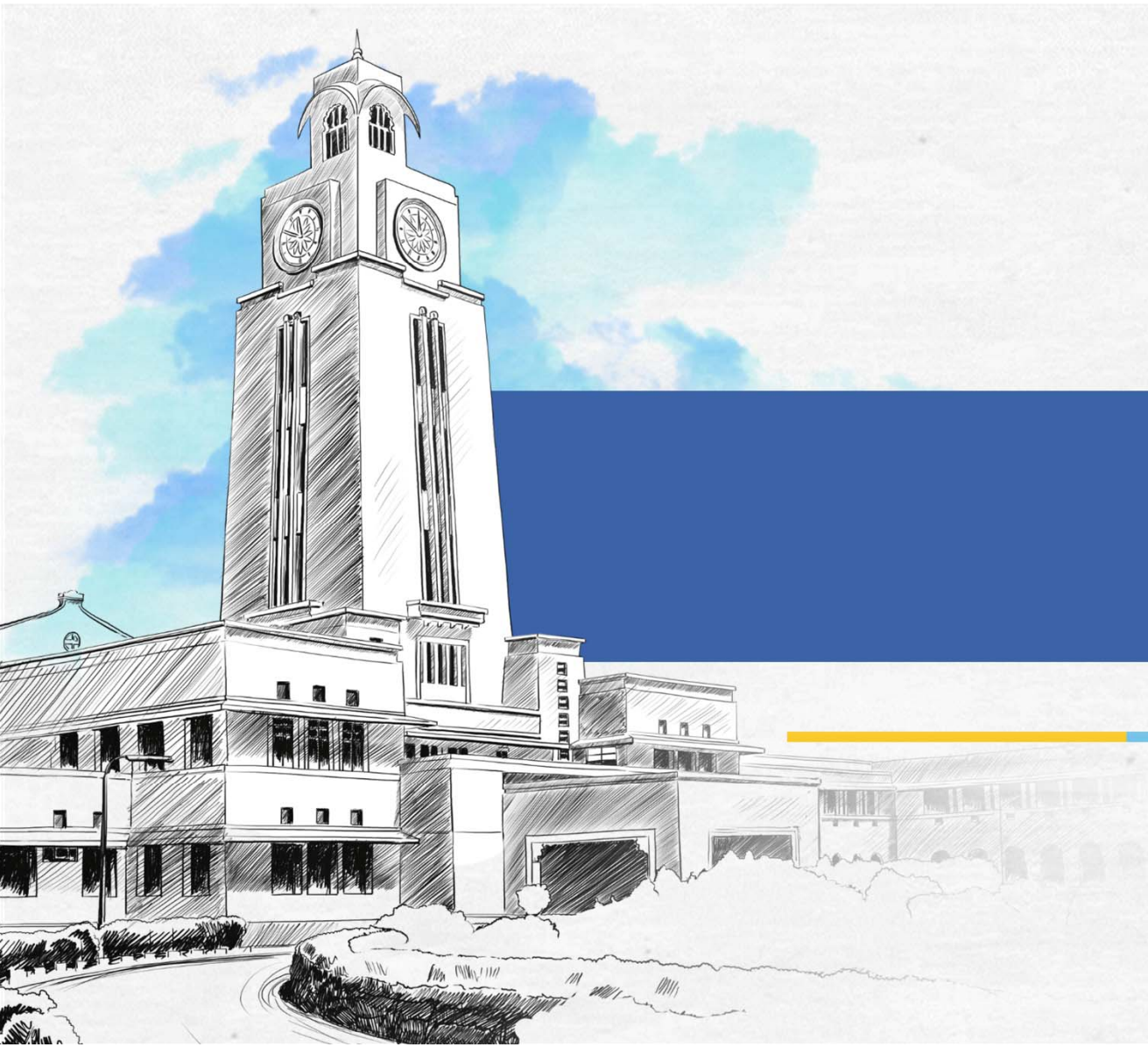


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Security - Introduction

innovate achieve lead

Agenda

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy
- Standards

Security Functional Requirements

Security Functional Requirements

innovate achieve lead

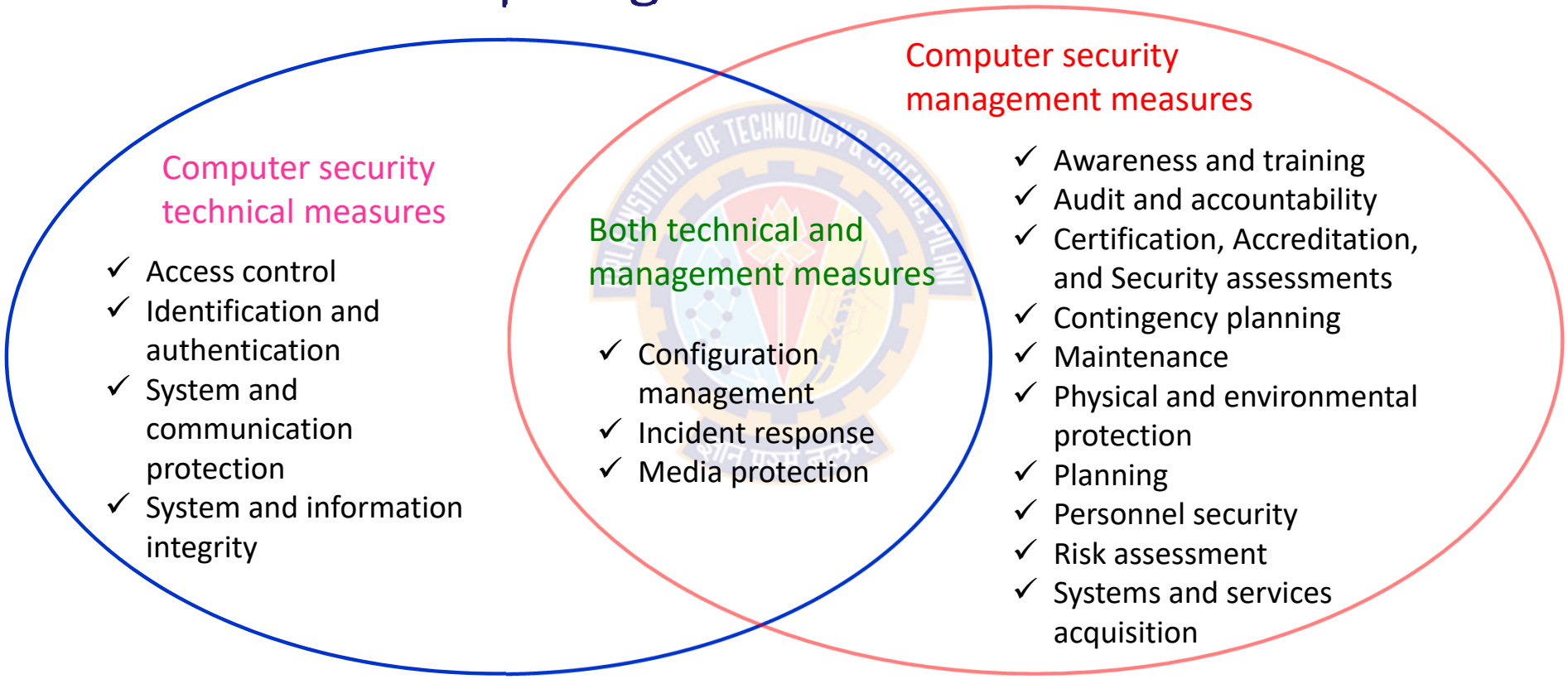
Classifying & Characterizing Countermeasures

- Countermeasures are viewed in terms of functional requirements
- FIPS pub 200 talks about:
  - the Minimum Security Requirements for Federal Information and Information Systems
- FIPS 200 enumerates 17 security areas with regard to protecting the CIA of
  - the information systems and
  - the information processed, stored, and transmitted by those systems
- The requirements in FIPS 200 can be divided into two categories:
  - Those that require computer security technical measure
  - Those that require management measure
- https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Security Functional Requirements

innovate achieve lead

Functional Areas Requiring...



Security Functional Requirements

innovate achieve lead

Functional areas involving technical measures

- Identification and Authentication
  - Identify the IS users, processes acting on behalf of users, other ISs and devices, and authenticate (or verify) their identities as a prerequisite to allowing access to OISs
- System and Communication Protection
  - Monitor, control, and protect OCs (i.e., information transmitted or received by OISs) at the external boundaries and key internal boundaries of the ISs; and
  - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within OISs

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Security Functional Requirements

innovate achieve lead

Functional areas involving technical measures

- Access Control
  - Limit IS access to:
    - authorized users, processes acting on behalf of authorized users, other ISs and devices, and to the transactions and functions that authorized users are permitted to exercise
- System and Information Integrity
  - Identify, report, and correct the flaws in information and ISs in a timely manner;
  - Provide protection from malicious code at appropriate locations within OISs; and
  - Monitor IS security alerts and advisories and take appropriate actions in response.

