Computer Security Concepts

Overview

- News
- Key Terms
- Security Design Principles
- Fundamentals, Standards and Guidelines
- Labtainer preview
- Preview of next module

News Links

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
- https://www.justice.gov/usao-nj/pr/former-employee-national-industrial-company-arrested-attempted-data-extortion
- https://www.zaun.co.uk/zaun-data-breach-update/?ref=thestack.technology
- https://www.cisa.gov/news-events/bulletins
  - Subscribe at bottom

Key Security Concepts

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

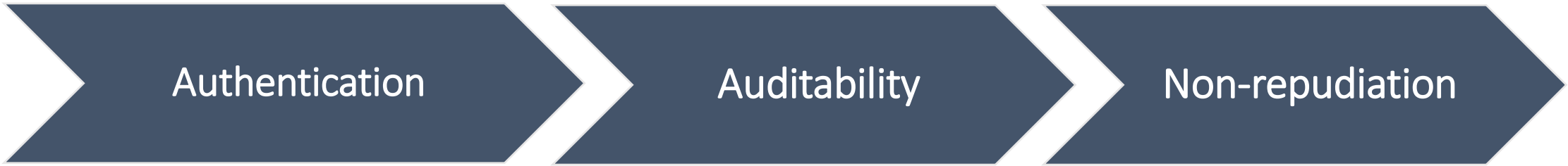
Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information

Expanded CIA



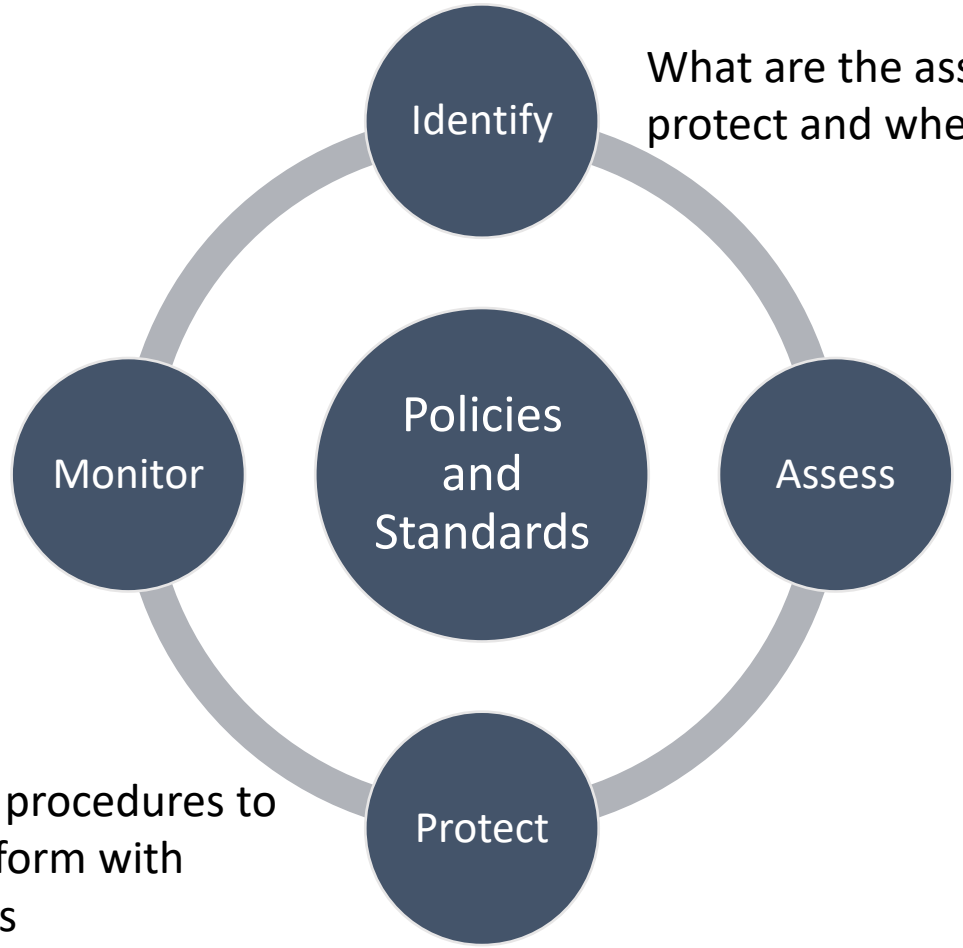
- Ensure that an individual is who they claim to be
- Or Accountability
- Ability to verify the functioning of controls
- Verify authenticated sending and receipt of messages

