Lecture 5

Threats and Security in Development

Reference:

Michael Shin, Don Pathirage, Dongsoo Jang "Threat and Security Modeling for Secure Software Requirements and Architecture," SEKE, 2020.

Existing Threat Modeling

- Several threat modeling approaches suggested
  - Software, asset, and attacker centered threat modeling
  - Do not specify when and what types of threats identified and modeled in software development
  - May require all threats identified in one development phase only (e.g., requirements specification or design)

Motivation

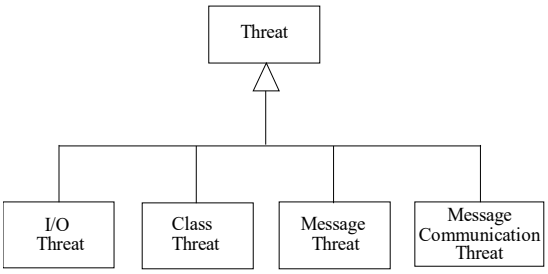
- When and what types of threats
  - In requirements specification/analysis and software architecture design
  - Threats Identified and modeled
  - Modeling of security countermeasures
- Approaches
  - Threats identified at each development phase
  - Develop threat model and security measures at the phase
  - Next phase include the security measures defined in previous phase
  - Then identify threats in the current phase and develop security countermeasures
  - Repeat this process through secure development cycle

3

3

Threats

- The threats to systems determined
  - by considering the threats to assets
    - In software requirements and architecture
- Threats in software requirements and architecture



4

4

Threats

- I/O threats
  - Induced by an actor's interactions with a system
  - In software requirements specification modeled with the use case model
    - Actor's sensitive input to and/or output from a system compromised
    - Actor's untrusted input compromising the system
- Class threats
  - Occur when the objects of classes engaged in processing or storing sensitive data
  - In requirements analysis modeled using class diagram

5

5

Threats

- Message threats
  - Sensitive messages passed between objects threatened
  - In requirements analysis modeled with communication diagram or sequence diagram
- Message communication threats
  - Messages communicated between components compromised
    - Components and connectors for software architecture
    - Connectors
      - Encapsulate the detail of message communication
      - Breach of connectors
  - In software architecture modeled with connectors

6

6

Threats in Use Case Model

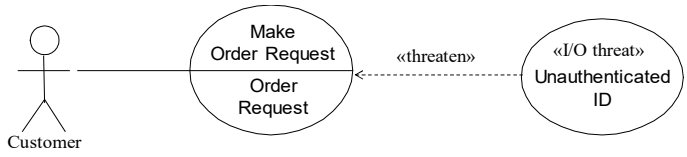
- I/O threats caused by the interaction between actors and the system
  - Compromised Input threat, such as dirty input from human or external system
  - Confidential (privacy) input threat, such as disclosure of sensitive input/output
  - Availability input threat, such as denial of service attack input caused by a bot or mal-timer
- I/O threats identified by analyzing the use case description

7

7

Threat modeling for use case model

- Threat represented using the use case notation
- E.g., unauthorized ID input threat in *make order request* use case at the order request threat point



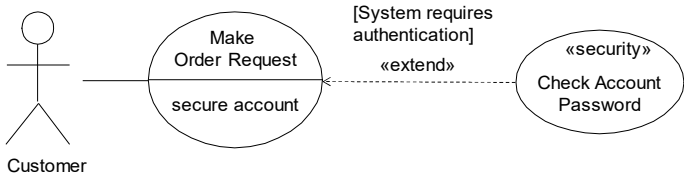
- Threat name: unauthenticated ID
- Threat type: I/O threat
- Threat point: order request
- Security asset: customer account
- Description: a legitimate customer's account can be used to make an order maliciously.
- Security need: authentication

8

8

Security modeling for use case model

- Security countermeasure against an I/O threat
  - Specified using a security use case separately from application use cases
  - When a system requires a security countermeasure, the security use case extends the application use case
- Security use case for Make Order Request use case



