Identify Scope
3. Identify Method
4. Identify Tools
COLLECT INFORMATION
1. Identify Assets
2. Assign Value to Assets
3. Identify Vulnerabilities and Threats
4. Calculate Risks
5. Cost/benefit Analysis
DEFINE RECOMMENDATIONS
1. Risk Mitigation
2. Risk Transference
3. Risk Acceptance
4. Risk Avoidance
MANAGEMENT
RISK MITIGATION
Control selection
Implementation
Monitoring
RISK TRANSFERENCE
Purchasing insurance
RISK ACCEPTANCE
Do nothing
RISK AVOIDANCE
Discontinue activity

Security Life Cycle

- Security should be treated as an ongoing and continuous improving process rather than a project with start and end date.



The CIA Triad

Ensures that the information is accessible only to those who authorized to have access.

Prevention of unauthorized disclosure of data and resources.

Ensures that authorized users have access to information and associated assets when required.

Prevention of loss of, or loss of access to, data and resources.

Safeguards the accuracy and completeness of information and processing methods.

Prevention of unauthorized modification of data and resources.

Availability

- All systems should perform in a predictable manner and with the condition that the performance is of an acceptable level.
- Causes of availability problems:
  - Software
    - Denied access to information resulting in software non availability
    - Denied access to due strong encryption
  - Hardware
    - Denial of service due to DDOS attacks
    - Denial of service due to hardware non availability
  - Unexpected circumstances:
    - As result of natural event
    - As result of man-made disasters

Integrity

- Requires a combination of hardware, software and communication methods to ensure that the data is not compromised.
- Carefully developed controls are key to preventing data integrity problems.
- The integrity of the data can be compromised either by mistake or with specific intent.
- The integrity principle can be interpreted as to:
  - Whether the information is valid
  - Whether the data has been compromised
  - Whether the data source can be determined and verified.

Confidentiality

- The privacy of the data can be protected through a combination of data access control and encryption.
- The secrecy can be compromised in several ways:
  - Malware
  - Intruders
  - Insecure networks
  - Poorly administrated system
  - Packet capture
  - Social engineering
  - Password attacks

Other Security Concepts

- Authentication: act of verifying a claim of identity

- Authorization: after a person, program or system has been identified and authenticated, it must be determined what informational resources they should have access to and what actions they could perform on the resources.

- Non-repudiation: one party of a transaction cannot deny having participated in a transaction.

Security Design Principles

- Saltzer & Schroeder describe 8 principles for design and implementation of security mechanisms.
- The general ideas behind these principles are:
  - Simplicity:
    - Makes designs and mechanisms easy to understand;
    - Also makes it less possible to make mistakes;
    - Reduces potential for inconsistencies.
  - Restriction:
    - Minimizes the power of an entity, therefore, reduce potential harm;
    - Entities communication with one another only when necessary, and in as few(and narrow) ways as possible.

Source: J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems, " Proceedings of the IEEE 63 (9), pp. 1278-1308 (Sep. 1975)

Principle of Least Privilege

- Principle of Least Privilege: a subject should be given only those privileges that it needs in order to complete its task.
  - The “need to know” rule
  - In reality, this principle often cannot be applied precisely

Principle of Fail-Safe Defaults

- Principle of Fail-Safe Defaults: unless a subject is given explicit access to an object, it should be denied access to that object.
  - Default access to an object should be none.
  - It is a conservative design that is based on the arguments why objects should be accessible, rather than why they should not.

Principle of Economy of Mechanism

- Principle of Economy of Mechanism: the security mechanisms should be as simple as possible.
  - The rule applies to any aspect of a system especially the protection mechanism.
  - Small and simple design reduce the possibility of error.
  - Small and simple design also make it possible to inspect software and hardware for potential vulnerabilities.

Principle of Complete Mediation

- Principle of Complete Mediation: requires that all accesses to objects be checked to ensure that they are allowed.
  - For a subject that wants access to an object, operating systems should determine if the action is allowed.
  - If the access attempt is made again, check should be performed again.

Principle of Open Design

- Principle of Open Design: the security of a mechanism should not depend on the secrecy of its design or implementation.
  - If the strength of the program's security depends on the ignorance of the user, a knowledgeable user can defeat the security mechanism—"security through obscurity".
  - Issues of proprietary software and trade secrets complicate the application of this principle.