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Security Functional Requirements

innovate achieve lead

Functional areas involving managerial measures

- Awareness and training
  - (i) Ensure that managers and users of OISs are aware of the
    - security risks associated with their activities
    - applicable laws, regulation, and policies related to the security of OISs
  - (ii) Ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- Audit and accountability
  - (i) Create, protect, and retain IS audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate IS activity
  - (ii) Ensure that the actions of individual IS users can be uniquely traced to those users so they can be held accountable for their actions.

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Security Functional Requirements

innovate achieve lead

Functional areas involving managerial measures

- Certification, Accreditation, and Security assessments
  - (i) Periodically assess the security controls in OISs to determine if the controls are effective in their application;
  - (ii) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in OISs
  - (iii) Authorize the operation of OISs and any associated IS connections
  - (iv) Monitor IS security controls on an ongoing basis to ensure the continued effectiveness of the controls
- Contingency planning
  - Establish, maintain, and implement plans for emergency response, backup operations, and post-disaster recovery for OISs to ensure the availability of critical information resources and continuity of operations

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Security Functional Requirements

innovate achieve lead

Functional areas involving managerial measures

- Maintenance
  - Perform periodic and timely maintenance on OISs
  - Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance
- Physical and environmental protection
  - Limit physical access to ISs, equipment, and the respective operating environments to authorized individuals
  - Protect the physical plant and support infrastructure for ISs
  - Provide supporting utilities for ISs
  - Protect ISs against environmental hazards
  - Provide appropriate environmental controls in facilities containing ISs

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Security Functional Requirements

innovate achieve lead

Functional areas involving managerial measures

- Planning
  - Develop, document, periodically update, and implement security plans for OISs
  - These plans should describe the security controls in place or planned for the ISs and the rules of behavior for individuals accessing the ISs
- Personnel security
  - Ensure that organizational personnel (including third-party service providers) are trustworthy and meet established security criteria for their positions
  - Ensure that organizational information and ISs are protected during and after personnel actions such as terminations and transfers
  - Employ formal sanctions for personnel failing to comply with organizational security policies and procedures

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Security Functional Requirements

innovate achieve lead

Functional areas involving managerial measures

- Risk assessment
  - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of OISs and the associated processing, storage, or transmission of organizational information.
- Systems and services acquisition
  - Allocate sufficient resources to adequately protect OISs
  - Employ system development life cycle processes that incorporate information security considerations
  - Employ software usage and installation restrictions
  - Ensure that third party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Security Functional Requirements

innovate achieve lead

Functional areas that overlap both

- Configuration management
  - Establish and maintain baseline configurations and inventories of OISs (including hardware, software, firmware, and documentation) throughout the respective system development life cycles
  - Establish and enforce security configuration settings for IT products employed in OISs
- Incident response
  - Establish an operational incident-handling capability for OISs that includes adequate preparation, detection, analysis, containment, recovery, and user-response activities
  - Track, document, and report incidents to appropriate organizational officials and/or authorities
- Media protection
  - Protect IS media, both paper and digital
  - Limit access to information on IS media to authorized users
  - Sanitize or destroy IS media before disposal or release for reuse.

OIS = Organizational Information Systems; IS = Information System; OC = Organizational Communication

Fundamental Security Design Principles

Security Design Principles

Scenario – Ordering Pizza

Caller	Google
Is this Pizza Delight?	No sir, it's Google Pizza
I must have dialed a wrong number. Sorry	No sir, Google bought Pizza Delight last month
OK. I would like to order a pizza.	Do you want your usual, sir?
My usual? You know me?	According to our caller ID data sheet, the last 12 times you called, you ordered an extra-large pizza with three cheeses, sausage, pepperoni, mushrooms and meatballs on a thick crust.
OK! That's what I want ...	May I suggest that this time you order a pizza with ricotta, arugula, sun-dried tomatoes and olives on a whole wheat gluten-free thin crust?
What? I detest vegetable!	Your cholesterol is not good, sir.
How the hell do you know!	Well, we cross-referenced your home phone number with your medical records. We have the result of your blood tests for the last 7 years.
Okay, but I do not want your rotten vegetable pizza! I already take medication for my cholesterol.	Excuse me sir, but you have not taken your medication regularly. According to our database, you purchased only a box of 30 cholesterol tablets once, at Drug RX Network, 4 months ago.

