Security Analysis
Part I: Basics

Ketil Stølen, SINTEF & UiO
Acknowledgments

- The research for the contents of this tutorial has partly been funded by the European Commission through the FP7 project SecureChange and the FP7 network of excellence NESSoS
Objectives for the three Lectures on Security Analysis

- Classify security concepts
- Introduce, motivate and explain a basic apparatus for risk management in general and risk analysis in particular
- Relate risk management to system development
- Describe the different processes that risk management involve
- Motivate and illustrate model-driven security risk analysis (or security analysis, for short)
- Demonstrate the use of risk analysis techniques
The three Lectures on Security Analysis

- Part I: Basics
- Part II: Example-Driven Walkthrough of the CORAS Method
- Part III: Change Management
Overview of Part I

- What is security?
- What is risk?
- What is risk management?
- Central terms
- What is CORAS?
- Main concepts
- The CORAS process
- Risk modeling
- Semantics
- Likelihood reasoning
- The CORAS tool
What is Security Analysis?

- Security analysis is a specialized form of risk analysis focusing on security risks
What is Security?

- **Confidentiality**: Only authorised actors have access to information.
- **Integrity**: Only authorised actors can change, create or delete information.
- **Availability**: Authorised actors have access to information they need when they need it.
- **Accountability**: It is possible to audit the sequence of events in the system.

**CORAS 7**
Security is more than Technology

- From a technical standpoint, security solutions are available – but what good is security if no one can use the systems?

- Security requires more than technical understanding

- Security problems are often of non-technical origin

- A sound security evaluation requires a uniform description of the system as a whole
  - how it is used, the surrounding organisation, etc.
Security – Part of System Development

- Security is traditionally added as an “afterthought”
  - Solutions often reactive rather than proactive
  - Security issues often solved in isolation
  - Costly redesign
  - Security not completely integrated

Enforcing security only at the end of the development process “by preventing certain behaviors...may result in a so useless system that the complete development effort would be wasted” [Mantel'01].

“It would be desirable to consider security aspects already in the design phase, before a system is actually implemented, since removing security flaws in the design phase saves cost and time” [Jürjens'02].
In what way is “Security” related to

- safety
- reliability
- dependability
- maintainability
- data protection
- privacy
- trustworthy
- trust
- public key infrastructure based on trusted third party
- authentication and authorization
<table>
<thead>
<tr>
<th>English</th>
<th>Norwegian</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset</td>
<td>aktivum (noe med verdi)</td>
</tr>
<tr>
<td>threat</td>
<td>trussel</td>
</tr>
<tr>
<td>unwanted incident</td>
<td>uønsket hendelse</td>
</tr>
<tr>
<td>risk</td>
<td>risiko</td>
</tr>
<tr>
<td>vulnerability</td>
<td>sårbarhet</td>
</tr>
<tr>
<td>consequence</td>
<td>konsekvens</td>
</tr>
<tr>
<td>probability</td>
<td>sannsynlighet</td>
</tr>
<tr>
<td>frequency</td>
<td>frekvens/hyppighet</td>
</tr>
<tr>
<td>treatment</td>
<td>behandling</td>
</tr>
</tbody>
</table>
What is Risk?

- Many kinds of risk
  - Contractual risk
  - Economic risk
  - Operational risk
  - Environmental risk
  - Health risk
  - Political risk
  - Legal risk
  - Security risk
**Definition of Risk from ISO 31000**

- **Risk**: Effect of uncertainty on objectives
  - NOTE 1 An effect is a deviation from the expected — positive and/or negative
  - NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)
  - NOTE 3 Risk is often characterized by reference to potential *events* and **consequences**, or a combination of these
  - NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** of occurrence
  - NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood
What is Risk Management?

- Risk management: Coordinated activities to direct and control an organization with regard to risk [ISO 31000:2009]
Risk Analysis Involves

- Determining what can happen, why and how
- Systematic use of available information to determine the level of risk
- Prioritization by comparing the level of risk against predetermined criteria
- Selection and implementation of appropriate options for dealing with risk
Terms

Asset vulnerability threat risk

Need to introduce risk treatment

Reduced risk
Terms

Computer running Outlook

Vulnerability

Worm

Threat

Unwanted incident

Infected PC

Risk

- Infected twice per year
- Infected mail send to all contacts

Internet

Treatment

Install virus scanner
Security Analysis Using CORAS
Overview

- What is CORAS?
- Main concepts
- Process of eight steps
- Risk modeling
- Semantics
- Calculus
- Tool support
- Further reading
What is CORAS?

- **CORAS consists of**
  - Method for risk analysis
  - Language for risk modeling
  - Tool for editing diagrams

- **Stepwise, structured and systematic process**
  - Directed by assets
  - Concrete tasks with practical guidelines
  - Model-driven
    - Models as basis for analysis
    - Models as documentation of results

- **Based on international standards**
Main Concepts

- Asset
- Vulnerability
- Threat
- Unwanted incident
- Likelihood
- Consequence
- Risk
- Party
- Treatment
Definitions

- **Asset:** Something to which a party assigns value and hence for which the party requires protection
- **Consequence:** The impact of an unwanted incident on an asset in terms of harm or reduced asset value
- **Likelihood:** The frequency or probability of something to occur
- **Party:** An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- **Risk:** The likelihood of an unwanted incident and its consequence for a specific asset
- **Risk level:** The level or value of a risk as derived from its likelihood and consequence
- **Threat:** A potential cause of an unwanted incident
- **Treatment:** An appropriate measure to reduce risk level
- **Unwanted incident:** An event that harms or reduces the value of an asset
- **Vulnerability:** A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset
Exercise 1