Principle of Separation of Privilege

- Principle of Separation of Privilege: a system should not grant permission based on a single condition.
  - The idea is the protection mechanism requires two keys instead of one to unlock the access.
  - This way, no single accident, deception, or breach of trust is sufficient to compromise the protected information.

Principle of Least Common Mechanism

- Principle of Least Common Mechanism: mechanisms used to access resources should not be shared.
  - Every shared mechanism represents a potential information path between users.
  - Such mechanism must be designed carefully to ensure it does not unintentionally compromise security.

Principle of Psychological Acceptability

- Principle of Psychological Acceptability: security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present.
  - Security mechanism will add extra burden, but it must be both minimal and reasonable.

What is Access Control?

- Access control is the granting or denying approval to use specific resources.

- Access control prevents unauthorized use of a resource, including the prevention of use f a resource in an unauthorized manner.

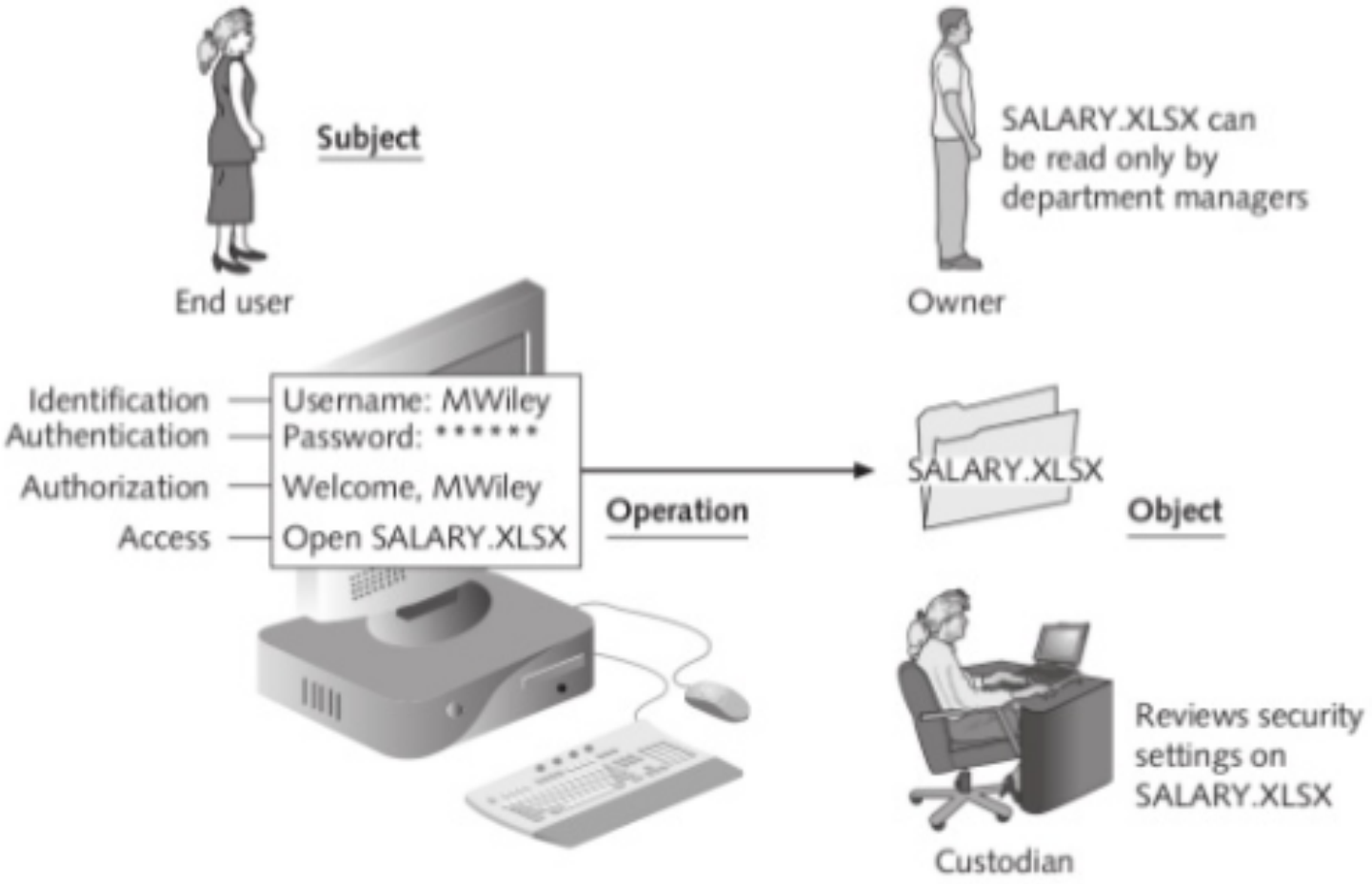
- Access control is the central element of computer security.