Security Design Principles

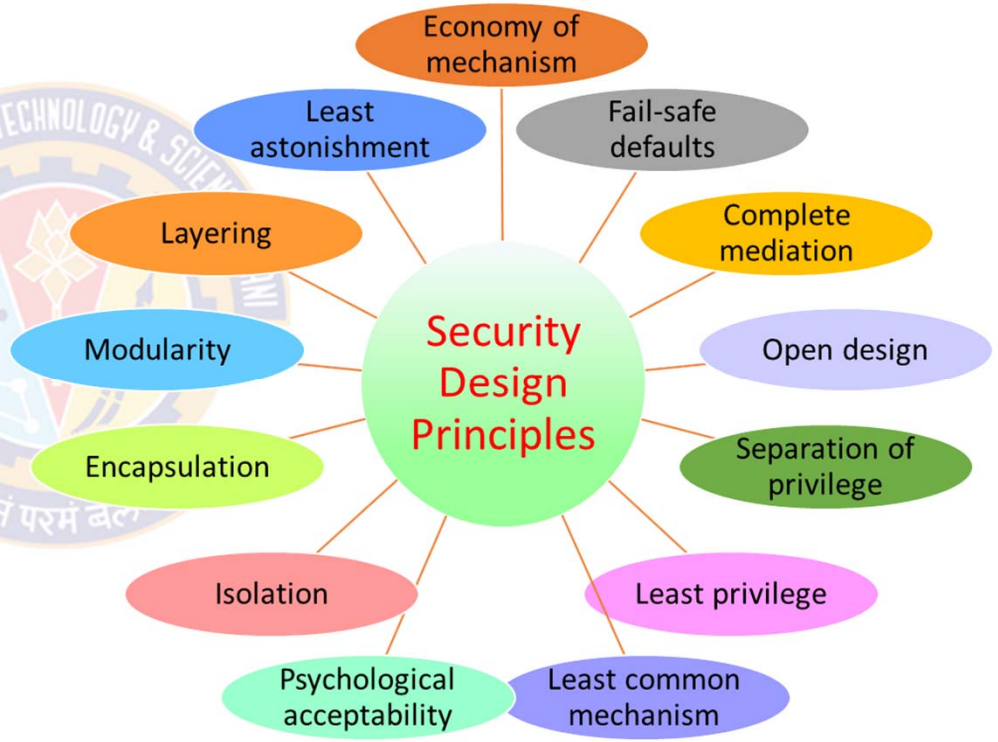
Scenario – Ordering Pizza

Caller	Google
I bought more from another drugstore.	That doesn't show on your credit card statement.
I paid in cash.	But you did not withdraw enough cash according to your bank statement.
I have other sources of cash.	That doesn't show on your last tax return unless you bought them using an undeclared income source, which is against the law.
WHAT THE HELL!	I'm sorry, sir, we use such information only with the sole intention of helping you.
Enough already! I'm sick to death of Google, Facebook, Twitter, WhatsApp and all the others. I'm going to an island without internet, cable TV, where there is no cell phone service and no one to watch me or spy on me.	I understand sir, but you need to renew your passport first. It expired 6 weeks ago...

Security Design Principles

Design Principles from NCAE in IA/CD

- NCAE in IA/CD lists the following principles
- Security design principles are meant to guide the development of protection mechanisms



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

Security Design Principles

Economy of Mechanism

- EoM means that the design of software and hardware security measures should be as simple and small as possible
- This is the most difficult principle to honor because there is a constant demand for new features in both hardware and software
- The best that can be done is to keep this principle in mind during system design to try to eliminate unnecessary complexity

Simple and Small Design	Complex Design
Simple mechanisms tend to have fewer exploitable flaws and require less maintenance	More likely to possess exploitable flaws
Makes it easier to test and verify thoroughly	Adversaries may discover and exploit subtle weaknesses that are difficult to spot ahead of time
Configuration management issues are simplified	Configuration management issues become more complex
Updating or replacing a simple mechanism becomes a less intensive process	Updating or replacing a complex mechanism becomes more intensive process