McCumber's Cube

- http://e-mate2.s3-website-us-east-1.amazonaws.com/cube/cube.html
- Cube Challenge First 10:
  - http://e-mate2.s3-website-us-east-1.amazonaws.com/cube_challenge/cube_challenge.html

Security Design Principles

Security Life Cycle



What are the assets you want to protect and where are they located

Consider the risk to the asset and vulnerabilities and prioritize highest risk assets

Configure systems and procedures to protect assets and conform with policies and procedures

Implement policies and tools to monitor for security incidents and comply with potential legal requirements for monitoring

Standards

Standards have been developed to cover management practices and the overall architecture of security mechanisms and services

- **National Institute of Standards and Technology (NIST)**
  - **NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation**
- **Internet Society (ISOC)**
  - **ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards**
- **International Telecommunication Union (ITU-T)**
  - **ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services**
- **International Organization for Standardization (ISO)**
  - **ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards**

Example Security Standards

- Center for Internet Security Controls
- https://www.cisecurity.org/
  - List in Canvas

Fundamental Security Design Principles

Economy of mechanism	Fail-safe defaults	Complete mediation	Open design	Separation of privilege
Least privilege	Least common mechanism	Psychological acceptability	Isolation	Encapsulation
	Modularity	Layering	Least astonishment	

Source: The National Centers of Academic Excellence in Information Assurance/Cyber Defense

Security Design Principles in Detail

- http://e-mate2.s3-website-us-east-1.amazonaws.com/cybersecurity_principles_v4/cybersecurity_principles_v4.html

