Introduction to Secure System Modelling

Raimundas Matulevičius

Institute of Computer Sciences
University of Tartu
Goal

Introduce the bases used in the remaining of the course. This includes

Definition of the system and security engineering
Overview of few security and security modelling and different modelling perspectives
Motivation

Software-intensive systems play an important role in different areas of human life

**Confidentiality, Integrity, and Availability**

The need to secure information becomes a necessity than an option
What is the System?

“A system is a set of correlated phenomenon, which itself is a phenomenon. Each phenomenon that is contained in the system is part of the system”

Software-Intensive System

Infrastructure

Component

Applications

IT staff

Customer and external user

Internal user and management

Environment

How to break encrypted message?
How to break encrypted message?

Acquire massive amount of computing power and brute-force all the possible combinations of the encrypted key (Attacker's dream scenario)
**How to break encrypted message?**

- Install **keylogger** or **trojanised** version of the message viewer
  - Remote control malware
  - Decrypted message could be read from computer’s memory or hard disk
How to break encrypted message?

<table>
<thead>
<tr>
<th>Password</th>
<th>Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456</td>
<td>sunshine</td>
</tr>
<tr>
<td>12345678</td>
<td>ashley</td>
</tr>
<tr>
<td>qwerty</td>
<td>bailey</td>
</tr>
<tr>
<td>abc123</td>
<td>passw0rd</td>
</tr>
<tr>
<td>monkey</td>
<td>shadow</td>
</tr>
<tr>
<td>1234567</td>
<td>123123</td>
</tr>
<tr>
<td>letmein</td>
<td>654321</td>
</tr>
<tr>
<td>trustno1</td>
<td>superman</td>
</tr>
<tr>
<td>dragon</td>
<td>qazwsx</td>
</tr>
<tr>
<td>baseball</td>
<td>michael</td>
</tr>
<tr>
<td>111111</td>
<td>football</td>
</tr>
<tr>
<td>iloveyou</td>
<td></td>
</tr>
</tbody>
</table>
How to break encrypted message?

Just ask!

https://www.youtube.com/watch?v=opRMrEfAliI&app=desktop
Motivation
Security engineering
Security modelling
Security modelling perspectives
Running example
Table of Contents

Motivation
Security engineering
Security modelling
Security modelling perspectives
Running example
Security Engineering

Lowering the risk of intentional unauthorized harm to valuable assets to a level that is acceptable to the system’s stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks.

Lowering the risk of intentional unauthorized harm to valuable assets to level that is acceptable to the system’s stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks.

Different from safety, values must be protected. There is no 100% security. Different risk forms.

Security Engineering

Standards
ISO/IEC 2700x series
NIST special publication
BSI standard 100 for information security
Common criteria
...

Techniques
Misuse cases
Mal-activity diagrams
SecureUML
UMLsec
Agile security requirements engineering
...

Frameworks
Framework for security requirements engineering: representation and analysis
Security-by-ontology: a knowledge-centric approach
...

Processes
CC-based security engineering process
Security requirements for software product lines
Requirements reuse for improving system security
...

Methods
Secure Tropos
SQUARE
SREBP
...
Table of Contents

Motivation
Security engineering
Security modelling
Security modelling perspectives
Running example
A model is assumed to be simpler, resemble, and have the same structure and way of functioning as the phenomena it represents

Language

A set of symbols

Syntax – the graphemes being the smallest units capable of causing contrast in meaning, a set of words constituting the vocabulary, rules to form sentences

Semantics – agreed definitions of what the different sentences mean

Professional language is used by a set of persons working in a certain kind of area or in a scientific discipline

### Passenger Check-in Process

**Tabular analysis**

<table>
<thead>
<tr>
<th>System asset</th>
<th>Passenger, Transmission channel, Check-in System Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability</td>
<td>Transmission can be intercepted</td>
</tr>
<tr>
<td>Threat</td>
<td>An attacker (1) intercepts transfer, (2) modifies passenger info and passes to the Check-in System Server, (3) reads and keeps boarding pass</td>
</tr>
<tr>
<td>Impact</td>
<td>Loss of integrity of Passenger info, Loss of confidentiality of the boarding pass. Harm to the Check-in process reliability. Harm to the Passenger’s info and Boarding pass</td>
</tr>
<tr>
<td>Risk</td>
<td>An attacker intercepts transfer and modifies passenger info and passes to the Check-in System Server, thus leading to the loss of integrity of Passenger info, and then reads and keeps boarding pass thus leading to the loss of confidentiality of the boarding pass.</td>
</tr>
</tbody>
</table>
## Passenger Check-in Process
### Tabular analysis

<table>
<thead>
<tr>
<th>System asset</th>
<th>Passenger, Transmission channel, Check-in System Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Transmission can be intercepted</td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>An attacker (1) intercepts transfer, (2) modifies passenger info and passes to the Check-in System Server, (3) reads and keeps boarding pass</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>Loss of integrity of Passenger info, Loss of confidentiality of the boarding pass. Harm to the Check-in process reliability. Harm to the Passenger’s info and Boarding pass</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>An attacker intercepts transfer and modifies passenger info and passes to the Check-in System Server, thus leading to the loss of integrity of Passenger info, and then reads and keeps boarding pass thus leading to the loss of confidentiality of the boarding pass.</td>
</tr>
</tbody>
</table>
An attacker intercepts transfer and modifies passenger info and passes to the Check-in System Server, thus leading to the loss of integrity of Passenger info, and then reads and keeps boarding pass thus leading to the loss of confidentiality of the boarding pass.
## Language alignment Domain of Security Risk Management