9

9

Secure Static Model

- Determine security classes for security use case
  - Security use cases need security classes
    - To realize the security use cases
  - Security classes
    - Provide security services
  - Application classes
    - Provide application logic
- Define relationships between application classes and security classes
  - Application classes request security services from security classes
- Develop threat/application/security diagram
  - Represent threat classes, application classes and security classes
  - Using class diagram notation
- Develop each security class description
  - Security class name, description, and threat

10

10

Threats in Class Model

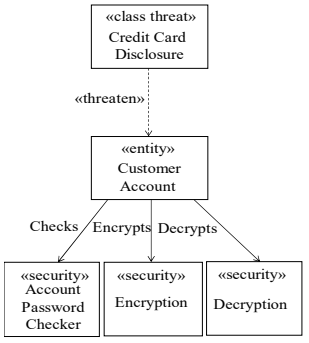
- Class threats identified
  - By considering the role of each class
- Interface class interfacing to and interacts with an actor
  - Same as use case threats
- Entity class that stores data
  - Might have sensitive data
- A control class that contains the system's sensitive state information or coordination logic
  - Might be compromised
- An application logic class that contains the details specific to applications
  - Might be tampered with

11

11

Threat modeling for class model

- A credit card disclosure class threat identified and modeled in the class diagram
  - Customer Account class stores the customer's sensitive credit card data
- Class threat modeled with the stereotype «class threat» and «threaten» Threat
- Security countermeasure against the credit card disclosure class threat
  - Modeled with Encryption and Decryption security classes



a) Class Threat and Security Classes for Customer Account class

- Threat Name: credit card disclosure
- Threat Type: class threat
- Security Asset: credit card
- Description: credit card can be disclosed
- Security Need: confidentiality

b) Class Threat Description for Credit Card Disclosure

12

12

Secure Dynamic Model

- Determine where security objects are participated in sequence of application object interactions
  - Security objects invoked by application objects
    - if application objects need security services
- Represent security objects in communication diagram or sequence diagram
  - Along with application objects
  - For most of cases, may not need to change the sequence numbers for application object interaction
  - Security objects are added to communication diagram
    - Using additional sequence numbers

Threats and security modeling for communication model

- Message threats in the communication model
  - Can be the threats to confidentiality, integrity or non-repudiation security of messages
  - When a sensitive message is sent by an object to another
- Message threats determined
  - By examining the messages passed between objects on the communication diagrams
  - Security objects incorporated into the communication diagrams

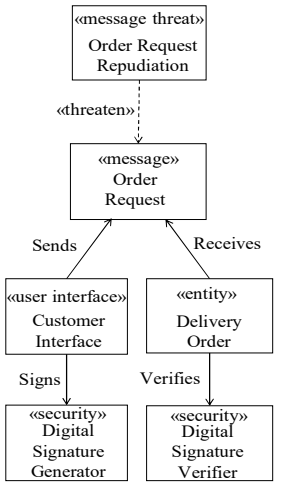
Threats and security modeling for communication model

- Message threats modeled using the class notation
  - Depicted with the stereotype «message»
  - Message threat depicted with the stereotype «message threat»
  - Has a «threaten» dependency relationship with message
- Each message threat described in a message threat description

