Security

Middleware for Distributed applications
Professor: Sophie Chabridon

- Ma Siqi
- Shalini Nagar
## CONTENTS

<table>
<thead>
<tr>
<th>Icon</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>📜️</td>
<td>Security Characterizing</td>
</tr>
<tr>
<td>📦</td>
<td>Security General Scenario</td>
</tr>
<tr>
<td>📈</td>
<td>Tactics for Security</td>
</tr>
<tr>
<td>🧑‍💼</td>
<td>A Design Checklist for Security</td>
</tr>
<tr>
<td>🔍</td>
<td>Summary</td>
</tr>
</tbody>
</table>
01 Security Characterizing

- Security & Attack
- CIA & Other characteristics support CIA
Security & Attack

What is Security?

- Security is a measure of the system’s ability to protect data and information from unauthorized access while still providing access to people and systems that are authorized.

What is Attack?

- An action taken against a computer system with the intention of doing harm is called an attack.
  - An unauthorized attempt to access data or services.
  - An unauthorized attempt to modify data.
  - An intention to deny services to legitimate users.
The simplest approach to characterizing security with CIA.

- **Confidentiality** is the property that data or services are protected from unauthorized access.
- **Integrity** is the property that data or services are not subject to unauthorized manipulation.
- **Availability** is the property that the system will be available for legitimate use.
Other characteristics support CIA

- **Authentication** verifies the identities of the parties to a transaction and checks if they are truly who they claim to be. For example, when you get an email purporting to come from a bank, authentication guarantees that it actually comes from the bank.

- **Nonrepudiation** guarantees that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. For example, you cannot deny ordering something from the Internet, or the merchant cannot disclaim getting your order.

- **Authorization** grants a user the privileges to perform a task. For example, an online banking system authorizes a legitimate user to access his account.
02 Security General Scenario

✓ Threat modeling - attack trees
✓ Security general scenario
✓ Sample concrete security scenario
Threat modeling - attack trees

The root is a successful attack
The nodes are possible direct causes of that successful attack.
Children nodes decompose the direct causes, and so forth.
The leaves of attack trees are the stimulus in the scenario.
Security general scenario

- Source of stimulus
- Stimulus
- Artifact
- Environment
- Response
- Response measure

<table>
<thead>
<tr>
<th>Portion of Scenario</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Human or another system which may have been previously identified (either correctly or incorrectly) or may be currently unknown. A human attacker may be from outside the organization or from inside the organization.</td>
</tr>
<tr>
<td>Stimulus</td>
<td>Unauthorized attempt is made to display data, change or delete data, access system services, change the system’s behavior, or reduce availability.</td>
</tr>
<tr>
<td>Artifact</td>
<td>System services, data within the system, a component or resources of the system, data produced or consumed by the system.</td>
</tr>
<tr>
<td>Environment</td>
<td>The system is either online or offline; either connected to or disconnected from a network; either behind a firewall or open to a network; fully operational, partially operational, or not operational.</td>
</tr>
</tbody>
</table>
| Response            | Transactions are carried out in a fashion such that:  
- Data or services are protected from unauthorized access.  
- Data or services are not being manipulated without authorization.  
- Parties to a transaction are identified with assurance.  
- The parties to the transaction cannot repudiate their involvements.  
- The data, resources, and system services will be available for legitimate use.  
The system tracks activities within it by:  
- Recording access or modification  
- Recording attempts to access data, resources, or services  
- Notifying appropriate entities (people or systems) when an apparent attack is occurring. |
| Response Measure     | One or more of the following:  
- How much of a system is compromised when a particular component or data value is compromised  
- How much time passed before an attack was detected  
- How many attacks were resisted  
- How long does it take to recover from a successful attack  
- How much data is vulnerable to a particular attack. |
Sample concrete security scenario

- A disgruntled employee from a remote location attempts to modify the pay rate table during normal operations. The system maintains an audit trail, and the correct data is restored within a day.
03 Tactics for Security

- Detect attacks
- Resist attacks
- React to attacks
- Recover from attacks
Tactics for Security

- One method for thinking about system security is to think about physical security.
- Secure installations have limited access to them (e.g., by using security checkpoints), have means of detecting intruders (e.g., by requiring legitimate visitors to wear badges), have deterrence mechanisms such as armed guards, have reaction mechanisms such as automatic locking of doors and have recovery mechanisms such as off-site back up.
- This leads to our four categories of tactics: detect, resist, react, and recover.
Categories as the goals of security tactics