Terminology of Access Control

- Object:
  - An object is a specific resource, such as a file or a hardware device.
- Subject:
  - A subject is a user or a process functioning on behalf of the user that attempts to access an object.
- Operation:
  - The action that is taken by the subject over the object.
  - For example, a user (subject) may attempt to delete (operation) a file (object).

Roles in Access Control

Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that the file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End user	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX


Subject
End user
SALARY.XLSX can be read only by department managers
Owner
Identification
Authentication
Authorization
Access
Username: MWiley
Password: ******
Welcome, MWiley
Open SALARY.XLSX
Operation
SALARY.XLSX
Object
Reviews security settings on SALARY.XLSX
Custodian

Access Control Models

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role-based Access Control (RBAC)

Mandatory Access Control-I

- Mandatory access controls are specified in a system-wide security policy. They are enforced by the operating system and applied to all operations on that system. Users do not have discretion.
- MAC has two key elements:
  - Labels: each object is assigned a classification label, which represents the relative importance of the object. Subjects are assigned privilege label.
  - Levels: a hierarchy based on the labels, for both objects and subjects.

Mandatory Access Control-II

- The implementation strategy of MAC is as follows:
  - It grants permissions by matching object labels with subject labels based on their respective levels.
  - To determine if a file can be opened by a user, the object and subject labels are compared.
  - The subject must have an equal or greater level than the object in order to be granted access.
  - Subjects cannot change the labels of objects or other subjects in order to modify the security settings.

Discretionary Access Control (DAC)-I

- MAC is the most restrictive model, DAC is the least restrictive.
- With DAC, every object has an owner, who has total control over that object.
- The owner (creator) of information has the discretion to decide about and set access control restrictions on the object in question.
- The flexibility for a user to decide access is an advantage. It is also a disadvantage because users may make wrong decisions.

Discretionary Access Control (DAC)-II

- Major drawbacks of DAC:
  - DAC relies on decisions by the end user to set the proper level of security. Incorrect permissions might be granted to a subject or permissions might be given to an unauthorized subject.
  - The subject's permissions will be inherited by any programs that the subject executes. Attackers can take advantage of this inheritance as end users in the DAC model often have a high level of privileges.

Role-Based Access Control (RBAC)-I

- Rights and permissions are assigned to roles instead of individual users.

- This added layer of abstraction allows easier and more flexible administration and enforcement of access controls.

Need for Security Models

- Design and implementation of secure computer systems is challenging.

- Need to develop a method to prove, logically or mathematically, that:
  - A particular design satisfies a stated set of security requirements
  - Implementation of the design conforms to the design specifications

- Formal models are needed to verify computer security design and implementation.

Bell-LaPadula Model-Intro

- Bell-LaPadula (BLP) model was developed in 1970s by David Elliott Bell and Leonard J. LaPadula.
- It is a formal state machine model for access control, to prevent secret information from being accessed in an unauthorized manner.
- BLP model enforces the confidentiality aspects of access control.
- It is the first mathematical model of multilevel security policy to define the concept of secure modes of access and outlined rules of access.

