Network Security Models: Overview and Relevance

M K Lokesh Kumar

B.Tech . CSE(Cyber Security)

22011103026

Introduction

- What are security models?
  - They define rules and methodologies for enforcing security policies
  - They aim to achieve the CIA triad:
    - Confidentiality
    - Integrity
    - Availability
  - By employing security models, we can design networks that are resilient to threats like unauthorized access and data breaches.

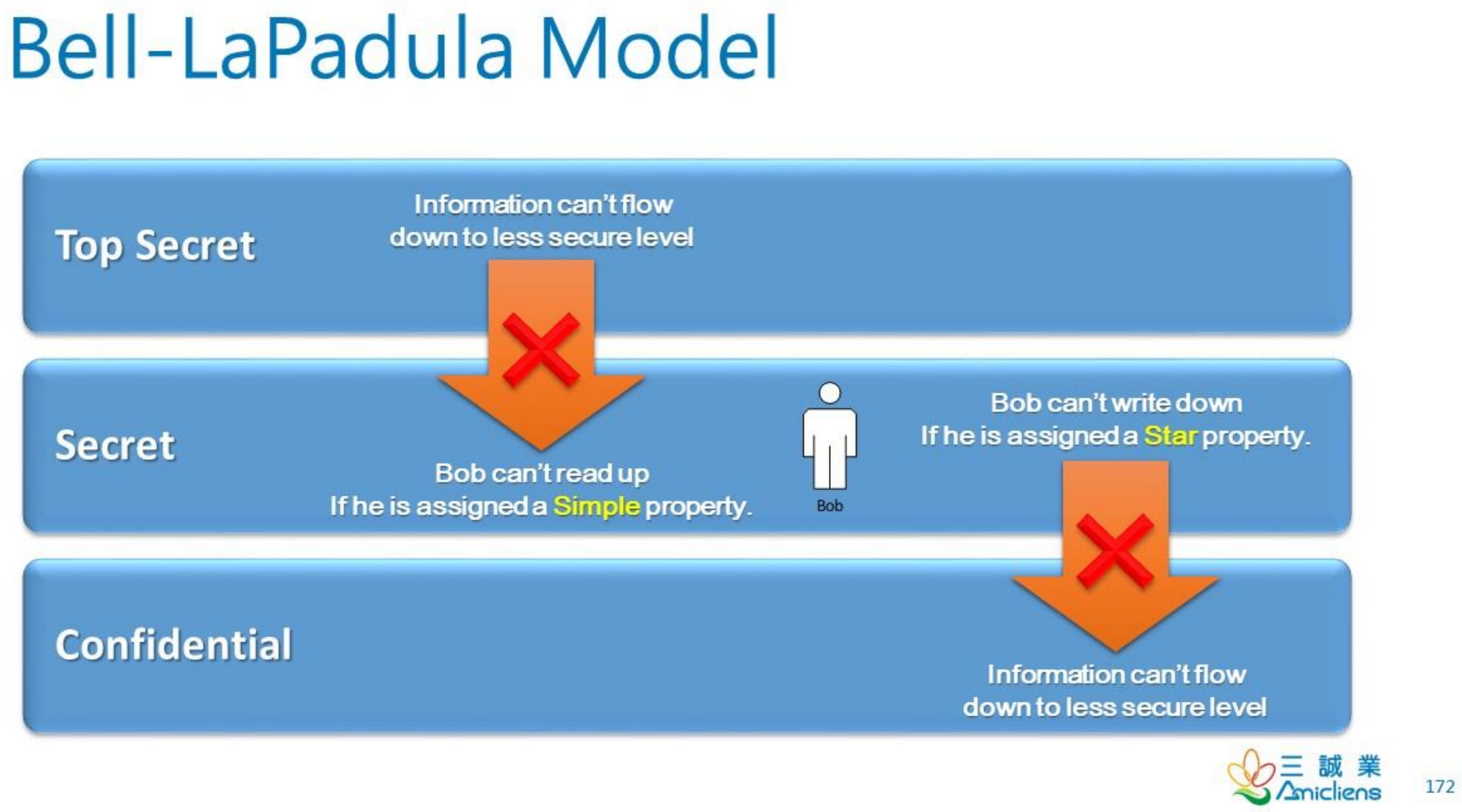
Common Security Models

- Bell-LaPadula model
  - Emphasizes on confidentiality
  - Prevents unauthorized access
- Biba model
  - Emphasizes on integrity
  - Ensures that data does not undergo unauthorized modification
- Charles-Wilson model
  - Its focus lies on commercial systems
  - Ensures well-formed transactions and separation of duties/concerns

Bell-LaPadula Model: An Overview

- Ensures confidentiality and ensures that there is no unauthorized access to data
- Key rules
  - "Simple Security Property": No read up; users cannot read data at a higher classification level than their clearance
  - "Star Property": No write down; users cannot write down data to a lower classification level to prevent data leakage

Bell-LaPadula Model: Hierarchy Levels



Bell-LaPadula Model

Top Secret

Information can't flow down to less secure level

Secret

Bob can't read up If he is assigned a Simple property.

Bob can't write down If he is assigned a Star property.

Confidential

Information can't flow down to less secure level

Bell-LaPadula Model: For Network Security Design

- Applications
  - Enforcing data access policies in multi-level secure systems
  - Preventing data breaches in multi-user environments
- Mechanisms used
  - Role-based access control(RBAC)
  - Secure file systems with classification labels
- Employing this model for a network's design ensures that only authorized users can access confidential data

Bell-LaPadula Model: Strengths

- Focus on confidentiality – To protect sensitive data
- Simplicity – Clear rules for data access
- Reduces the risk of accidental or intentional data leakage
- Widely applicable in a variety of environments including defense, where confidentiality is of great importance

Bell-LaPadula Model: Limitations

- Does not address data integrity i.e. ensuring that the data is not corrupted
- May not be suitable for modern systems with complex and dynamic access control
- Assumes trusted users at each level of the hierarchy
- May not guarantee data availability i.e. may not ensure that data is always available within the appropriate timeframe

Bell-LaPadula Model: Relevance in the present landscape

- Suitable for the following use cases
  - Classified systems in defense and government organizations
  - Cloud architectures with multi-user environments requiring strict access control
- Supports modern encryption standards and zero-trust principles