Tactics to Control Security

Attack → System Detects, Resists, Reacts, or Recovers
Security Tactics

- Detect Attacks
  - Detect Intrusion
  - Detect Service Denial
  - Verify Message Integrity
  - Detect Message Delay

- Resist Attacks
  - Identify Actors
  - Authenticate Actors
  - Authorize Actors
  - Limit Access
  - Limit Exposure
  - Encrypt Data
  - Separate Entities
  - Change Default Settings

- React to Attacks
  - Revoke Access
  - Lock Computer
  - Inform Actors

- Recover from Attacks
  - Maintain Audit Trail
  - Restore
  - See Availability

- System Detects, Resists, Reacts, or Recovers
Detect Attacks

- **Detect intrusion** – It is the comparison of network traffic or service request patterns within a system to a set of signatures or known patterns of malicious behavior stored in a database. The signatures can be based on protocol, TCP flags, payload sizes, applications, source or destination address, or port number.

- **Detect service denial** – It is the comparison of patterns or signature of network traffic coming into a system of known denial of service attacks.

- **Verify message integrity** – This tactics employs techniques such as checksums and hash value to verify the integrity of the message.

- **Detect message delay** – In this tactics time during the delivery of the message is checked to detect suspicious timing behavior.
Resist Attacks

- **Identify actors** – Identifying actors is really about identifying the source of any external input to the system through user ID’s.
- **Authenticate actors** – Authentication means ensuring that who is the actor. It is identified through Passwords, OTP, and biometrics.
- **Authorize actors** – Authorization means ensuring that an authenticated actor has the rights to access and modify either data or services.
- **Limit access** – Limiting access involves controlling what and who may access which parts of system.
React to Attacks

- **Revoke access** – If the system or a system administrator believes that an attack is underway, then access can be severely limited to sensitive resources, even for normally legitimate users and uses.

- **Lock computer** – Repeated failed login attempts may indicate a potential attack. Many systems limit access from a particular computer if there are repeated failed attempts to access an account from that computer. Legitimate users may make mistakes in attempting to log in. Therefore, the limited access may only be for a certain time period.

- **Inform Actors** – Ongoing attacks may require action by operators, other personnel, or cooperating systems. Such personnel or systems—the set of relevant actors — must be notified when the system has detected an attack.
Recover from Attacks

- Once a system has detected and attempted to resist a attack it needs to recover by means of restoration of services.
- Set of availability tactics can be brought to deal with recovering from failures and to restore services.
- Audit trial — that is, keep a record of user and system actions and their effects—to help trace the actions of, and to identify, an attacker.
- The audit trials can be analyzed to prosecute attackers or to create better defense for the system in the future.
04 Design checklist for security
A Design Checklist for Security

- **Allocation of Responsibilities**: Determine which system responsibilities need to be secure.
- **Coordination Model**: Determine mechanisms required to communicate and coordinate with other systems or individuals.
- **Data Model**: Determine the sensitivity of different data fields.
- **Mapping among Architectural Elements**:
  - Determine how alternative mappings of architectural elements that are under consideration may change how an individual or system may read, write, or modify data; access system services or resources; or reduce availability to system services or resources.
  - Determine how alternative mapping may effect the recording of access to data, services or resources and the recognition of unexpectedly high demands for resources.
A Design Checklist for Security

• **Resource Management:**
  – Determine the system resources required to identify and monitor a system or an individual who is internal or external, authorized or not authorized, with access to specific resources or all resources.
  – Determine the resources required to authenticate the actor, grant or deny access to data or resources, notify appropriate entities (people or systems), record attempts to access data or resources, encrypt data, recognize inexplicably high demand for resources, inform users or systems, and restrict access.

• **Binding Time:** Determine cases where an instance of a late-bound component may be untrusted.

• **Choice of Technology:** Determine what technologies are available.
05 Summary
Summary

- Attacks against a system can be characterized as attacks against the confidentiality, integrity, or availability of a system or its data.
- Identifying, authenticating, and authorizing actors are tactics used to identify which user are entitled to what kind of access to system.
- No security tactic is foolproof and that systems will be compromised. Hence, tactics exist to detect an attack, limit the spread of any attack, and to react and recover from an attack.
Bibliography

- [2013 sap_security] Bass, Clements & Kazman,
- Software Architecture in Practice, chapter Security,
- Addison-Wesley Professional (2013).
Questions

THANK YOU FOR LISTENING

Ma Siqi
Shalini Nagar