ASSURANCE CASE FOR MOBILE PAYMENT SYSTEM

Ojetunde Babatunde Segun
Mehnaz Seraj
Purpose of Exercise

- Experience system assurance lifecycle
- Learn background of the system assurance

- Learn techniques for system assurance
  - Describing a target system
  - Analyzing risk
  - Considering architectural design
  - Considering counter measures of the risk
  - Constructing arguments showing any risk is mitigated to acceptable level
Overview of Target System

- Customer can purchase items from merchant using endorsement after disaster happens
- This will ease difficulty of doing transaction where there is unavailability of network infrastructure
- The assurance case for Mobile Payment Systems for this exercise is created from mobile payment point of view
  - Normal daily transaction
  - Disaster area transaction
- We focus on disaster area transactions
Overview of Target System 2

Timing of Using the System

- Disaster Period
- Post Disaster Period (1 Month after Disaster)
- Post Disaster Period (3 Months after Disaster)
- Post Disaster Period (1 year after Disaster)
Endorsement - Hoshounin

- An Endorser must be:
  - Known to the bank (customer of the bank)
  - Must be a user of the mobile payment system

- Minimum of 5 Endorsers is assumed to avoid one person from paying too much money in case a Customer default

- In case of non-payment, Endorsers will pay for the item purchased by the customer

- Each Endorser decides maximum amount (Price) to pay for defaulted user

Provide at least five (5) Endorsers that will serve as a surety for each transaction
Overview: Normal Transaction

- The customer send transaction order to the merchant for the purchase of an item

- The Merchant forward the payment information to the bank
  - The bank deduct the money from the customer and pay the Merchant
  - If there is no money in the customer account, the transaction is declined
Overview: Disaster Area Transaction

1. Merchant
2. Customer
3. Endorsers
4. Bank/MP Service provider
5a. Merchant to Customer
5b. Customer to Merchants
6a. Customer to Bank/MP Service provider
6b. Endorsers to Bank/MP Service provider
7a. Bank/MP Service provider to Customer
7b. (optional)
Send digitally signed message to the Merchant (Item Order Form which includes Item, Quantity) and digitally signed picture of the customer

The Merchant Verify the Customer with the picture, there is no possibility the mobile phone is stolen
Here, we assume that there are Endorsers available.

Merchant M forward the message to Endorser.

Create Billing Form and forward Billing Form and Item Order Form to Endorsers.
Transaction Process (3/5)

Authenticate the Merchant & Create endorsement form
Send The Endorsement Form, Billing Form and Item Order form to the Merchant

Merchant forward the Billing Form, Endorsement Form and Item Order Form to the Bank
Bank authenticate the Customer, Merchant and Endorser.

Bank B checks if the content of Item Order Form, Endorsement Form and Bill Form is consistent.

Checks if Customer has enough fund in his account and transaction value is deducted from Customer’s account.

Merchant Send Transaction confirmation to Customer and copy the Endorsers.

Bank/MP Service provider

User C_A account is debit
If there is no fund in Customer account and the transaction value is deducted from the Endorsers account.

- Merchant account is credited.
- Default message is sent to the Endorsers and debit the Endorsers account.
- Send Default message to Endorsers and debit the Endorsers account.
- Debit Endorsers account for the Customer's transaction based on the Endorsed value.
- Send acknowledgement to Merchant, Customer and Endorser.
System Assurance Lifecycle

2. Possible Adverse Consequences
- Lose of Private information (user’s picture, contact list, account information and text message).
- Lose money.
- Stop the Mobile Payment Service.
- Users receive spam mails.
- Lose of mobile phone.

