Exam Cram Notes: Security Architecture Models

1. What are Security Architecture Models?

Security architecture models provide structured frameworks for designing and implementing secure systems. These models define how security policies, principles, and controls should be applied to protect data, systems, and networks from threats.

---

2. Common Security Architecture Models

1. **Bell-LaPadula Model (BLP) – Confidentiality Model**
    - **Purpose**: Focuses on maintaining **confidentiality** in multi-level security (MLS) systems, ensuring sensitive data is not accessed by unauthorized users.
    - **Key Rules**:
        - **Simple Security Property (No Read Up - NRU)**: Users can only read at or below their security level (prevents unauthorized reading of higher-classified data).
        - **Star Property (* Property, No Write Down - NWD)**: Users can only write data at or above their security level (prevents classified data from leaking to lower levels).
    - **Use Case**: Military and government environments where data confidentiality is critical.

---

2. **Biba Model – Integrity Model**
    - **Purpose**: Focuses on maintaining **data integrity**, ensuring that data is not modified by unauthorized users or processes.
    - **Key Rules**:
        - **Simple Integrity Property (No Read Down - NRD)**: Users can only read data at or above their integrity level (prevents contamination by untrusted sources).
        - **Star Integrity Property (No Write Up - NWU)**: Users can only write data at or below their integrity level (prevents untrusted data from corrupting higher-integrity levels).
    - **Use Case**: Financial systems, medical records, and databases where maintaining accurate data is critical.

---

3. **Clark-Wilson Model – Commercial Integrity Model**
    - **Purpose**: Ensures **data integrity** through well-formed transactions and separation of duties.
    - **Key Concepts**:

        - **Well-Formed Transactions**: Users cannot modify data directly; changes must go through controlled processes.
        - **Separation of Duties**: Different users must be involved in processing transactions to prevent fraud.
        - **Access Control Triplet**: Defines subjects (users), objects (data), and transformation procedures (programs).
    - **Use Case**: Banking systems, e-commerce, and enterprise applications that require strict transaction controls.

---

4. **Brewer-Nash Model (Chinese Wall Model) – Conflict of Interest Model**
    - **Purpose**: Prevents conflicts of interest by restricting access to data based on a user's past interactions with certain datasets.
    - **Key Concepts**:
        - Users working with one company's data cannot access competitors' data.
        - Prevents **insider trading** and **confidentiality breaches** in corporate environments.
    - **Use Case**: Financial firms, law firms, and consulting firms handling sensitive corporate data.

---

5. **Graham-Denning Model – Access Control Model**
    - **Purpose**: Defines **how subjects (users) access objects (files, systems, resources)** through a set of secure operations.
    - **Key Rules**:
        - **Create/Delete Subjects & Objects**: Determines who can create or remove users and resources.
        - **Access Rights Transfer**: Defines how permissions can be delegated.
        - **Access Control Mechanism**: Enforces permissions based on predefined rules.
    - **Use Case**: Operating systems, database management systems (DBMS), and enterprise security frameworks.

---

6. **Harrison-Ruzzo-Ullman (HRU) Model – Extended Access Control Model**
    - **Purpose**: Extends the **Graham-Denning model** to define **how access rights change over time**.
    - **Key Features**:
        - Supports **dynamic permission changes** based on conditions.
        - Allows creating, deleting, and modifying access rights to objects.
    - **Use Case**: File system security, network access control, and evolving security environments.

---

7. **Zachman Framework – Enterprise Security Architecture**
    - **Purpose**: A structured framework for designing secure **enterprise IT systems** by considering multiple perspectives.
    - **Key Views**:
        - **Planner (What is the system's purpose?)**
        - **Owner (What business processes are involved?)**
        - **Designer (What technologies are required?)**
        - **Builder (How will the system be implemented?)**
    - **Use Case**: Large corporations, government agencies, and businesses implementing robust IT security strategies.

---

3. Key Exam Tips

✅ **Bell-LaPadula (BLP) is for confidentiality (No Read Up, No Write Down).**
✅ **Biba is for integrity (No Read Down, No Write Up).**
✅ **Clark-Wilson focuses on well-formed transactions and separation of duties.**
✅ **Brewer-Nash (Chinese Wall) prevents conflicts of interest.**
✅ **Graham-Denning defines access control mechanisms.**
✅ **HRU extends access control with dynamic rights management.**
✅ **Zachman is an enterprise security framework for IT architecture.**