One More Example

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
// Security check failed.
// Inform user that access is denied.
} else {
// Security check OK.
}
```

- **How do you fix it?**

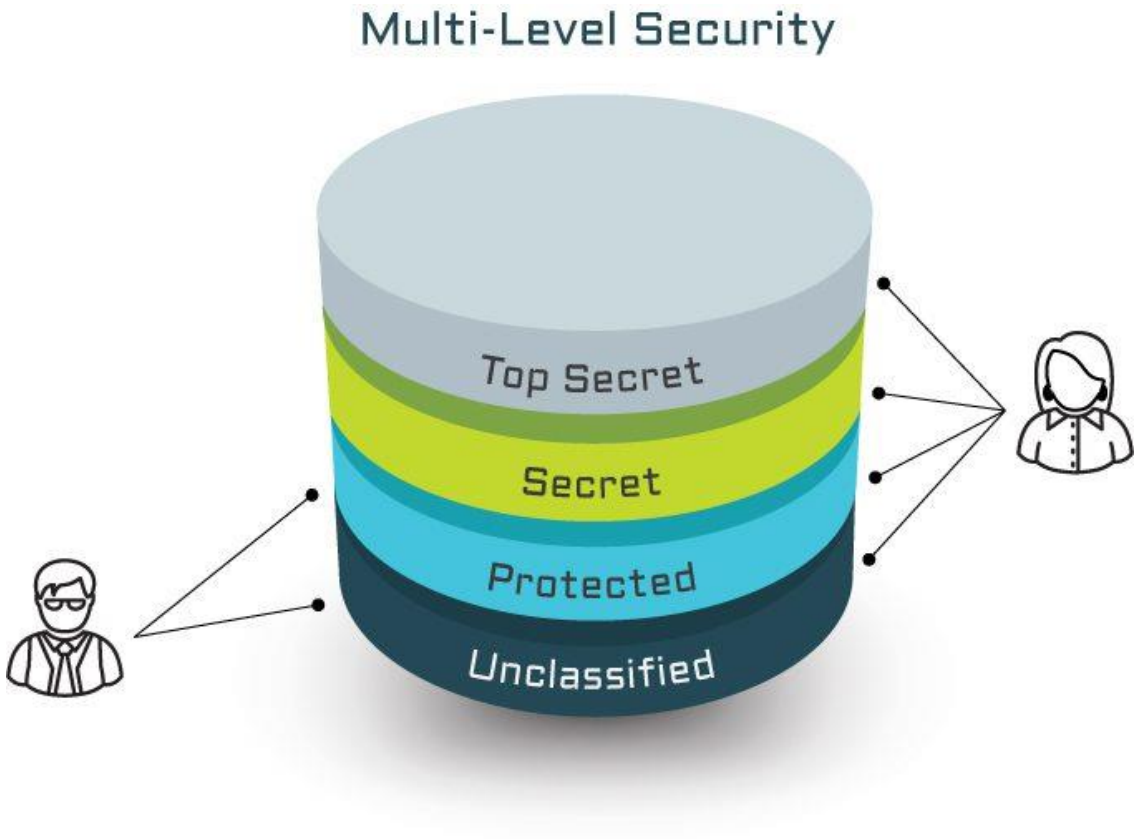
Theoretical Security Models

Overview

- Theoretical models form the basis for security implementations
- Achieving theoretically provable security is difficult
  - Even achieving functional security is difficult in large systems
- These models can be used to evaluate systems during development and production
- Different models have different objectives
  - CIA

Multi-Level Security

- no read up
  - subject can only read an object of less or equal security level
  - referred to as the *simple security property*
    - ss-property



Bell-LaPadula (BLP) Model

- AKA Multi-level Security
- formal model for access control and **Confidentiality**
- *subjects* and *objects* are assigned a security class
  - a *subject* has a *security clearance*
  - an *object* has a *security classification*
  - form a hierarchy and are referred to as security levels
    - top secret > secret > confidential > restricted >unclassified
  - security classes control the manner by which a subject may access an object

BLP Model Access Modes

- READ
  - the subject is allowed only read access to the object
- APPEND
  - the subject is allowed only write access to the object
- WRITE
  - the subject is allowed both read and write access to the object
- EXECUTE
  - the subject is allowed neither read nor write access to the object but may invoke the object for execution

