OSM - Ali Initial.xmi

Total Number of Threats Detected: 4/6

Spoofing (1)

Unmitigated Threats: 0

Potentially Mitigated Threats: 1

- Valid Accounts (T1078)

Mitigated Threats: 0

Repudiation (1)

Unmitigated Threats: 1

- Access Token Manipulation (T1134)

Potentially Mitigated Threats: 0

Mitigated Threats: 0

Information Disclosure (1)

Unmitigated Threats: 0

Potentially Mitigated Threats: 0

Mitigated Threats: 1

- Adversary-in-the-Middle (T1557)

Denial Of Service (1)

Unmitigated Threats: 0

Potentially Mitigated Threats: 1

- Denial of Service (T0814)

Mitigated Threats: 0

BSP Vector: < (1.11, 0.47), 12.00 >

CERI Values for Detection Elements:

- **CustomerDatabase (DataStoreNode)**
  - Worst-case CERI: 1.33, Best-case CERI: 0.67
- **DecisionNode1 (DecisionNode)**
  - Worst-case CERI: 0.0, Best-case CERI: 0.0
- **DecisionNode2 (DecisionNode)**
  - Worst-case CERI: 0.0, Best-case CERI: 0.0
- **Encrypt Data (OpaqueAction)**
  - Worst-case CERI: 0.0, Best-case CERI: 0.0
- **MergeNode1 (MergeNode)**
  - Worst-case CERI: 0.0, Best-case CERI: 0.0
- **Customer Information (SendSignalAction)**
  - Worst-case CERI: 0.0, Best-case CERI: 0.0
- **Customer Login Request (AcceptEventAction)**
  - Worst-case CERI: 2.0, Best-case CERI: 0.67
- **Request Customer Information (OpaqueAction)**
  - Worst-case CERI: 2.0, Best-case CERI: 0.67
- **Login Information (SendSignalAction)**
  - Worst-case CERI: 2.0, Best-case CERI: 1.0
- **Login Information (AcceptEventAction)**

  - Worst-case CERI: 2.0, Best-case CERI: 0.67
- **Customer Login Request (SendSignalAction)**
  - Worst-case CERI: 2.0, Best-case CERI: 2.0
- **Validate Customer Information (OpaqueAction)**
  - Worst-case CERI: 2.0, Best-case CERI: 0.0

Total Number of Flows Detected: 7

Has DataSanitizer Object? False

Suggested DataSanitizer Locations:

Protecting Expected Entry Points

It is recommended to place a DataSanitizer object between the following elements:
1. **InitialNode: InitialNode1** (parented by WebClient)
2. **SendSignalAction: Customer Login Request** (parented by WebClient)

This recommendation is useful if the threat of insider attacks is sufficiently small compared to the threat of external attacks. Examples of such external attacks include attempting to harm your system by threatening its availability or attempting a forceful takeover using arbitrary code execution via corrupted data.

Protecting Data Stores

It is recommended to place a DataSanitizer object between the following elements:
1. **AcceptEventAction: Login Information** (parented by CustomerManager)
2. **DataStoreNode: CustomerDatabase** (parented by CustomerManager)

This recommendation is beneficial if you want to maximize the protection of your data stores against corrupted data that would be damaging if destroyed or leaked to an attacker (e.g., data injection attacks).

Minimizing Corruption Propagation

It is recommended to place a DataSanitizer object between the following elements:
1. **DecisionNode: DecisionNode2** (parented by CustomerManager)
2. **OpaqueAction: Encrypt Data** (parented by CustomerManager)

This recommendation should be applied if you have the goal of minimizing the longest flow of corruption within your system, making system-wide data corruption attacks more difficult.

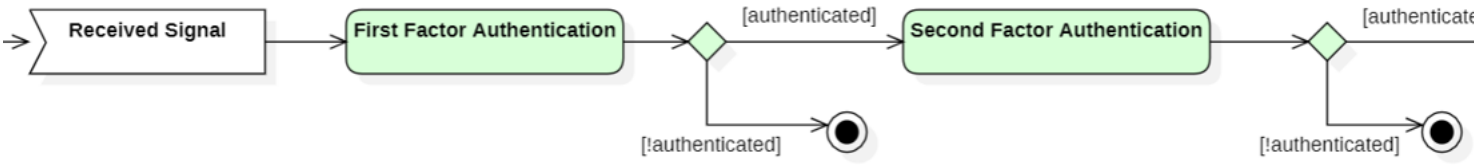
Mitigation Suggestions:

Spoofing Mitigation Suggestions

Dubhe detected that your system may be susceptible to the threat of **Valid Accounts** (T1078).

To help mitigate against this threat, we recommend the mitigation named **Account Use Policies** (M1036).

To give you an example of how that might look in a UML activity diagram, please see the example image below (of note the mitigation elements are coloured green):

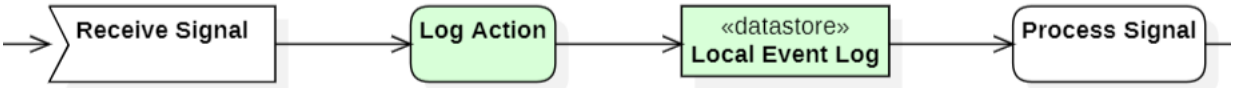


Repudiation Mitigation Suggestions

Dubhe detected that your system may be susceptible to the threat of **Access Token Manipulation** (T1134).

To help mitigate against this threat, we recommend the mitigation named **User Account Logging** (M1018).

To give you an example of how that might look in a UML activity diagram, please see the example image below (of note the mitigation elements are coloured green):



Denial Of Service Mitigation Suggestions

Dubhe detected that your system may be susceptible to the threat of **Denial of Service** (T0814).

To help mitigate against this threat, we recommend the mitigation named **Filter Network Traffic** (M1037).

To give you an example of how that might look in a UML activity diagram, please see the example image below (of note the mitigation elements are coloured green):