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

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:

Policies, Models, & Mechanism

Policies, Models, & Mechanism

innovate achieve lead

Security Policy

- A security policy is a statement of what is, and what is not, allowed
- A security policy
  - defines main security objectives
  - defines the scope of security needed by the organization
  - discusses the assets that require protection
  - identifies the major functional areas of data processing
  - defines all relevant terminology
  - acts as a strategic plan for implementing security
  - discusses the importance of security to every aspect of daily business operation
  - discusses the importance of senior management support for the implementation of security

Policies, Models, & Mechanism

Security Policy

- A security policy
  - serves as a proof that senior management has exercised due care in protecting the organization against intrusion, attack, and disaster
  - is used to
    - define roles
    - assign responsibilities
    - specify audit requirements
    - outline enforcement processes
    - indicate compliance requirements, and
    - define acceptable risk levels

Policies, Models, & Mechanism

Security Mechanism

- A security mechanism is a method, tool, or procedure for enforcing a security policy
- Mechanisms can be nontechnical
  - E.g., requiring proof of identity before entering a building
- Security policies often require some procedural mechanisms that technology cannot enforce
- Example
  - Suppose a university's computer science laboratory has a policy that prohibits any student from copying another student's homework files. The computer system provides mechanisms for preventing others from reading a user's files. Anna fails to use these mechanisms to protect her homework files, and Bill copies them. Here, a breach of security has occurred, because Bill has violated the security policy. However, Anna's failure to protect her files does not authorize Bill to copy them

Policies, Models, & Mechanism

Security Policy

- Policies may be presented as a list of allowed (secure) and disallowed (non-secure) states
- For our purposes, we will assume that any given policy provides an axiomatic description of secure states and non-secure states
  - axiomatic = self-evident, unquestionable
- However, in practice, policies are rarely so precise
  - They normally describe in English, what users and staff are allowed to do
- The ambiguity inherent in such a description leads to states that are not classified as "allowed" or "disallowed"
- For example, consider the homework policy discussed previously:
  - If someone looks through another user's directory without copying homework files, is that a violation of security?
  - The answer depends on site custom, rules, regulations, and laws, all of which are outside our focus and may change over time

Policies, Models, & Mechanism

innovate achieve lead

Security Policy between two organizations

- When two organizations work together, the entity they compose has a security policy based on the security policies of the two entities
- If those policies are inconsistent, both sites must decide what the security policy for the combined site should be
- The inconsistency often manifests itself as a security breach
- Example
  - Suppose a university and a corporation come together to collaborate on a project
  - Most universities have relatively more open security policies compared to corporations
  - If proprietary documents were given to the university, the corporation's confidentiality policy would conflict with more open policies of most universities
  - The university and the company must develop a mutual security policy that meets both their needs in order to produce a consistent policy

Policies, Models, & Mechanism

Security Model

- Provides a way to formalize (implement) security policies
- Is intended to provide an explicit set of rules that a computer can follow to implement the security policy
- Helps us understand how a computer operating system should be designed and developed to support a specific security policy
- Provides a way for designers to map statements from a security policy to algorithms and data structures necessary to build hardware and software
- Gives software designers something against which to measure their design and implementation
- Must support each part of the security policy so that the developers can be sure of their security implementation

Policies, Models, & Mechanism

innovate achieve lead

Goals of Security

- Given a security policy's definition of "secure" and "non-secure" actions and security mechanisms can
  - prevent
  - detect, or
  - recover

  from the attack
- These strategies may be used together or separately

Policies, Models, & Mechanism

Goals of Security – Prevention

- Prevention mechanisms can prevent compromise of parts of the system
- It means that an attack will fail. For example
  - If an attacker tries to break into a host server over the Internet and that host is not connected to the Internet, the attack has been prevented
- Prevention involves implementation of mechanisms that:
  - restrict users to specific actions and
  - are trusted to be implemented in a correct, unalterable way
  - ensure that an attacker cannot defeat the mechanism by changing it
- Preventative mechanisms often are very cumbersome and interfere with system use to the point that they hinder normal use of the system
- However, some simple mechanisms, such as passwords (to prevent unauthorized access to the system), are widely accepted
- Once the mechanism is in place, the resource protected by the mechanism need not be monitored for security problems, at least in theory

Policies, Models, & Mechanism

Goals of Security – Detection

- Is the option when an attack cannot be prevented
- Detection mechanisms accept that an attack will occur
- Indicates the effectiveness of preventative measures
- The goal is to determine that an attack is under way, or has occurred, and report it
- Sometimes, the attack is monitored to provide data about its nature, severity, and results
- Typical detection mechanisms monitor various aspects of the system, looking for actions or information indicating an attack

Policies, Models, & Mechanism

innovate achieve lead

Goals of Security – Detection

- A good example of a detection mechanism is one that gives a warning when a user enters an incorrect password three times
- The login may continue, but an error message in a system log reports the unusually high number of mistyped passwords
- Detection mechanisms do not prevent compromise of parts of the system, which is a serious drawback
- The resource protected by the detection mechanism is continuously or periodically monitored for security problems.

Policies, Models, & Mechanism

innovate achieve lead

Goals of Security – Recovery

- Recovery takes two forms:
- First: To stop an attack and to assess and repair any damage caused by that attack
  - For example
    - If the attacker deletes a file, one recovery mechanism would be to restore the file from backup media
  - In practice, recovery is far more complex
    - because the nature of every attack is unique
  - Thus, the type and extent of any damage can be difficult to characterize completely
  - Moreover, the attacker may return, so recovery involves identification and fixing of the vulnerabilities used by the attacker to enter the system
  - In some cases, retaliation (by attacking the attacker's system or taking legal steps to hold the attacker accountable) is part of recovery
  - In all these cases, the system's functioning is inhibited by the attack
  - By definition, recovery requires resumption of correct operation.

Policies, Models, & Mechanism

innovate achieve lead

Goals of Security – Recovery

- Second form: The system continues to function correctly while an attack is under way
  - This type of recovery is quite difficult to implement because of the complexity of computer systems
  - It draws on techniques of fault tolerance as well as techniques of security and is typically used in safety-critical systems
  - It differs from the first form of recovery, because at no point does the system function incorrectly
  - However, the system may disable nonessential functionality
  - This type of recovery is often implemented in a weaker form whereby the system detects incorrect functioning automatically and then corrects (or attempts to correct) the error.


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!