Lecture 12:
Related (to Security) Requirements

Outline

• Safety analysis
• Privacy definition
• Trust and Trustworthiness
Dependability

- **Dependability**
  - degree to which various kinds of users can depend on a work product

- **Defensibility**
  - degree to which a system or component defends itself from accidents and attacks

---

Security

- **Security**
  - degree to which malicious harm is properly addressed (e.g., prevented, identified, reacted to, and adapted to)

Safety

- **Safety**
  - degree to which accidental harm is properly addressed (e.g., prevented, identified, reacted to, and adapted to)

Survivability

- **Survivability**
  - degree to which essential, mission-critical services continue to be provided in spite of either accidental or malicious harm

---

# Safety Domain

<table>
<thead>
<tr>
<th>Security concept</th>
<th>Safety concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Asset</td>
</tr>
<tr>
<td></td>
<td>• everything that could be considered as valuable to protect from harm</td>
</tr>
<tr>
<td></td>
<td>• Health safety, Property safety, Environment</td>
</tr>
<tr>
<td>Security criterion</td>
<td>Safety goal</td>
</tr>
<tr>
<td></td>
<td>• a target of safety level that is expected to meet by the information system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security concept</th>
<th>Safety concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Risk</td>
</tr>
<tr>
<td></td>
<td>• accidental harm to an asset that is possible to occur when accident happens due to ignoring vulnerability</td>
</tr>
<tr>
<td>Event</td>
<td>Accident</td>
</tr>
<tr>
<td></td>
<td>• Series of events or one single event resulting with harm to an asset that is unplanned and unintended of creating it</td>
</tr>
<tr>
<td>Impact</td>
<td>Harm</td>
</tr>
<tr>
<td></td>
<td>• Specific damage an asset gets because of a hazardous situation turning into reality and causing accidental situation</td>
</tr>
<tr>
<td>Threat</td>
<td>Hazard</td>
</tr>
<tr>
<td></td>
<td>• Situations that is potentially or actually increasing the chances of accidental situations</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Vulnerability</td>
</tr>
<tr>
<td></td>
<td>• Weak points in the system in terms of safety that is increasing the chance of possible accidental situation</td>
</tr>
<tr>
<td></td>
<td>• Occur due to design, implementation, architecture or deployment mistakes and result with harm to the asset</td>
</tr>
</tbody>
</table>
### Safety Domain

<table>
<thead>
<tr>
<th>Security concept</th>
<th>Safety concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk treatment</td>
<td>Safety sub factors</td>
</tr>
<tr>
<td></td>
<td>• asset protection</td>
</tr>
<tr>
<td></td>
<td>• safety incident detection</td>
</tr>
<tr>
<td></td>
<td>• safety incident reaction</td>
</tr>
<tr>
<td></td>
<td>• system adaptation</td>
</tr>
<tr>
<td>Security requirement</td>
<td>Safety requirement</td>
</tr>
<tr>
<td></td>
<td>• minimum needed measure of safety information system has to reach to ensure quality in terms of safety</td>
</tr>
<tr>
<td>Control</td>
<td>Safety mechanism</td>
</tr>
<tr>
<td></td>
<td>• architectural mechanism that aims to reduce chances of accidental situations by fulfilling safety requirements</td>
</tr>
</tbody>
</table>

---

![UML Diagram](attachment:uml_diagram.png)
Domain Model

- Harm
  - Accident
    - Hazard
    - Vulnerability
- Impact
- Event
  - Vulnerability
  - Threat
  - Threat agent
Example

Promotion policy:
- Changes every 30 minutes
- Directly connected to the incoming emails
- Updated according to the last received email within 30 minutes

Security criterion: Integrity of promotion policy

IS asset: email server, email client file container, cash desk(s)

Example

Threat agent: Insider
- aware of Promotion policy setup
- has access to Store client computer
- knows how to initiate virus program

Attack method:
- Install virus to store client
- Attack email client once the email server is down

Vulnerability: Email server down for more than 3 hours

Impact:
- Negation of Promotion policy integrity
- Harm to the Promotion policy
- Harm Email client, Store client computer
Summary

• Safety analysis
  • Privacy definition
  • Trust and Trustworthiness

• Unintentional
  – Accident, Hazard, Vulnerability, Harm

• Safety and Security are dependent for system defensibility

Outline

• Safety analysis
  • Privacy definition
  • Trust and Trustworthiness
What is Privacy?


