

FOUNDATIONS IN IT SECURITY: SECURITY MODELS

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)

TODAY

Today we will look at a number of fundamental security models; these include:

- Bell LaPadula Security Model
- BIBA Security Model
- MAC Security Model
- DAC Security Model
- RBAC Security Model
- Information Flow Security Model



GORDON | REYNOLDS (2019)

SECURITY MODELS

- A model is a simplified representation used to explain a real world system
- Security models are used to design a system to protect secrets

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES: BELL LAPADULA & BIBA SECURITY MODELS

GORDON | REYNOLDS (2018)

BELL LAPADULA SECURITY MODEL (1973)

- *State machine* model that addresses the **confidentiality** of information.
- Uses No Read Up & No Write Down
- No Read Up (NRU)
 - A subject can read all documents at or below his level of security but cannot read any documents above his level of security
 - Prevents learning secrets at a higher security level

BELL LAPADULA SECURITY MODEL (CONT.)

- No Write Down (NWD)
 - A subject can write documents at or above his level of security but cannot write documents below his level
 - Prevents leaks of secrets

BELL LAPADULA SECURITY MODEL (CONT.)

- What is the major flaw of this model?

BELL LAPADULA MODEL PROBLEM

- In Bell LaPadula
 - A subject at a lower security level can overwrite and potentially destroy secret information at a higher level (even though they cannot see it)
 - No Write Down and No Read Up don't prevent this "Write Up" operation
- Bell LaPadula protects **confidentiality** but not **integrity**

BIBA SECURITY MODEL (1977)

- The first formal **integrity** model, by preventing modifications to data by unauthorized persons.
- A subject cannot read documents below his level (*no read down*, NRD)
- A subject cannot write documents above his level (*no write up*, NWU)

EXAMPLE: MILITARY ORDERS

- Write Down is allowed
 - A General may write orders to a Colonel, who can issue these orders to a Major
- Integrity is preserved
 - In this fashion, the General's original orders are kept intact and the mission of the military is protected
- Write Up is forbidden
 - Conversely, a Private can never issue orders to his Sergeant, who may never issue orders to a Lieutenant, also protecting the integrity of the mission

COMPARING THE MODELS

- If you need to **protect secrets**, use Bell-Lapadula
 - No Write Down
 - No Read Up
- If you need to **stay on target**, use Biba
 - No Write Up
 - No Read Down
- Both of these are designed for the military, to protect high-level secrets

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES: CLARK-WILSON SECURITY MODEL

GORDON | REYNOLDS (2018)

CLARK-WILSON SECURITY MODEL (1987)

- Designed for businesses, to protect the integrity of data at all levels, not just the high value secrets
- Based on **Transactions**
 - **Well-formed transactions** move a system from one consistent state to another consistent state

CLARK-WILSON SECURITY MODEL (1987)

- A **data integrity model**
- Two principals: users and programs (called *transformation procedures*, or TPs)
- Two types of data: *unconstrained data items* (UDIs), and *constrained data items* (CDIs).

UDIS AND CDIS

- **Unconstrained Data Items (UDIs)**
 - Untrusted data, like user input
 - Not necessarily safe
 - May even be from an attacker
- **Constrained Data Items (CDIs)**
 - Data that has been verified and is now guaranteed to be valid
 - Data that is "safe"

CLARK-WILSON SECURITY MODEL (CONT.)

- **Integrity Verification Procedure (IVP)**
 - Transforms Unconstrained Data Items (UDIs) into Constrained Data Items (CDIs)
 - Changes "unsafe" data into "safe" data

CLARK-WILSON SECURITY MODEL (CONT.)

- Users must be authenticated
- Transaction logs are kept

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES: ACCESS MATRIX SECURITY MODEL

GORDON | REYNOLDS (2018)

ACCESS MATRIX SECURITY MODEL

- Defines which subjects are permitted to access which objects

| Subject | Contracts Directory | Personnel Directory | Expense Reports |
|---------|---------------------|---------------------|-----------------|
| Warren | Read | Read | Submit |
| Wilson | None | None | Approve |
| Wyland | Read/Write | None | Submit |
| Yelte | Read/Write | None | None |

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES:
MULTI-LEVEL SECURITY
MODEL

GORDON | REYNOLDS (2018)

MULTI-LEVEL SECURITY MODEL

- Several levels of security
 - Such as Confidential, Secret, Top Secret
- People have varying levels of security clearance
 - Such as Confidential, Secret, Top Secret
- System will control access to objects according to their level and the level of the persons accessing them

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES: MANDATORY ACCESS CONTROL (MAC) SECURITY MODEL

GORDON | REYNOLDS (2018)

MANDATORY ACCESS CONTROL (MAC) SECURITY MODEL

- System controls access to resources
- When a subject requests access to an object
 - The system examines the user's identity and access rights, and compares to access permissions of the object
- System then permits or denies the access
 - Example: shared file server where access permissions are administered by an administrator

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES: DISCRETIONARY ACCESS CONTROL (DAC) SECURITY MODEL

GORDON | REYNOLDS (2018)

DISCRETIONARY ACCESS CONTROL (DAC) SECURITY MODEL

- The **owner** of an object controls who and what may access it. Access is at the owner's discretion.
- Example: shared file server where access permissions are administered by the owners (users) of its contents.

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES: ROLE-BASED ACCESS CONTROL (RBAC) SECURITY MODEL

GORDON | REYNOLDS (2018)

ROLE-BASED ACCESS CONTROL (RBAC) SECURITY MODEL

- An improvement over the mandatory access control (MAC) security model
- Access permissions are granted to “roles” instead of “persons.”
 - Example: "Managers" can write to the Personnel folder, but "Help Desk Workers" cannot

ROLE-BASED ACCESS CONTROL (RBAC) SECURITY MODEL (CONT.)

- Simplifies management in a complex system with many users and objects
- Makes changes much easier, because they involve changes to roles instead of to individuals

COMPUTER SYSTEMS
SECURITY

CORE SECURITY PRINCIPLES: INFORMATION FLOW SECURITY MODEL

GORDON | REYNOLDS (2018)

INFORMATION FLOW SECURITY MODEL

- Based upon flow of information rather than on access controls
- Data objects are assigned to a class or level of security
- Flow of objects are controlled by security policy that specifies where objects of various levels are permitted to flow

SUMMARY

Today we looked at a number of fundamental security models; these include:

- Bell LaPadula Security Model
- BIBA Security Model
- MAC Security Model
- DAC Security Model
- RBAC Security Model
- Information Flow Security Model



GORDON | REYNOLDS (2019)

EXERCISE

- DevTechIT is an IT based company with several users spread across several roles.
- Using several security models, such as RBAC, MAC and the Access Matrix model, propose an information access solution for DevTechIT.
- Requirements:
 - Managers can Read&Write&Delete to the Company's News Information Folder and to the Managers Information Folder and to the Team Leads Information Folder.
 - Team Leads can modify and append to the Company's News Information Folder and Read&Write&Delete to the Team Leads Information Folder.
 - General Users can Read the Company's News Information Folder.
 - All users have a Home Folder which they can Read&Write&Delete to/from. No one else has access to this folder, but users can share files and/or folders with other users.