Analysing Risk in Practice

The CORAS Approach to Model-Driven Risk Analysis

Bjørnar Solhaug

SECURWARE 2011-08-21

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

Contact

- Bjørnar Solhaug
- SINTEF ICT, Norway
- E-mail: Bjornar.Solhaug@sintef.no
- Web: www.sintef.no

Overview

- Part I Introduction – Risk management and the CORAS approach
- Part II Example-driven walkthrough of the CORAS method
- Part III Change management

Part I: Introduction

Risk Management and the CORAS Approach

Overview of Part I

- 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
- Further reading

What is Risk?

- Many kinds of risk
  - Contractual risk
  - Economic risk
  - Operational risk
  - Environmental risk
  - Health risk
  - Political risk
  - Legal risk
  - Security risk

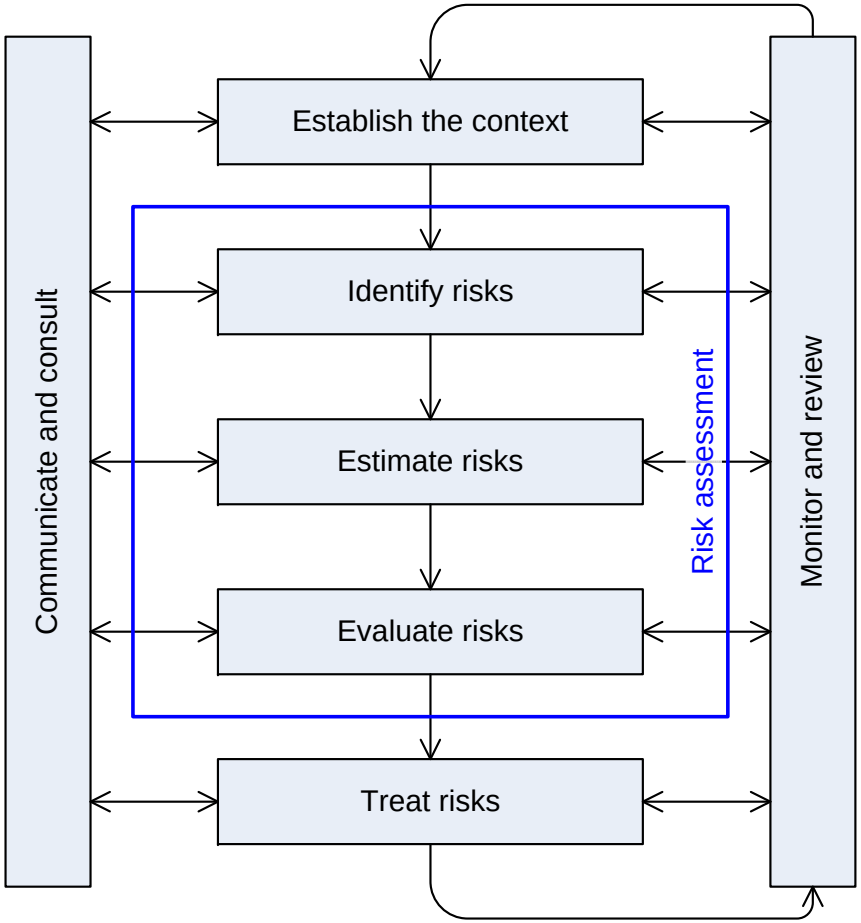
Definition of risk from ISO 31000

- **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?

