Trust Boundaries

Trust boundaries are **conceptual lines within a system or network architecture that separate areas of different trust levels**. **Crossing a trust boundary generally requires authentication, authorization, or inspection to ensure that data and operations are permitted**. By defining trust boundaries, organizations **can identify where sensitive operations or data interactions occur and apply appropriate security controls to protect against unauthorized access or abuse**.

Key Concepts of Trust Boundaries:

1. **Different Levels of Trust**:

- Trust boundaries **separate areas with different security requirements**. For example, a public-facing web server is typically less trusted than an internal database containing sensitive data, so a trust boundary would exist between them.
- Examples of trust boundaries include:
    - **Internal vs. External Networks**: Separating internal corporate networks from the internet.
    - **Application Layers**: Dividing the application's front-end (e.g., user input forms) from its back-end (e.g., databases).
    - **User Roles**: Separating areas accessible to regular users from those accessible only to administrators.

2. **Identification of Sensitive Interactions**:

- Trust boundaries **help identify where sensitive interactions take place in a system**. These interactions require stricter controls, such as encryption, authentication, and access restrictions.
- Example: Between a web application's front end and a database where user credentials are stored, a trust boundary would exist, as unauthorized access to the database could expose sensitive information.

3. **Security Controls at Trust Boundaries**:

- To secure trust boundaries, security controls are implemented based on the sensitivity of the resources and the level of trust required.
- Common controls include:
    - **Firewalls**: Separate trusted internal networks from untrusted external networks.
    - **Access Control**: Role-based access to limit interactions across boundaries to authorized users.
    - **Encryption**: Protects data as it crosses boundaries, such as between client devices and servers.
    - **Input Validation**: Ensures data integrity when crossing boundaries, such as filtering user input to prevent SQL injection.

4. Trust Boundary Violations:

- Attackers often try to exploit trust boundaries to gain access to restricted areas of a system. By crossing a trust boundary without proper authorization, attackers can potentially access sensitive data or services.

- Example: A compromised web server might allow attackers to access the internal database if there aren't strict boundary controls.

5. Examples of Trust Boundaries in Different Environments:

- Web Applications: **Between the client and server**; for instance, user input fields (client) are separated from the database (server) by a trust boundary.
- Network Segmentation: **Separates user devices from sensitive networks**, such as corporate or server networks.
- Microservices and Containers: In microservices architectures, **each service might have a trust boundary to isolate sensitive services and prevent unauthorized data access between them**.

Why Trust Boundaries Matter in Threat Modeling:

In threat modeling, **defining trust boundaries helps identify where security risks are the greatest**. By understanding where untrusted or partially trusted entities interact with sensitive data or services, security teams can:

- **Map Attack Surfaces**: Understand which parts of the system are exposed to potential attacks and focus on protecting these boundaries.
- **Apply Appropriate Controls**: Decide on the right level of security controls based on the sensitivity of data or services crossing each boundary.
- **Prevent Privilege Escalation**: Prevent attackers from moving laterally across boundaries and gaining unauthorized access to restricted areas.

Summary:

Trust boundaries define the separation of areas with different trust levels within a system or network. They highlight sensitive areas where security controls are essential to prevent unauthorized access, data leakage, or privilege escalation. Properly managing trust boundaries is crucial for securing interactions in systems and networks, helping to prevent attackers from exploiting boundaries to gain unauthorized access to sensitive information or systems.