BLP Summary

- **No Read Up**
  - subject can only read an object of less or equal security level
  - referred to as the *simple security property*
    - ss-property
- **No Write Down**
  - a subject can only write into an object of greater or equal security level
  - referred to as the *-property

Covert Channels

A covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

- What condition could exist if a user was allowed roles at two different security levels in the BLP model?

SS Property - Database Inference Problems

DBMS enforces simple security rule (no read up)

- easy if granularity is entire database or at table level
- inference problems if have column granularity or row
  - if a person can query on restricted data they can infer its existence
    - SELECT Ename FROM Employee WHERE Salary > 250
  - solution is to check access to all query data
- Inference creates a covert channel

Name	FName	City	Age	Salary
Smith	John	3	35	$280
Doe	Jane	1	28	$325
Brown	Scott	3	41	$265
Howard	Shemp	4	48	$359
Taylor	Tom	2	22	$250

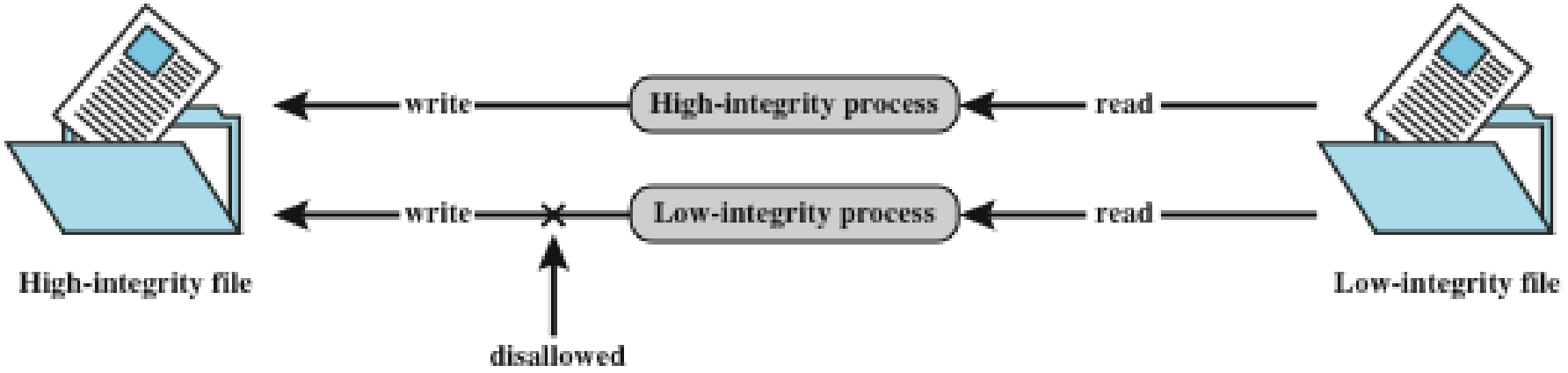
*-security rule Database Inference

- enforce *-security rule (no write down)
- problem if a low clearance user wants to insert or update a row with a primary key that already exists in a higher level row:
  - can reject, but user knows row exists - **inference**
  - can replace, compromises data integrity
- Solutions:
  - use database/table granularity
  - **polyinstantiation** and insert multiple rows with same key