Security Design Principles

innovate achieve lead

Fail-safe Default

- Means that access decisions should be based on permission rather than exclusion
- That is, by default no access to all, and the access is permitted based on the requirement
  - E.g., most file access systems, and virtually all protected services on client/server systems work on this principle

Default is lack of access	Default is permit access
Involves explicitly giving permission	Involves explicitly excluding access
Exhibits better failure mode than the default permit access approach	Exhibits poor failure mode than the default lack of access
Implementation mistake (giving explicit permission) only results in refusing permission, which is a safe situation and can be quickly detected	Implementation mistake (explicitly excluding access) results in allowing access, which is an unsafe situation and can long go unnoticed

Security Design Principles

Complete Mediation

- It means that every access must be checked against the access control mechanism rather than access decisions retrieved from a cache
- For example:
  - File access systems complies with this principle
  - However, typically, once a user has opened a file, no check is made to see of permissions change
- In a system designed to operate continuously, this principle requires that, if access decisions are remembered for future use, careful consideration be given to how changes in authority are propagated into such local memories
- To fully implement complete mediation, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control
- This resource-intensive approach is rarely used

Security Design Principles

Open Design

- It means that the design of a security mechanism should be open rather than secret
- For example:
  - although encryption keys must be secret, encryption algorithms should be open to public scrutiny
- The algorithms should be reviewed by many experts so that users can have high confidence in them
- This is the philosophy behind the NIST program of standardizing encryption and hash algorithms
  - That's why there is a widespread adoption of NIST-approved algorithms

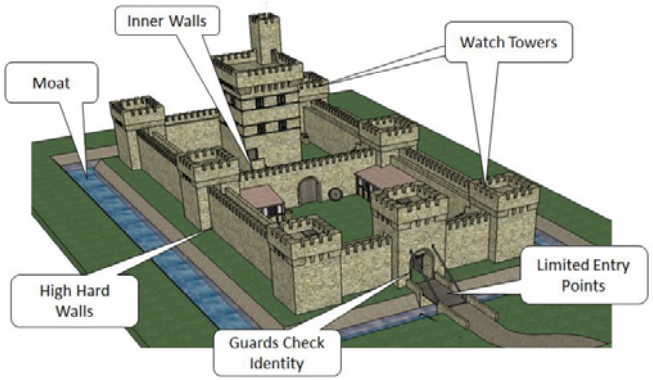
NIST = National Institute of Standards and Technology

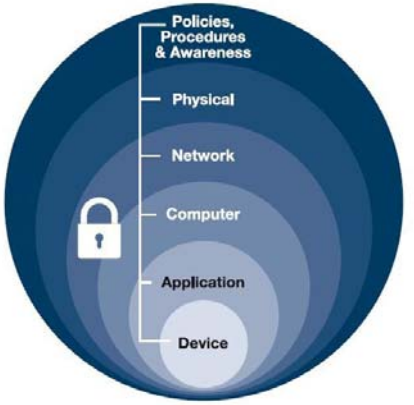
Security Design Principles

innovate achieve lead

Separation of Privilege

- Also known as defense in depth
  - Requires multiple privilege actions to achieve access to a restricted resource
- The principle states that a system should not grant permission based on a single condition
- This principle is equivalent to the separation of duty principle. For example:
  - Company checks for more than $100,000 must be signed by two officers of the company
  - If either does not sign, the check is not valid
    - The two conditions are the signatures of both officers



