



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Security Architecture: Policies, Models and Mechanisms

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

Security Architecture: Policies, Models and Mechanisms



Agenda

- Introduction to security policies, models and mechanisms
- The Nature of Security Policies
- Types of Security Policies
- The Role of Trust
- Types of Access Control
- Policy Languages
- The CIA Classification:
 - Confidentiality Policies:
 - Integrity Policies:
 - Availability Policies:





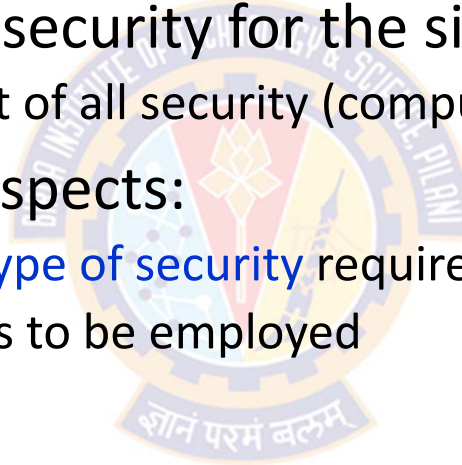
Assumptions and Trust

Assumptions and Trust



Overview

- How do we determine whether a policy correctly describes the required level and type of security for the site?
 - This question lies at the heart of all security (computer and non-computer)
- The answer rests on two aspects:
 - **assumptions** specific to the **type of security** required and
 - the **environment** in which it is to be employed



Assumptions and Trust



Example – Opening a Door Lock Scenario

- Opening a door lock requires a key
- The **assumption** is that the **lock is secure against lock picking**
- This assumption is treated as an **axiom** and is made because most people would require a key to open a door lock
 - Axiom: a statement accepted as true as the basis for argument or inference
- A good lock picker, however, can open a lock without a key
- Hence, in an environment with a **skilled, untrustworthy** lock picker, the **assumption is wrong** and the conclusion invalid

Assumptions and Trust



Example – Opening a Door Lock Scenario

- If the lock picker is **trustworthy**, then the assumption is still valid
- The term "**trustworthy**" implies that the lock picker will not pick a lock unless the owner of the lock **authorizes** the lock picking
 - This is an example of the role of "**trust**"
- An **exception** to the rule provides a "**back door**" through which the security mechanism (the locks) can be bypassed
- The trust resides in the belief that this **back door will not be used except as specified by the policy**
 - If used, then the **trust has been breached** and the security mechanism (the lock) provides no security

Assumptions and Trust



Assumptions

- A policy consists of a **set of axioms** that the policy makers **believe** can be enforced
- Designers of policies make two assumptions:
 - 1) The policy **correctly** and **unambiguously** partitions the set of system states into "**secure**" and "**non-secure**" states
 - This assumption asserts that the policy is a **correct description** of what constitutes a "**secure**" system
 - 2) The security mechanisms prevent the system from entering a "**non-secure**" state
 - This assumption says that the security policy **can be enforced** by security mechanisms
- If either assumption is erroneous, the system will be non-secure

Assumptions and Trust



Assumption-1 - Example

- *The policy is a correct description of what constitutes a "secure" system*
- A bank's policy may state that officers of the bank are authorized to shift money among accounts
- If a bank officer puts \$100,000 in his account, has the bank's security been violated?
 - Answer is NO, as per policy statement, because the officer was authorized to move the money
 - In the "real world," that action would constitute embezzlement, something any bank would consider a security violation

Assumptions and Trust



Assumption-2 - Example

- *The security policy can be enforced by security mechanisms*
- These mechanisms can be categorized as either **secure**, **precise**, or **broad**
- Let P be the set of all possible states (secure and non-secure)
- Let S be the set of secure states (as specified by the security policy)
- Let the security mechanisms restrict the system to some set of states R (where, $R \subseteq P$)
- Now, we can say that a security mechanism is considered:
 - **secure** if $R \subseteq S$;
 - **precise** if $R = S$; and
 - **broad** if there are states r such that $r \in R$ and $r \notin S$

Assumptions and Trust



Assumptions

- Ideally, the union of all security mechanisms active on a system would produce a single precise mechanism (that is, $R = S$)
- However, in practice, security mechanisms are broad; they allow the system to enter non-secure states
- Trusting that mechanisms work requires several assumptions:
 - Each mechanism is designed to implement one or more parts of the security policy
 - The union of the mechanisms implements all aspects of the security policy
 - The mechanisms are tamperproof
 - The mechanisms are implemented, installed, and administered correctly



Thank You!