    - creates other problems with conflicting entries

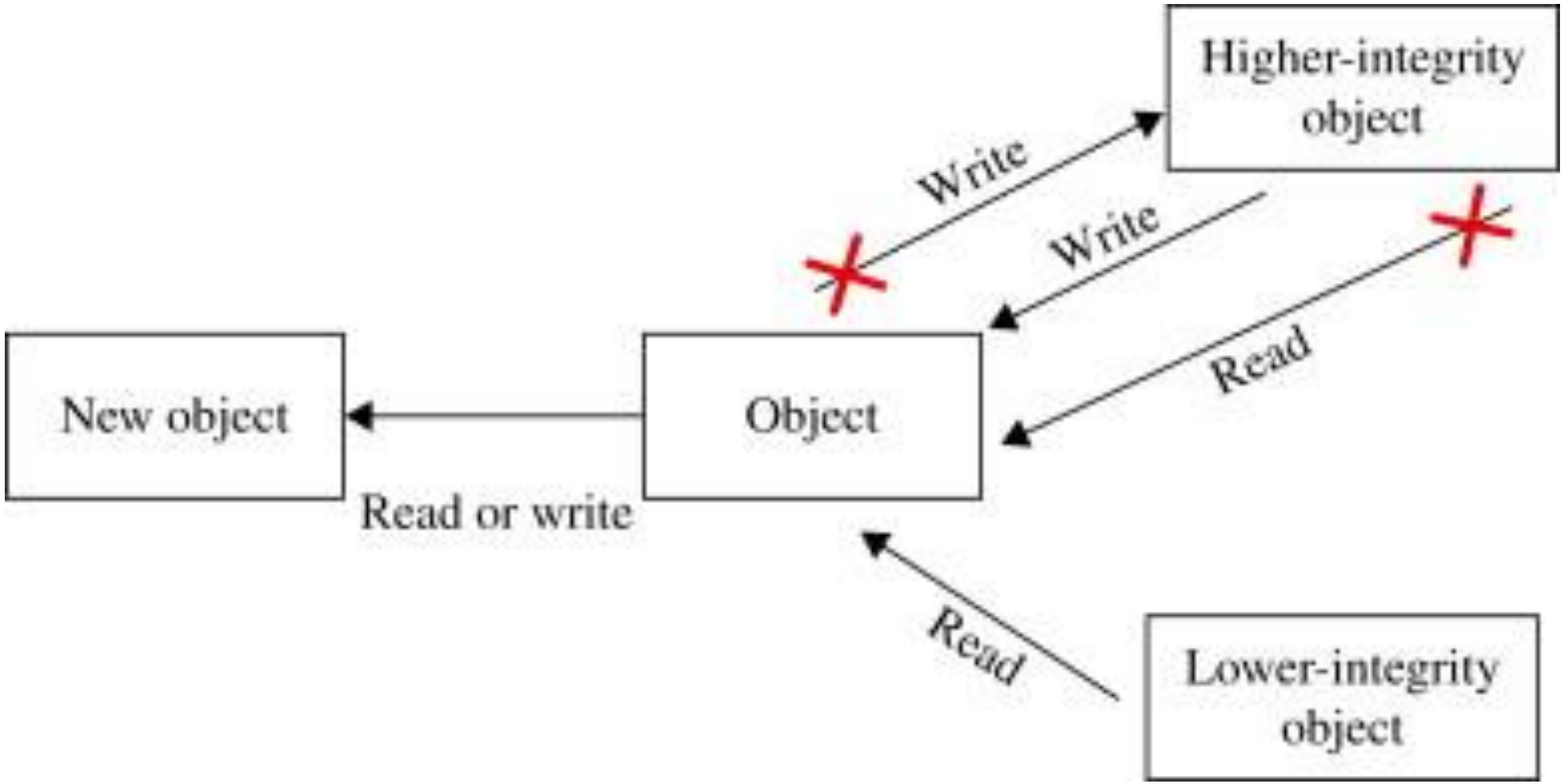
Name	FName	City	Age	Salary
Smith	John	3	35	$280
Doe	Jane	1	28	$325
Brown	Scott	3	41	$265
Howard	Shemp	4	48	$359
Taylor	Tom	2	22	$250

Biba Integrity Model

- Strict integrity policy
  - **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
- No Write UP, No Read DOWN



Biba Integrity Model



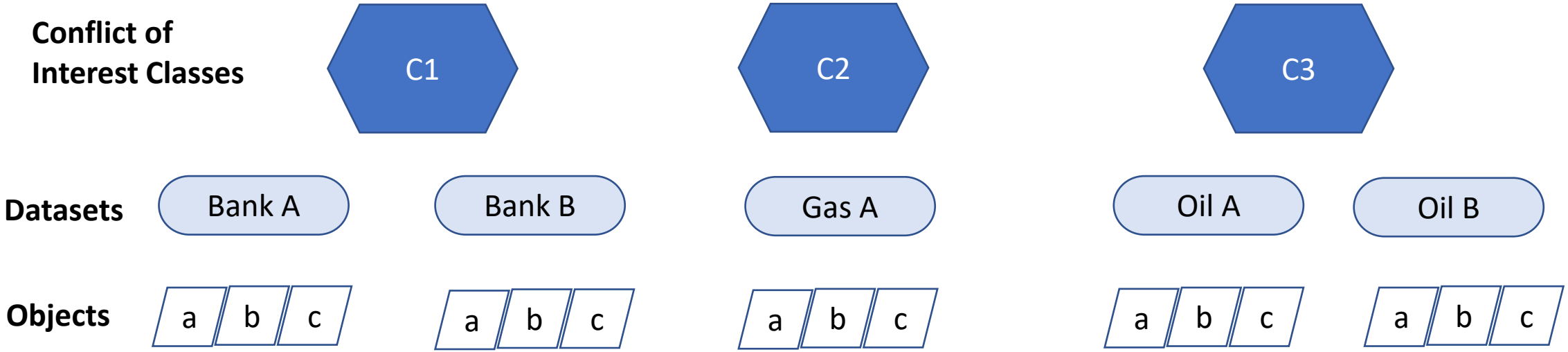
Clark-Wilson Integrity Model

- Closely models commercial operations
- Enforces separation of duties
- Uses transactions as a basis for rules
  - Two levels of integrity
    - Constrained data items (CDIs) are subject to integrity controls
    - Unconstrained data items (UDIs) are not subject to integrity controls
  - Two types of processes
    - The first are integrity verification processes (IVPs)
    - The second are transformation processes (TPs)

Brewer-Nash (Chinese Wall) Model

- Integrity, confidentiality **conflict of interest**
- Uses both discretionary and mandatory access
  - **Subjects**: Active entities that may wish to access protected objects
  - **Information**: Information organized into a hierarchy
    - **Objects**: Individual items of information, each concerning a single corporation
    - **Dataset** (DS): All objects that concern the same corporation
    - **Conflict of interest** (CI) **class**: All datasets whose corporations are in competition
  - **Access rules**: Rules for read and write access

Brewer-Nash Model Example



Operational Security Models

Fortress Model

