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

Components:
- Infrastructure
- Applications
- Customer and external user
- Internal user and management
- IT staff
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>passwd0rd</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>lloveyou</td>
<td></td>
</tr>
</tbody>
</table>
How to break encrypted message?

Just ask!

https://www.youtube.com/watch?v=opRMrEfAlll&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 level that is acceptable to the system’s stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks.

Security Engineering

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 Values must be protected. There 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>
<thead>
<tr>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security engineering</td>
</tr>
<tr>
<td><strong>Security modelling</strong></td>
</tr>
<tr>
<td>Security modelling perspectives</td>
</tr>
<tr>
<td>Running example</td>
</tr>
</tbody>
</table>
“An abstraction externalised in a professional language

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><strong>System asset</strong></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>
### 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><strong>Asset</strong></td>
<td>Combination of Flow Objects (Event, Gateway, Tasks) using sequence flow.</td>
<td>![Asset diagram]</td>
</tr>
<tr>
<td>For Business assets</td>
<td>![Diagram for Business assets]</td>
<td></td>
</tr>
<tr>
<td>For IS assets</td>
<td>![Diagram for IS assets]</td>
<td></td>
</tr>
<tr>
<td><strong>Business asset</strong></td>
<td>Data object</td>
<td>![Diagram for Data object]</td>
</tr>
<tr>
<td><strong>IS asset</strong></td>
<td>a) Data store</td>
<td>![Diagram for Data store]</td>
</tr>
<tr>
<td></td>
<td>b) Containers (Pool and Lanes)</td>
<td>![Diagram for Containers]</td>
</tr>
<tr>
<td><strong>Supports</strong></td>
<td>a) Container (IS asset) supports combination of Flow Objects (Business assets) by containing them.</td>
<td>![Diagram for Supports]</td>
</tr>
<tr>
<td></td>
<td>b) Sequence flow between Flow Objects (IS assets) and Flow Objects (Business assets)</td>
<td>![Diagram for Sequence flow]</td>
</tr>
<tr>
<td></td>
<td>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>![Diagram for Data Association]</td>
</tr>
<tr>
<td><strong>Constraint of</strong></td>
<td>a) Lock and Association Flow, which point from the Lock to an Annotation.</td>
<td>![Diagram for Constraint of]</td>
</tr>
<tr>
<td></td>
<td>b) Lock is a property of constructs that describe Business assets (Data Objects and Tasks)</td>
<td>![Diagram for Lock and Association Flow]</td>
</tr>
<tr>
<td><strong>Security objective</strong></td>
<td>Is a property of a Lock that can have a value: c – confidentiality, i – integrity, and a – availability</td>
<td>![Diagram for Security objective]</td>
</tr>
<tr>
<td><strong>Security criterion</strong></td>
<td>Annotation</td>
<td>![Diagram for Annotation]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISSRM</th>
<th>BPMN constructs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Combination of Flow Objects (Event, Gateway, Tasks) using sequence flow.</td>
</tr>
<tr>
<td>Business asset</td>
<td>For Business assets, For IS asset</td>
</tr>
<tr>
<td>IS asset</td>
<td>Supports</td>
</tr>
<tr>
<td></td>
<td>a) Container (IS asset) supports combination of Flow Objects (Business assets) by containing them.</td>
</tr>
<tr>
<td></td>
<td>b) Sequence flow between Flow Objects (IS assets) and Flow Objects (Business assets)</td>
</tr>
<tr>
<td></td>
<td>c) Data Association Flow between Task (IS asset) and Data Object (Business asset) and between Data Store (IS asset) and Task (Business asset)</td>
</tr>
<tr>
<td>Constraint of</td>
<td>a) Lock and Association Flow, which point from the Lock to an Annotation.</td>
</tr>
<tr>
<td></td>
<td>b) Lock is a property of constructs that describe Business assets (Data Objects and Tasks)</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>
</tr>
<tr>
<td>Security criterion</td>
<td>Annotation</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ISSRM</th>
<th>BPMN constructs</th>
<th>Concrete syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Combination of Event and Impact</td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Combination of constructs for Threat and Vulnerability</td>
<td></td>
</tr>
<tr>
<td>Targets / leads to (harm of IS assets)</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>a)</td>
</tr>
<tr>
<td>Leads to harm of Business assets</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>b)</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

Encryption algorithm

Check algorithm

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

Data access control (or Control of database signature changes)

Firewall, DoS Defense System

1. Enter booking number
2. Fill in required information
3. M1.SRP2a.1 Make passenger info unreadable to attacker
4. M1.SRP2b.1 Calculate checksum of passenger info
5. Send check-in information and checksum
6. Check booking number
7. M1.SRP3a.1 Filter passenger info
8. M1.SRP2a.2 Make passenger info readable
9. M1.SRP2b.2 Verify integrity of passenger info
10. Request valid?
11. YES
12. Request discarded
13. Passenger info checksum
14. Request discarded
15. Passenger info
16. M1.SRP2c.1 Make passenger info invisible
17. Check booking number
18. YES
19. M1.SRP3c.1 Make passenger info invisible
20. Store passenger information
21. Issue boarding pass
22. Send boarding pass and checksum
23. M1.SRP4a.1 Check for abnormal request
24. Received
25. M1.SRP5a.1 Monitor data store for malicious changes
26. YES
27. Boarding pass
28. Boarding pass integral?
29. YES
30. Check-in completed
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
- Functional perspective
- Behavioral perspective
- Goal and rule perspective
- Actor and role perspective
- Topological perspective

Modelling Languages

- Archimate
- BPMN

System model

- KAOS
- Tropos

Use cases

Notations with topology

Security Modelling Languages

Security model

Security Modelling Languages

Security Risk-aware Archimate

Security model

How security solutions affect system architecture

Security Modelling Languages

Security Risk-aware Archimate

Security risk-oriented BPMN

Security model

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 Risk-aware Secure Tropos

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

Security Modelling Languages

What security functions should be implemented in the system

Security Risk-aware Archimate

KAOS extensions to security

Security risk-oriented BPMN

Security Risk-aware Secure Tropos

Security risk-oriented misuse cases

Security Modelling Languages

Security Modelling Languages include:

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

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

ENVIRONMENT

Team Representative
Umpire

Other system in environment

USER INTERFACE

Information Processing System

DATABASE

ERIS

Other system in Football Federation
Other system in Football Federation

Football Federation Employee
Administrator

FOOTBALL FEDERATION

© Springer International Publishing AG 2017
Running example

Football Federation

Umpire
-umpireInfo
-umpireAccess
-assignedGames

Game
-gameInfo
-gameReport
-confirmation

Player
-playerInfo
-playerPerformance

consists of

Team
-teamInfo
-teamRep
-participationDecision
-regionAndLeague

consists of

Timetable
-timeTableInfo
-schedule
-timetableConfirmation

assigned to
plays in
reported in
included to

1 1
1
1

3-5
Running example
Football Federation
Running example
Football Federation
Thank you!