- **Attacker** - interested in
  - monitoring what communication is occurring
  - what patterns of communication exist
  - or even in manipulating the communication
• **Anonymity**
  
  – the subject is not identifiable within a set of subjects, the *anonymity set*
  
  – from an attacker’s perspective means that the attacker cannot sufficiently identify
  the subject within a set of subjects, the *anonymity set*

• **Unlinkability** of two or more *items of interest* (e.g., subjects, messages, actions, etc.)
  
  – from an attacker’s perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these *items of interest* are related or not.
• **Undetectability**
  – of an *item of interest* from an attacker’s perspective means that the attacker cannot sufficiently distinguish whether it exists or not

• **Unobservability**
  – *undetectability* of the *item of interest* against all subjects uninvolved in it
  – *anonymity* of the subject(s) involved in the *item of interest* even against the other subject(s) involved in that *item of interest*
Unobservability

- **Unobservability** of an **item of interest**
  - *undetectability* of the item of interest against all subjects uninvolved in it
  - *anonymity* of the subject(s) involved in the item of interest even against the other subject(s) involved in that item of interest

Pseudonymity

- **Pseudonymity** – the use of pseudonyms as identifiers
  - A *pseudonym* is an identifier of a subject other than one of the subject's real names
Summary

- Safety analysis
- **Privacy definition**
- Trust and Trustworthiness

Outline

- Safety analysis
- Privacy definition
- **Trust and Trustworthiness**
What is trust?

Firm belief in the reliability, truth, or ability of someone or something

• Trust
  – Attributable only towards intentional entities such as humans
  – Technology can be reliable at its best, not trusted

• Devices and software systems can be trusted only under assumption
  – They are perceived as intentional
  – Trust is directed towards the humans behind the systems and not the systems itself

Source: Adapted from Mouratidis, ABPSM 2011

What is trust?

Are humans willing to trust software systems, as they trust other humans, knowing that there are potential risks?

• Trust
  – Attributable only towards intentional entities such as humans
  – Technology can be reliable at its best, not trusted

• Devices and software systems can be trusted only under assumption
  – They are perceived as intentional
  – Trust is directed towards the humans behind the systems and not the systems itself

Source: Adapted from Mouratidis, ABPSM 2011
What is trust?

Firm belief in the reliability, truth, or ability of someone or something

- Trust
  - Attributable only towards intentional entities such as humans
  - Technology can be reliable at its best, not trusted
- Devices and software systems can be trusted only under assumption
  - They are perceived as intentional
  - Trust is directed towards the humans behind the systems and not the systems itself

Are humans willing to trust software systems, as they trust other humans, knowing that there are potential risks?

E-commerce  E-prescription
Electronic banking  i-voting

Trustworthiness
deserving of trust or confidence; dependable, reliable

- Trust is based on the perception of the trustor about the trustworthiness of the trustee
  - Estimation of trustworthy characteristics he has according to the trustor

Source: Adapted from Mouratidis, ABPSM 2011
**Trust** is based on the perception of the *trustor* about the *trustworthiness* of the *trustee* – Estimation of trustworthy characteristics he has according to the trustor

**Trust modelling**

- Trust is the positive expectation of one actor, the trustor, about the behaviour of another actor, the trustee, by whom he might be positively or negatively affected.
  - Trust is a characteristic of the trustor
  - Trustworthiness is a characteristic on the trustee
• Early requirements analysis
• Late requirements analysis
• Architectural design
• Detailed design

• **Actor modeling**
  – actors of the environment and the system’s actors and analyzes their goals

• **Functional dependency modeling**
  – how actors depend on one another for obtaining services

• **Permission trust modeling**
  – identify actors who trust other actors for services, and actors which own services

• **Permission delegation modeling**
  – identifying actors who delegate to other actors the permission on services

Source: Adapted from Giorgini et al., 2004
Early Requirements Functional Model

Early Requirements trust model

*Source: Adapted from Giorgini et al., 2004*
Early Requirements
Trust Management Implementation

Goal diagrams
Late Requirements
Functional Model

Source: Adapted from Giorgini et al., 2004

Late Requirements trust model

Source: Adapted from Giorgini et al., 2004
Late Requirements
Trust Management Implementation

Goal diagram for Medical IT system

Source: Adapted from Giorgini et al., 2004
Summary

• Safety analysis
• Privacy definition
• Trust and Trustworthiness

Trust is based on the perception of the trustor about the trustworthiness of the trustee

What we have learnt today?

• Safety analysis
• Privacy definition
• Trust and Trustworthiness