- Keep the bad out, allow in the good
  - This was a natural model: build a series of defenses and your system can be secure
- Endpoint security
  - A new version of the fortress model
  - Involves securing of all endpoints in a network so they are secured from all threats

The Operational Model of Computer Security

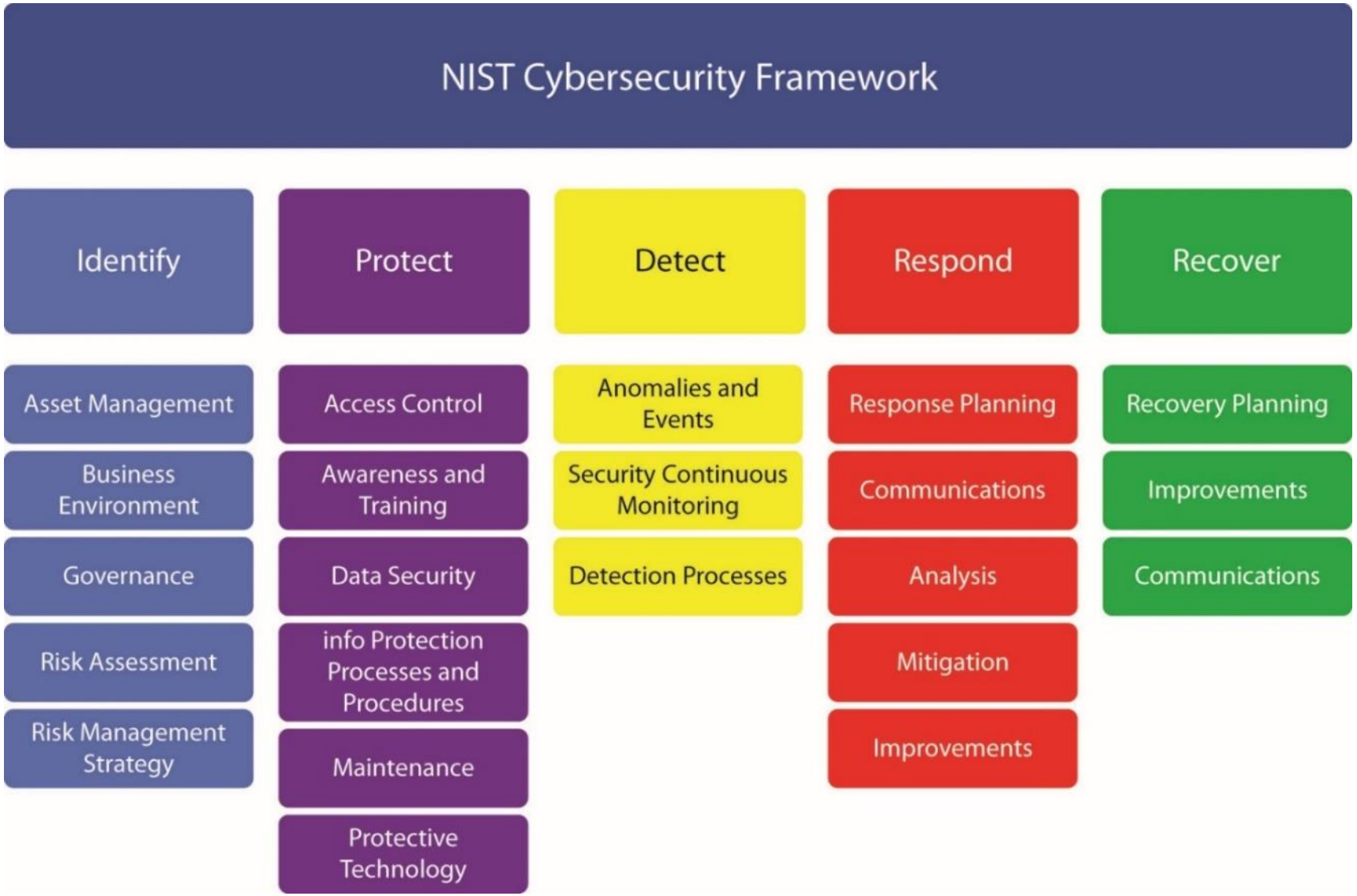
- Prevention was the focus of security for many years
  - Protection was equated with prevention
  - Somebody always seems to find a way around safeguards
- Operational model of computer security
  - One security equation is:
    Protection = Prevention + (Detection + Response)
    - Every security technique and technology falls into at least one of the three elements of the equation

Time-Based Security

- Time-based security allows us to understand the relationship between prevention, detection, and response
  - The amount of time offered by a protection device, P_t, should be greater than the time it takes to detect the attack, D_t, plus the reaction time of the organization, R_t:
    - $P_t > D_t + R_t$

Cybersecurity Framework Model

- *Framework for Improving Critical Infrastructure Cybersecurity*
  - Common taxonomy and mechanism to assist in aligning management practices with existing standards, guidelines, and practices
  - Complements and enhances risk management efforts
  - Core functions: identify, protect, detect, respond, and recover
  - Tiers represent the organization's ability, from Partial (Tier 1) to Adaptive (Tier 4)


NIST Cybersecurity Framework
Identify