- How would you represent risk in UML sequence diagrams?
# Process of Eight Steps

1. Preparations for the analysis  
2. Customer presentation of the target  
3. Refining the target description using asset diagrams  
4. Approval of the target description  
5. Risk identification using threat diagrams  
6. Risk estimation using threat diagrams  
7. Risk evaluation using risk diagrams  
8. Risk treatment using treatment diagrams

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Preparations for the analysis</td>
<td>Establish context</td>
</tr>
<tr>
<td>2</td>
<td>Customer presentation of the target</td>
<td>Assess risk</td>
</tr>
<tr>
<td>3</td>
<td>Refining the target description using asset diagrams</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Approval of the target description</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Risk identification using threat diagrams</td>
<td>Assess risk</td>
</tr>
<tr>
<td>6</td>
<td>Risk estimation using threat diagrams</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Risk evaluation using risk diagrams</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Risk treatment using treatment diagrams</td>
<td>Treat risk</td>
</tr>
</tbody>
</table>
Risk Modeling

- The CORAS language consists of five kinds of diagrams:
  - Asset diagrams
  - Threat diagrams
  - Risk diagrams
  - Treatment diagrams
  - Treatment overview diagrams

- Each kind supports concrete steps in the risk analysis process.

- In addition, there are three kinds of diagrams for specific needs:
  - High-level CORAS diagrams
  - Dependent CORAS diagrams
  - Legal CORAS diagrams
Example: Threat Diagram

**Threat Scenario:**
- **Threat:** Hacker
  - **Likelihood:** 0.1
- **Vulnerability:** Computer virus
  - **Virus protection not up to date**
- **Server is infected by computer virus**

**Threat:**
- **Virus creates back door to server**
  - **Likelihood:** 0.2
- **Server goes down**

**Consequence:**
- **Unwanted incident**
  - **Confidentiality of information:** high
  - **Integrity of server:** low
  - **Availability of server:** high
  - **Asset:** $
Semantics

- How to interpret and understand a CORAS diagram?
- Users need a precise and unambiguous explanation of the meaning of a given diagram

- Natural language semantics
  - CORAS comes with rules for systematic translation of any diagram into sentences in English

- Formal semantics
  - Semantics in terms of a probability space on traces
Example

- Elements
  - *Computer virus* is a non-human threat.
  - *Virus protection not up to date* is a vulnerability.
  - *Threat scenario* *Server is infected by computer virus occurs with likelihood* possible.
  - *Unwanted incident* *Server goes down occurs with likelihood* unlikely.
  - *Availability of server* is an asset.

- Relations
  - *Computer virus* exploits vulnerability *Virus protection not up to date* to initiate *Server is infected by computer virus* with undefined likelihood.
  - *Server is infected by computer virus* leads to *Server goes down* with conditional likelihood 0.2.
  - *Server goes down* impacts *Availability of server* with consequence high.
Calculus for Likelihood Reasoning

- Relation

\[
\frac{v_1(P_1)}{(v_1 \sqcap v_2)(P_1 \cdot P_2)} \quad \frac{P_2}{v_1 \rightarrow v_2}
\]

- Mutually exclusive vertices

\[
\frac{v_1(P_1)}{(v_1 \sqcup v_2)(P_1 + P_2)} \quad \frac{v_2(P_2)}{}
\]

- Statistically independent vertices

\[
\frac{v_1(P_1)}{(v_1 \sqcup v_2)(P_1 + P_2 - P_1 \cdot P_2)} \quad \frac{v_2(P_2)}{}
\]
Guidelines for Consistency Checking

How to check consistency of likelihoods in CORAS diagrams

**Exact values in complete diagrams**
- Assigned value: $v(p)$
- Calculated value: $v(p')$
- Consistency check: $p = p'$

**Exact values in incomplete diagrams**
- Assigned value: $v(p)$
- Calculated value: $v(p')$
- Consistency check: $p \geq p'$

**Intervals in complete diagrams**
- Assigned interval: $v([p_i, p_j])$
- Calculated interval: $v([p'_i, p'_j])$
- Consistency check: $[p'_i, p'_j] \subseteq [p_i, p_j]$ or, equivalently, $p_i \leq p'_i$ and $p_j \geq p'_j$

**Intervals in incomplete diagrams**
- Assigned interval: $v([p_i, p_j])$
- Calculated interval: $v([p'_i, p'_j])$
- Consistency check: $p_j \geq p'_j$
Tool Support

- The CORAS tool is a diagram editor
- Supports all kinds of CORAS diagrams
- Suited for on-the-fly modeling during workshops
- Ensures syntactic correctness
- May be used during all the steps of a risk analysis
  - Documents input to the various tasks
  - Selection and structuring of information during tasks
  - Documentation of analysis results
Screenshot

- Pull-down menu
- Tool bar
- Palette
- Canvas
- Outline
- Properties window

CORAS 32
Where to Find the Tool

- Open source
Mandatory Reading


Criticism from System Developers

- The CORAS language is too simplistic
- It is too cumbersome to use graphical icons
Criticism from Risk Analysts

- What’s new with the CORAS language?
- We have been using something similar for years, namely VISIO!
Exercise II

- Discuss the statements made by the critics?
- Argue why the critics are wrong.