1. Scope of Systems
- Customer can purchase items from merchant using endorsement after disaster happens

4. Attack Tree

5. Architectural Design/Deployment Diagram

6. Assurance Case

5. Specialist Comment
Roles of D-Case in this Exercise

- To show justification of using generalized common criteria framework

- Traceability
  - from threats to security objectives
  - from security objectives to security requirements
The workflow of this project with Redmine and D-Case
<table>
<thead>
<tr>
<th>Document ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID1</td>
<td>Informal description of the target system</td>
</tr>
<tr>
<td>ID2</td>
<td>Informal description of physical overview</td>
</tr>
<tr>
<td>ID3</td>
<td>Informal description of bad scenarios</td>
</tr>
<tr>
<td>ID4</td>
<td>General requirements</td>
</tr>
<tr>
<td>ID5</td>
<td>Use case diagram in UML</td>
</tr>
<tr>
<td>ID6</td>
<td>Deployment diagram in UML</td>
</tr>
<tr>
<td>ID7</td>
<td>Message Sequence diagram in UML</td>
</tr>
<tr>
<td>ID8</td>
<td>Class diagram in UML</td>
</tr>
<tr>
<td>ID9</td>
<td>List of base standards</td>
</tr>
<tr>
<td>ID10</td>
<td>List of adverse consequences</td>
</tr>
<tr>
<td>ID11</td>
<td>Attack tree diagram in UML</td>
</tr>
</tbody>
</table>
Examples of Documents content (Use case)
Examples of Documents content (Specification of Participants)
Examples of Documents content
Examples of Documents content (Message Sequence)
Examples of Documents content (Attack tree)
Examples of Documents content (Assurance Case)

- **Goal G.1**: The mobile payment system is secure created 0%
  - **Strategy S.1**: Arguments over each sub-goal (depending on risk mitigation argument structure)
  - **Content C.1**: Risk treatment/mitigation structure for mobile payment system
  - **Goal G.2**: Customer's money is secure created 0%
  - **Goal G.3**: Customer's private information is secure created 0%
  - **Goal G.4**: Response time delay failure can be recovered created 0%
  - **Strategy S.2**: Argue over each sub-goal
  - **Content C.2**: Definition and list of each sub-goal
  - **Strategy S.3**: Argue over each sub-goal
  - **Content C.3**: Security objectives specification documents for this sub-goal
  - **Goal G.5**: Attacker cannot order items illegally
  - **Evidence E.1**: Test results for authentication
  - **Evidence E.2**: Test result for access control
  - **Goal G.6**: Payment server is secure
    - **Evidence E.3**: Test result for access control
  - **Goal G.7**: Very few private information is used for doing a transaction
    - **Evidence E.4**: User's picture and delivery address is visible only
  - **Goal G.8**: Attacker can attack the MANET network
  - **Goal G.9**: The payment server is secure
    - **Evidence E.5**: Security testing result for access control
    - Undeveloped...
Review of our project

- Visiting companies
  - National Institute of Advanced Science and Technology (AIST)
  - Nagoya Institute of Technology
  - Atelier Corporation
Comments from AIST

- **System failure**
  - If the system fails by itself what measure can be taken

- **Mobile vulnerability**
  - Issues that concern the mobile phone that are not related to the payment system

- **False disaster alert**
  - Countermeasures to prevent attacker from given false disaster alert

- **Consider common criteria framework for threat analysis**

- **What are the assumptions of the environment of the system**
Comments from Nagoya Institute of Technology

- What are the set rules/constraints to using the system
  - Upper limit of purchase
  - Number of transaction per day

- Attack tree should be created from attacker’s viewpoint

- How or what level data is gathered

- Highlight the vulnerabilities of the system
Comments from Atelier Corporation

- Specify asset, threat and counter measures required by common criteria

- Show traceability from threats to security objectives and from security objectives to security requirements

- Show why our constraints are necessary and complete
Feb, 10

- Intensive Lectures
- Tunde-san’s ppt Slides
- Initial list of adverse consequence
- Risk table based on EVITA
- Feb 20 Visit AIST
- Feb 27 Visit Nagoya Institute of Technology

Feb, 10

- Use case diagram (detailed version)
- FTA/Attack tree
- Attack tree

Feb, 25

- Product Activity Event
- Fixing limitation of the amount of transactions
- Organizing documents based on common criteria framework
- Use case diagram having mobile phone as an external actor
- List of threat (not containing general attacks for network/Mobile phone)

Mar, 6

- Fix process guideline for using D-Case & Redmine
- Atelier

Mar, 11

- Noticed stakeholder list should have been fixed first

Mar, 4

- Matsuno-Sensei’s D-Case lecture

Mar, 18

- Record/log of activities
Current problems of D-case methodology

- Too many viewpoint of argument structure
  - No guideline for integrating them

- Effectiveness of D-case from a view of one aspect is not clear.
Problematic Characteristics of our system

- Boundary is unclear
- Involve other huge system
- Changing it’s configuration continuously
- Relating a number of users
- Expected to work correctly in emergency
Acknowledgement

- We are grateful to Dr. Taguchi, Prof. Koshijima, Dr. Daichi Mizuguchi, Dr. Hiroki Takamura, Dr. Matsuno for their valuable comments.
THANK YOU