<table>
<thead>
<tr>
<th>ISSRM</th>
<th>BPMN constructs</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Combination of Flow Objects (Event, Gateway, Tasks) using sequence flow. For Business assets: 8 For IS assets: 9</td>
<td></td>
</tr>
<tr>
<td>Business asset</td>
<td>Data object</td>
<td>Data Object</td>
</tr>
<tr>
<td>IS asset</td>
<td>a) Data store&lt;br&gt;b) Containers (Pool and Lanes)</td>
<td></td>
</tr>
<tr>
<td>Supports</td>
<td>a) Container (IS asset) supports combination of Flow Objects (Business assets) by containing them.&lt;br&gt;b) Sequence flow between Flow Objects (IS assets) and Flow Objects (Business assets)&lt;br&gt;c) Data Association Flow between Task (IS asset) and Data Object (Business asset) and between Data Store (IS asset) and Task (Business asset)</td>
<td></td>
</tr>
<tr>
<td>Constraint of</td>
<td>a) Lock and Association Flow, which point from the Lock to an Annotation.&lt;br&gt;b) Lock is a property of constructs that describe Business assets (Data Objects and Tasks)</td>
<td></td>
</tr>
<tr>
<td>Security objective</td>
<td>Is a property of a Lock that can have a value: c – confidentiality, i – integrity, and a – availability</td>
<td></td>
</tr>
<tr>
<td>Security criterion</td>
<td>Annotation</td>
<td>Annotation</td>
</tr>
</tbody>
</table>

Risk modelling constructs

<table>
<thead>
<tr>
<th>ISSRM</th>
<th>BPMN constructs</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk</strong></td>
<td>Combination of Event and Impact</td>
<td></td>
</tr>
<tr>
<td><strong>Event</strong></td>
<td>Combination of constructs for Threat and Vulnerability</td>
<td></td>
</tr>
<tr>
<td><strong>Targets / leads to (harm of IS assets)</strong></td>
<td>a) Sequence Flow from Flow Objects (Attack method) to Flow Objects (IS assets). b) Data Association Flow from Task (Attack method) to Data Store (IS asset).</td>
<td></td>
</tr>
<tr>
<td><strong>Leads to harm of Business assets</strong></td>
<td>a) Sequence Flow from Flow Objects (Attack method) to Flow Objects (Business assets). b) Data Association Flow from Task (Attack method) to Data Object (Business asset).</td>
<td></td>
</tr>
<tr>
<td><strong>Impact / negates / harms</strong></td>
<td>a) Unlock b) Unlock is a property of constructs that describe the Business assets</td>
<td></td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>Combination of construct for Threat Agent and Attack method</td>
<td></td>
</tr>
<tr>
<td><strong>Vulnerability</strong></td>
<td>Annotation</td>
<td></td>
</tr>
<tr>
<td><strong>Characteristics of</strong></td>
<td>a) Vulnerability point and Association Flow that points to Annotation. b) Vulnerability point is a property of constructs that describe IS assets, i.e. Data Object and Task</td>
<td></td>
</tr>
<tr>
<td><strong>Threat agent</strong></td>
<td>Pool and Lane (Containers)</td>
<td></td>
</tr>
<tr>
<td><strong>Attack method</strong></td>
<td>Combination of Flow Objects (Event, Gateway, Task) using Sequence Flow and Data Flows</td>
<td></td>
</tr>
<tr>
<td><strong>Uses</strong></td>
<td>Data Flow</td>
<td></td>
</tr>
</tbody>
</table>

---

Countermeasure modelling constructs

Passenger Check-in Process

Security Risk-oriented BPMN

Passenger Check-in Process

Security Risk-oriented BPMN

Passenger Check-in Process

Security Risk-oriented BPMN

Filter input for special characters and keywords, use whitelist of acceptable inputs

Data access control (or Control of database signature changes)
Models serve as a bridge from the problem domain to the computer system domain.

Security models help reasoning why security countermeasures needs to be implemented.

Filter input for special characters and keywords, use whitelist of acceptable inputs.
Table of Contents

Motivation
Security engineering
Security modelling

Security modelling perspectives

Running example
Modelling Perspective

System model

Modelling Perspective

- Structural perspective
- Goal and rule perspective
- Functional perspective
- Actor and role perspective
- Behavioral perspective
- Topological perspective

Modelling Languages

Archimate

BPMN

KAOS

Tropos

System model

Use cases

Notations with topology

Security Modelling Languages

Security model

Security Modelling Languages

Security Modelling Languages

How security solutions changes business processes

What are stakeholder goals towards system security?
Security Modelling Languages

Security Risk-aware Archimate

KAOS extensions to security

Security oriented BPMN

Security model

Security Risk-aware Secure Tropos

What are anti-goals, which achievement should be avoided?

Security Modelling Languages

- Security Risk-aware Archimate
- Security Risk-aware BPMN
- Security Risk-aware Tropos
- KAOS extensions to security
- Security risk-oriented misuse cases

What security functions should be implemented in the system

Security Modelling Languages

- Security Risk-aware Archimate
- Security Risk-aware BPMN
- Security Risk-aware Secure Tropos
- Risk-oriented notations with topology
- KAOS extensions to security
- Security risk-oriented misuse cases

Security modelling is a multi-facet activity

- Allows stakeholders to communicate security concerns in the language they know
- Capture various security concerns through different viewpoints
- Enhances the security model
- Supports model-driven security approach
Concluding Remarks

Security risks – at different system layers

System, risk and countermeasure modelling visualize and explain valuable assets, system asset vulnerabilities and potential countermeasures

Security modelling perspectives explore and explain security risk impact at different system layers
Table of Contents

Motivation
Security engineering
Security modelling
Security modelling perspectives
Running example
Running example
Football Federation
Running example
Football Federation
Running example
Football Federation
Running example
Football Federation
Thank you!