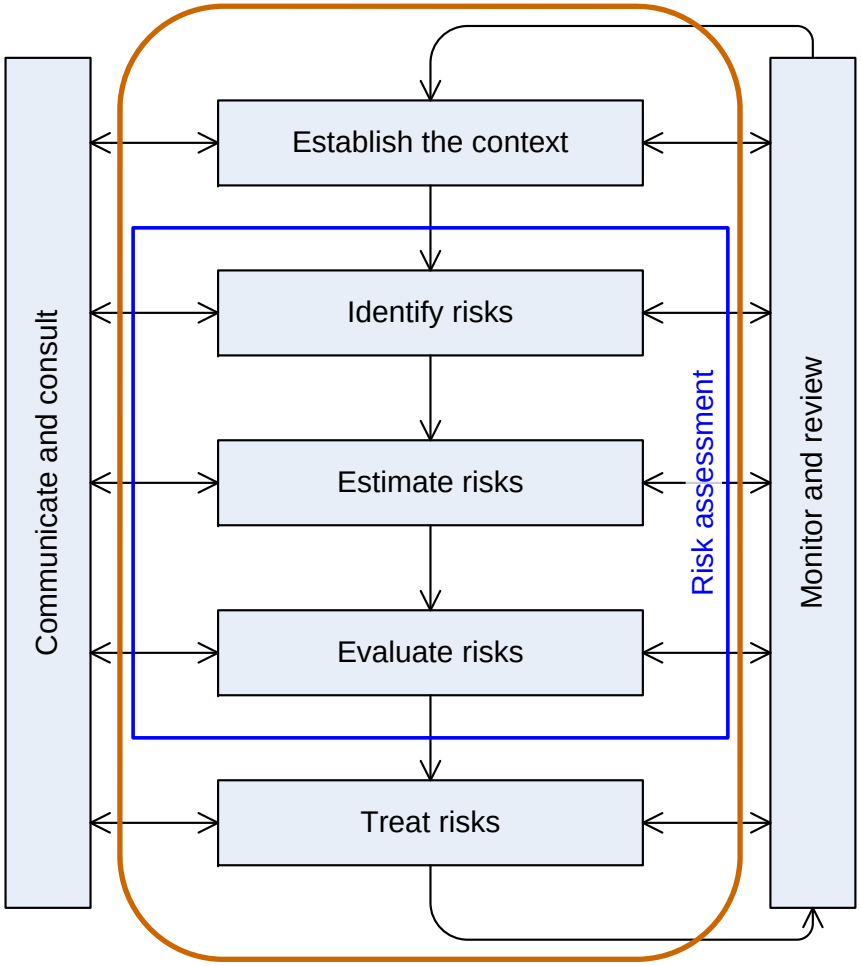
- **Risk management:** Coordinated activities to direct and control an organization with regard to **risk**

  [ISO 31000:2009]

