Eliciting Software Security Requirements through Misuse Actions

Fabricio Braz

03/07/08
Intro

• Software Systems
  – World wide dependency
• Failures consequences
  – Embarrassment
    • “Illegal” affair uncovered
  – Infrastructure harm
    • CIA Confirms Cyber Attack Caused Multi-City Power Outage (01/18/08)
• CERT-CC statistics show hopeless tendency
Security from the beginning

- Experiences’ shown about added-on security [McGraw06]
- Security as an integral part of lifecycle
  - No single software engineering meth. [Mouratidis06]
  - Software security requirements claim more comprehensive approach [Redwine06]
Software Security Requirements (1)

• Wide range from software to software
  – Each system has its particular security goals
    • Authentication, authorization, transaction integrity, logging & auditing ...

• Systems fails
  – wrong things are protected correctly
  – right things are protected in the wrong way

• What’s important to be protected, and what protection is needed
Software Security Requirements (2)

• Higher system perspective analysis
• What’s the attacker goal
  – theft of identity, money ...
• Security requirements should define the sec needs without mechanisms commitment
  – Uncovering the potential attack (threat)
Objective

- Evolve the misuse approach in order to
  - give a more systematic way to elicit software security requirements by
    - detailing its dynamics so that analysts can easily uncover threats and select the suitable security policies to mitigate and/or stop them.
Misuse approach (1)

• Systematic way to:
  – identify system threats
    • use case flow of events depicted by activity diagram
    • analysis of each activity in a way to find misuse
  – determining policies to stop/mitigate their effects
    • authentication, logging, separation of duties, closed system, etc. [Fernandez06]
Misuse approach (2)

Customer

Provide personal info

:Customer

Check credit

Create account

:Account1

Initial deposit

Create authorization

Issue card

:Card1

Manager

External Attacker

:Account1

Impostor

false info

Provide personal info

:Customer

Check credit

Create account

:Account3

Illegal dissemination

Create spurious account

:Account2

:Card1

Issue card

:Card2

Manager

Impostor

Illegal dissemination

Create spurious account

:Account2

:Card1

Issue card

:Card2

Legend

- object
- activity
- control flow
- data flow
- misuse activity
- misuse flow

Secure Systems Research Group - FAU
## Misuse approach (3)

<table>
<thead>
<tr>
<th>Threats</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>The customer provides false information and opens spurious account</td>
<td>Mutual authentication. Every interaction across system nodes is authenticated</td>
</tr>
<tr>
<td>The manager creates a spurious account with the customer’s information</td>
<td>Logging. Since the manager is using his legitimate rights we can only log his actions for auditing at a later time</td>
</tr>
<tr>
<td>The manager creates a spurious authorization card to access the account.</td>
<td>Separation of administration from use of data. For example, a manager can create accounts but should have no rights to withdraw or deposit money in the account.</td>
</tr>
<tr>
<td>An attacker tries to prevent the customers access to their accounts</td>
<td>Protection against denial of service. We need some redundancy in the system to increase its availability.</td>
</tr>
</tbody>
</table>
Misuse approach (4)

• How should the analysis of the activity be employed?
• What is the path between the misuse action and the related system policy or policies?
• What role do high level security policies play?
Misuse Actions Dynamics
System Activities Analysis (1)

- Three levels of systematic
  - Use case
    - Entails all system interactions
  - Source of threat [Cole2005]
    - External
      - Any person without access to org. system
    - Internal authorized
      - Has access to org. system, but not the system/action in consideration
    - Internal unauthorized
      - Has access to org. system, the system/action in consideration included
  - Security concern [Pfleeger2002]
    - Confidentiality, Integrity, Availability, Accountability
System Activities Analysis (2)

- What misuse could be done in <activity> by <source> which compromise <sec prop.>
  - <activity> : find out in the activity diagram
  - <source> : external, internal authorized, internal unauthorized
  - <sec prop.>
    - Conf: snooping, disclosure, eavesdropping
    - Integrity: deception, masquerading, spoofing, usurp
    - Availability: denial of service, disruption
    - Accountability: repudiation
<table>
<thead>
<tr>
<th>Actor</th>
<th>Action</th>
<th>Sec. Prop. CO/IN/AV/AC</th>
<th>Source InA/InU/Out</th>
<th>Description</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>Provide Info</td>
<td>AC</td>
<td>InA</td>
<td>Claims did not authorize the account opening</td>
<td>Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AV</td>
<td>Out</td>
<td>Overwhelm application</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>Out</td>
<td>Eavesdropping</td>
<td>Customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>Out</td>
<td>Uncover customer relationship with inst. by trying to create new account in his/her name</td>
<td>Customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IN</td>
<td>InA</td>
<td>Invalid financial info provided</td>
<td>Customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IN</td>
<td>InA</td>
<td>Personal spurious info provided</td>
<td>Customer</td>
</tr>
<tr>
<td>Manager</td>
<td>Check credit</td>
<td>AC</td>
<td>InA</td>
<td>Refuses modification in customer credit info</td>
<td>Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AV</td>
<td>InU</td>
<td>Overwhelm application</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>InU</td>
<td>Eavesdropping</td>
<td>Customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>InA</td>
<td>Collects customer personal info to disseminate illegally</td>
<td>Customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IN</td>
<td>InA</td>
<td>Changes the cust. credit info to get more clients</td>
<td>Customer</td>
</tr>
<tr>
<td>Manager</td>
<td>Create account</td>
<td>CO</td>
<td>InU</td>
<td>Eavesdropping</td>
<td>Account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CO</td>
<td>InA</td>
<td>Collects customer personal info to disseminate illegally</td>
<td>Account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IN</td>
<td>InA</td>
<td>Creates spurious account</td>
<td>Account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AC</td>
<td>InA</td>
<td>Refuses creating spurious account</td>
<td>Log</td>
</tr>
<tr>
<td>Customer</td>
<td>Initial deposit</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Manager</td>
<td>Create authorization</td>
<td>CO</td>
<td>InA</td>
<td>Create a spurious authorization / card</td>
<td>Card</td>
</tr>
<tr>
<td>Manager</td>
<td>Issue card</td>
<td>CO</td>
<td>InA</td>
<td>Do not issue card</td>
<td>Card</td>
</tr>
</tbody>
</table>

Legenda: CO - Confidentiality; IN - Integrity; AV - Availability; AC - Accountability; Out - Outsider; InA - Insider Authorized; InU/Out - High, M. Medium, L. Low
How to select the security policies? coming soon

• Would the threat details uncovered help?
  – <source> + <sec property> leads <policy>

• Would be interesting to apply a preliminary risk analysis?
  – Find out relevant threats which really deserve deep analysis, e.g. attack tree

• What else?
Security Requirements Area Overview

- Misuse case
  - Alexander,
- Threat modeling
  - Lipner
- Problem frames
  - Heisel, Haley
- SQUARE
  - Mead
- CEPAC
  - Attack patterns – McGraw (Cigital)
References so far

Thanks'

- Happy international women’s day (march 8th)