Security Class

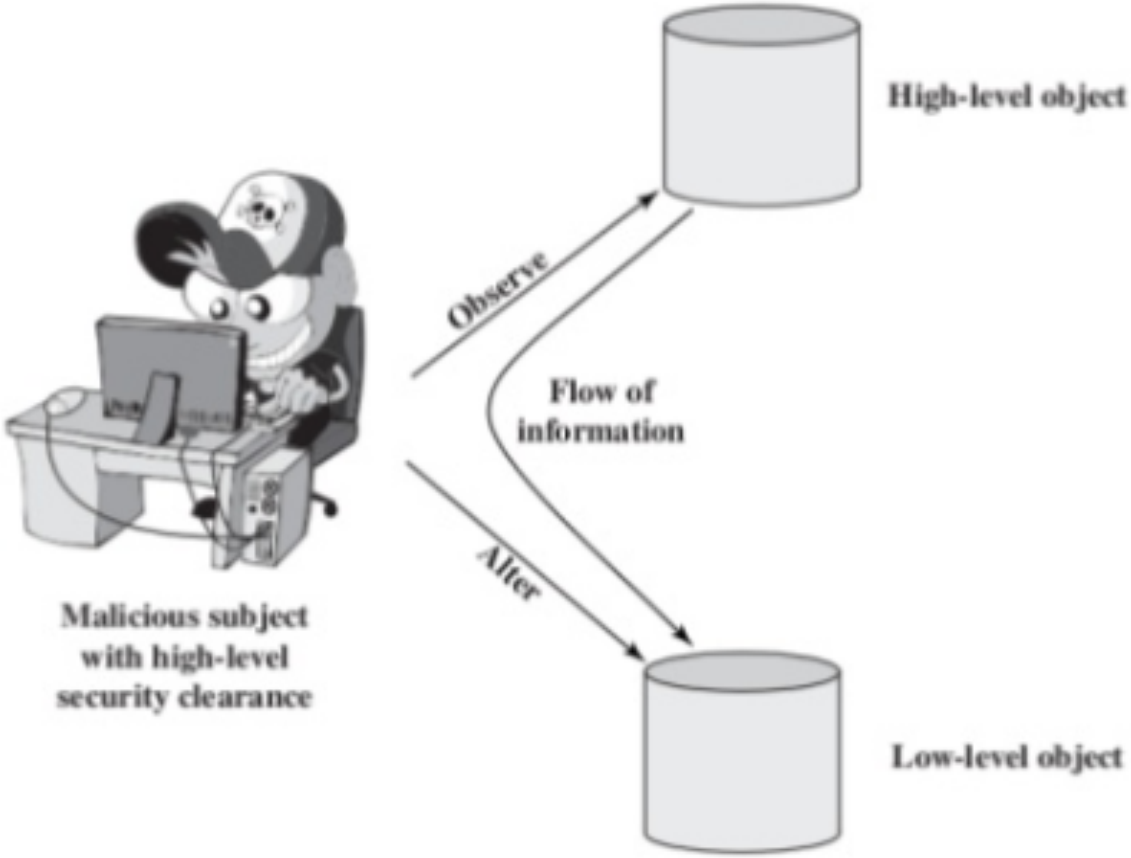
- Each subject and object is assigned a security class.
- Security classes form security level such as U.S. military classification as follows:

  Top secret > secret > confidential > restricted > unclassified

- A subject has a security clearance of a given level.
- An object has a security classification of a given level.
- The security classes control the manner by which a subject may access an object.
- Four access modes are: read, append, write, execute.

BLP Model Properties

- Simple security property (No read up)
  - A subject can only read an object of less or equal security level.
- *-property (No write down)
  - A subject in a given security level cannot write information to a lower security level.
- Discretionary security property (ds-property)
  - An individual (or role) may grant to another individual (or role) access to a document based on the owner's discretion, constrained by the MAC rule.


High-level object
Observe
Flow of information
Alter
Malicious subject with high-level security clearance
Low-level object

Biba Model

- Biba model addresses integrity, not confidentiality.
- It is concerned with unauthorized modification of data.
- Each subject and object is assigned an integrity level.
- The model consider access modes as follows:
  - Modify: to write or update information in an object
  - Observe: to read information in an object
  - Execute: to execute an object
  - Invoke: communication from one subject to another

Biba Model Rules

- *-integrity axiom
  - A subject cannot write data to an object at a higher integrity level (no write up).
  - This dictates how subjects can modify objects.
- Simple integrity axiom
  - A subject cannot read data from a lower integrity level (no read down).
  - This dictates how subjects can read objects.
- Invocation property
  - A subject cannot request service (invoke) at a higher integrity.
  - This dictates how one subject can communicate with and initialize other subjects at run time.

Clark-Wilson Integrity Model

- This model also protects integrity.
- It is a more practical model suitable for commercial operations.
- The model is based on two concepts:
  - Well-formed transactions: A user should not manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of the data.
  - Separation of duty among users: any person permitted to create or certify a well-formed transaction may not be permitted to execute it.

Clark-Wilson Model Components

- Constrained data items (CDIs)
  - Subject to strict integrity controls.
  - Can be manipulated only by TPs.
- Unconstrained data items (UDIs)
  - Unchecked data items.
  - Can be manipulated by users via primitive read and write operations.
- Integrity verification procedures (IVPs)
  - Intended to assure that all CDIs conform to some application-specific model of integrity and consistency.
- Transformation procedures (TPs)
  - System transactions that change the set of CDIs from one consistent state to another. Such as read, write, and modify.