15

15

Order Request Repudiation message threat and Description



a) Order Request Repudiation threat

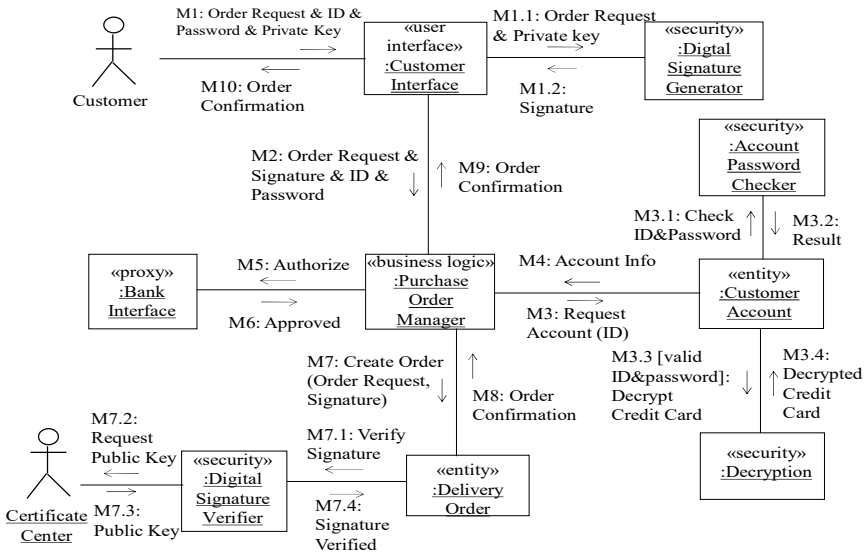
- Threat Name: Order Request Repudiation
- Threat Type: message threat
- Security Asset: Order Request
- Description: Customer can repudiate an order request.
- Security Need: Non-repudiation

b) Message Threat Description for Order Request Repudiation threat

16

16

Communication diagram for Make Order Request use case



17

Threats and security modeling for software architecture

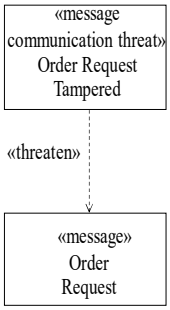
- Message communication threats identified in terms of
  - Integrity, confidentiality, non-repudiation, authentication and authorization
  - Sensitive messages communicated between components tampered with
  - Sensitive messages disclosed
  - Sensitive message repudiated by the sender component later
  - Message sender component's identity may require authentication
    - When the sender component sends a sensitive message to a receiver component
  - Sender component requires authorization if it needs to access the sensitive data

18

18

Order Request Tampered communication message threat

- Message communication threat to order request message
- Message communication threat description



a) Order Request Tampered Message Communication threat

- Threat Name: Order Request Tampered
- Threat Type: Message communication threat
- Security Asset: Order Request
- Description: Customer's order request can be tampered.
- Security Need: Integrity

b) Order Request Tampered Message Communication Threat Description

19

19

Secure Connectors for software architecture

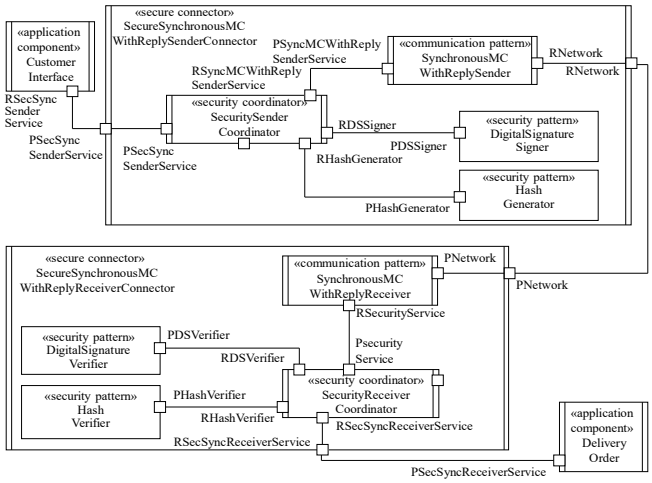
- A secure connector is a distributed connector,
  - A secure sender connector for a sender application component
  - A secure receiver connector for a receiver application component
- Each sender connector and receiver connector
  - A communication pattern object
  - One or more security pattern objects
  - A security coordinator object
    - Sequences the interactions with one or more security pattern objects and with a communication pattern object

20

20

Example – Designed Secure Connector

- Structural view of secure synchronous message communication with reply (SMCWR) connector
  - With Digital Signature security pattern and Hashing security pattern
  - Applied for making an order request



21

21