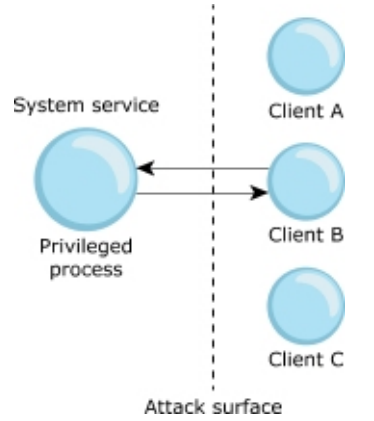


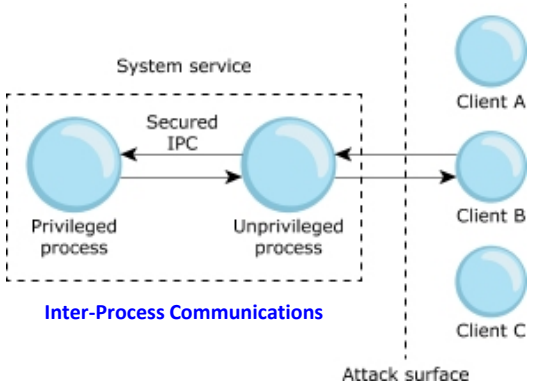
Security Design Principles

innovate achieve lead

Separation of Privilege

- In a software context, a program is divided into multiple parts
- Each part has limited privileges it requires in order to perform a specific task
- For example, the computer program forks into two processes:
  - The main program drops privileges, and the smaller program keeps privileges in order to perform a certain task
  - The two halves then communicate via a socket pair.





http://www.qnx.com/developers/docs/qnxcar2/index.jsp?topic=%2Fcom.qnx.doc.neutrino.prog%2Ftopic%2Fprocess_Privilege_separation.html

Security Design Principles

Least Privilege

- A subject (a user, application, or process) should have only the minimum necessary privileges to perform its task, with no additional permissions.
- Example: Role-based privileges
  - The system security policy identifies and defines various roles of users or processes
  - Each role is assigned only those permissions needed to perform its functions.
- Each permission specifies certain access to a particular resource:
  - E.g., users may have access to the files on their workstations and a select set of files on a file server, but no access to data that is held within the database
  - E.g., read and write access to a specified file or directory, and connect access to a given host and port
- Temporal aspect to the least privilege principle
  - E.g., individuals who have special privileges should have those privileges only for the specific purpose.
  - When they are doing ordinary activities the privileges should be withdrawn.

Security Design Principles

Least Common Mechanism

- This principle states that mechanisms used to access resources should not be shared
- For example:
  - A program that enables employees to check their payroll information (read) should be separate from a program that modifies the information (write)
- Covert channels
  - Covert channel attack creates capability to transfer information between processes that are not supposed to be communicating by the computer security policy.
- Sharing resources provides a channel along which information can be transmitted, and so such sharing should be minimized
- Solutions using isolation:
  - Virtual machines
  - Sandboxes

Least Common Mechanism - Example

- Example
  - A website provides e-commerce services for a major company.
  - Attackers try to deprive the company of the revenue it obtains from that website
  - They flood the site with messages and tie up the e-commerce services
    - Legitimate customers are unable to access the website and, as a result, take their business elsewhere.
- Explanation
  - Here, the sharing of the Internet with the attackers' sites caused the attack to succeed
  - The appropriate countermeasure would be to restrict the attackers' access to the segment of the Internet connected to the website
  - Techniques for doing this include proxy servers or traffic throttling
    - Throttling is concerned with limiting traffic coming from legitimate visitors as opposed to dealing with denial-of-service attacks

Security Design Principles

innovate achieve lead

Psychological Acceptability

- Security mechanisms should not add to the difficulty of accessing a resource
  - Simultaneously should meet the needs of those who authorize access
  - E.g., requesting hair samples from the users who have gone completely bald (lost hair) in order to comply with a biometric authentication mechanism
- If security mechanisms hinder the usability or accessibility of resources, users will look for ways to defeat those mechanisms
  - Users write down passwords which are too difficult to remember
  - Authentication for Remote Logins (rlogin): .rhosts mechanism bypasses password security check
    - The .rhosts file contains a list of hosts and user names that determines who can log in to a system remotely without a password.
    - if you set up the /etc/hosts.equiv or .rhosts file, you are not asked for a password, because the network already knows who you are

Security Design Principles

Isolation

- This principle applies in three contexts
- Restricting public access to critical resources
  - The system that has critical data, processes, or resources must be isolated such that it restricts public access:
    - Physical isolation:
      - The system with critical information is physically isolated from the system with public access information.
    - Logical isolation:
      - Security services layers are established between the public system and the critical systems.
- Files or data of one user must be kept isolated with the files or data of another user
  - New operating systems have this functionality.
  - Each user operating the system have an isolated memory space, process space, file space along with the mechanism to prevent unwanted access.
- The security mechanisms themselves must be isolated such that they are prevented from unwanted access.
  - E.g., isolating cryptographic software from other parts of the host system so that the software is protected from tampering


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!