Clark-Wilson Model

- When a system uses Clark-Wilson model:
  - It separates data into one subset that needs to be highly protected—CDI
  - And another subset that does not require a high level of protection—UDI
  - User cannot modify CDI directly.
    - Software procedures (TPs) will carry out the operation on behalf of the user.
  - UDI can be manipulated directly by the user.

Brewer Nash Model

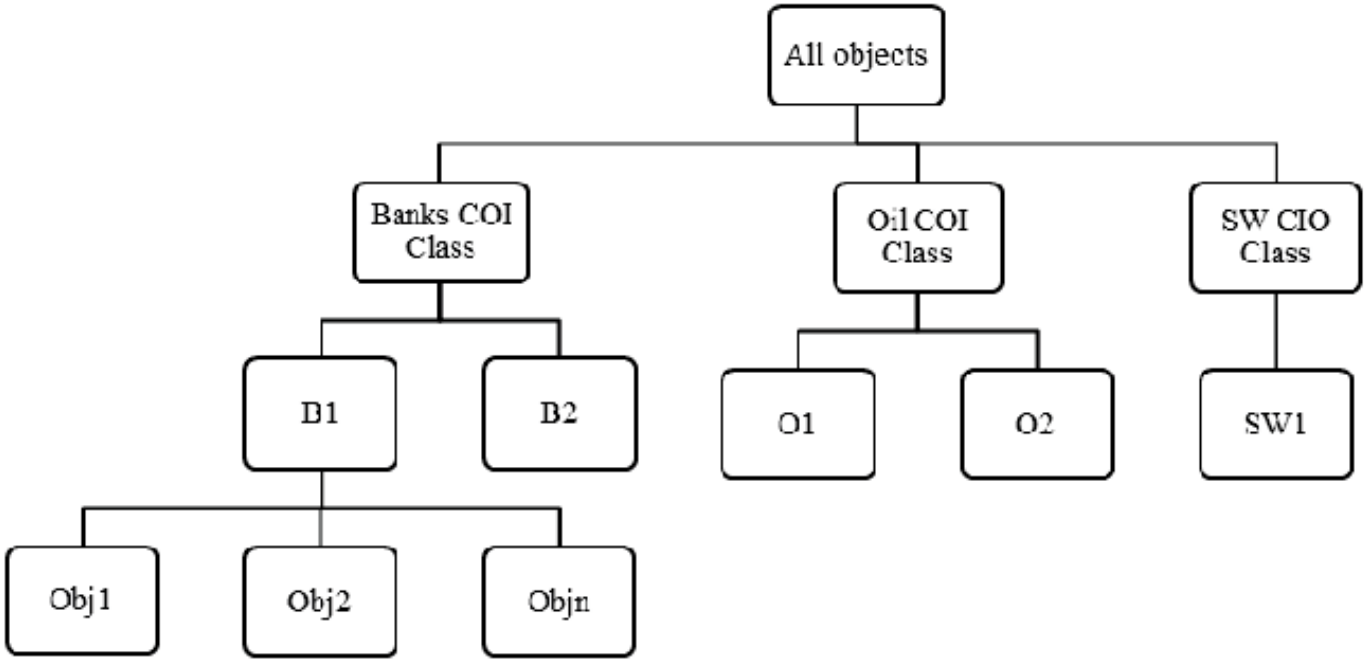
- Also known as the Chinese Wall model.
- The model was developed for commercial applications to prevent a conflict of interest.
- This model is not a multilevel security model because it does not assign security levels to subjects and objects.

Chinese Wall Model Components

- Subjects
  - Active entities including users and processes that may wish to access protected objects.
- Information: corporate information organized into a hierarchy with three levels.
  - Objects: individual items of information, each concerning a single corporation.
  - Dataset (DS): all objects that concern that same corporation.
  - Conflict of interest (CI) class: all datasets whose corporations are in competition.
- Access rules: rules for read and write access.

Chinese Wall Policy

- A subject's previous access determines access control.
  - Subjects are only allowed access to information that is not held to conflict with any other information that they already possess.
  - Once a subject accesses information from one dataset, a wall is set up to protect information in other datasets in the same CI.
  - The subject can access information on one side of the wall but not the other side.
  - When additional accesses are made in other CIs by the same subject, the shape of the wall changes to maintain the desired protection.


All objects
Banks COI Class
Oil COI Class
SW CIO Class
B1
B2
O1
O2
SW1
Obj1
Obj2
Objn