Protect
Detect
Respond
Recover
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Access Control
Awareness and Training
Data Security
info Protection Processes and Procedures
Maintenance
Protective Technology
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Response Planning
Communications
Analysis
Mitigation
Improvements
Recovery Planning
Improvements
Communications

Active Defense Model

- The actual hunting of intruders inside the enterprise
  - This model capitalizes on elements of both the operational model and time-based security models
  - Built around the actions necessary to actively seek out attackers that make it past the defenses
  - Active hunters use their knowledge of baseline conditions for the systems and search for things that are abnormal

McCumber's Cube Last 10

Labtainer

- Select the file C:\tmp\Labtainer\Labtainer.ova
- Name the machine CS450, and use the provided storage path

For a copy on your personal machine, download the appropriate appliance here: https://nps.edu/web/c3o/virtual-machine-images

Assignments

- Assignment 2 Labtainer nix-commands
- Read Module 3 Chapter
- Create a disposable gmail account and **keep a record of the account name and password.** Consider violating a security rule and using the same password for all class-specific logins

NSA Codebreaker Challenge

- https://nsa-codebreaker.org/home

NSA Summer Internships

- UNR is an NSA partner institution
- Applications are NOW for next summer (Sept. 1 – Oct. 1)
- https://www.intelligencecareers.gov/NSA/students-and-internships