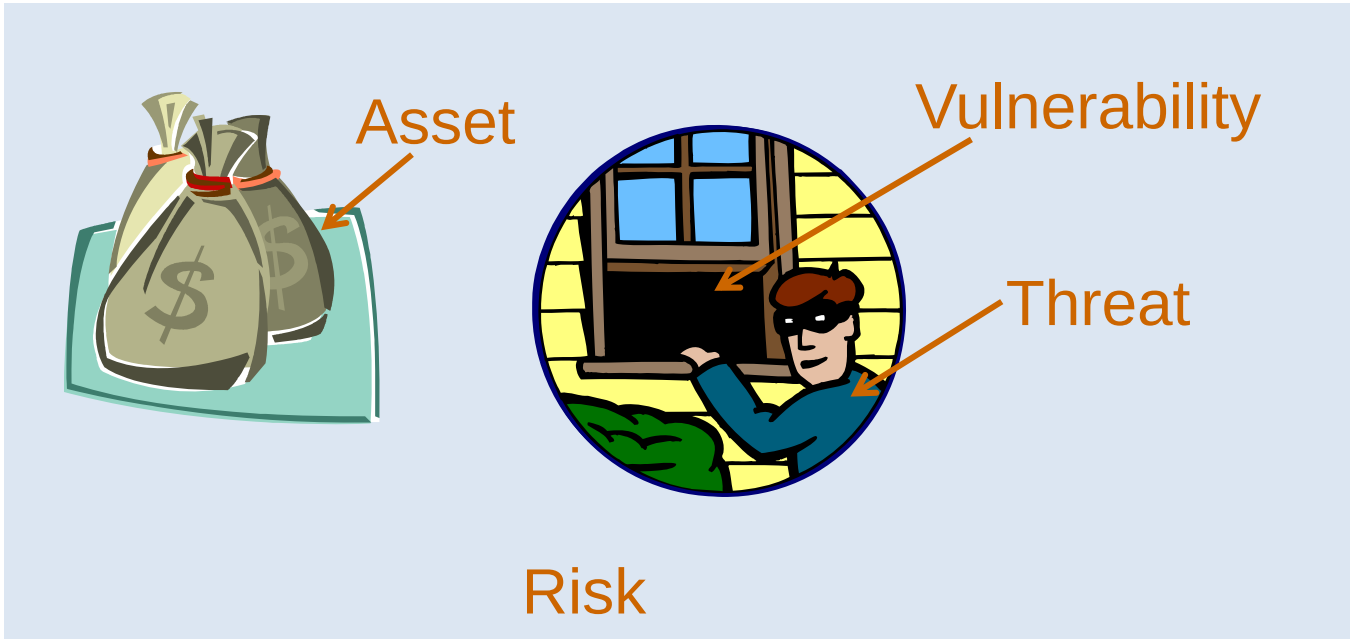


Risk Analysis Involves

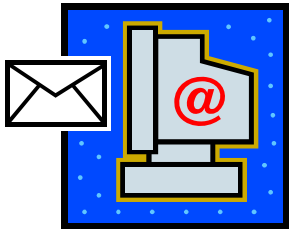
- Determining what can happen, why and how
- Systematic use of available information to determine the level of risk
- Prioritization by comparing the level of risk against predetermined criteria
- Selection and implementation of appropriate options for dealing with risk



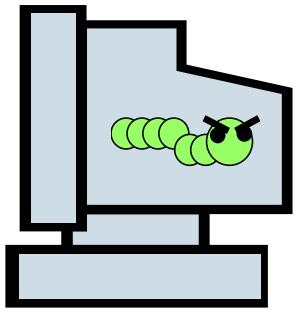
Terms


Asset
Vulnerability
Threat
Risk
Reduced risk
Need to introduce risk treatment

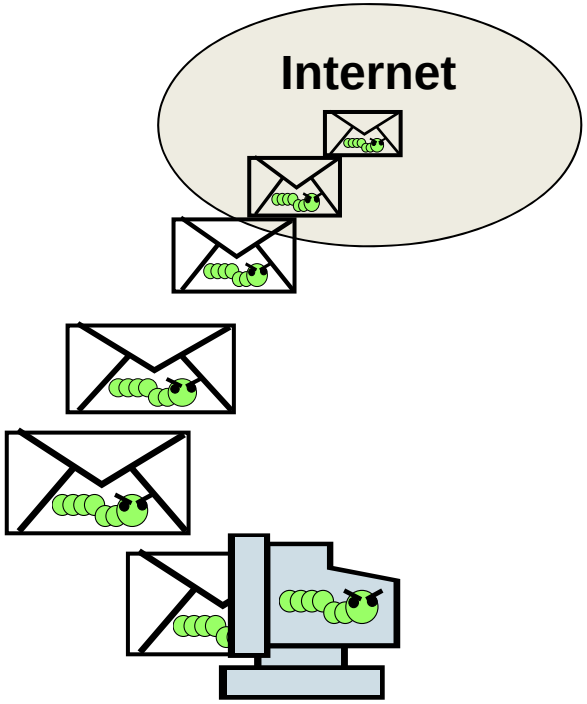
Terms



Computer running Outlook



Infected PC



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

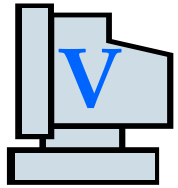
Vulnerability

Unwanted incident

Risk

Worm

Threat



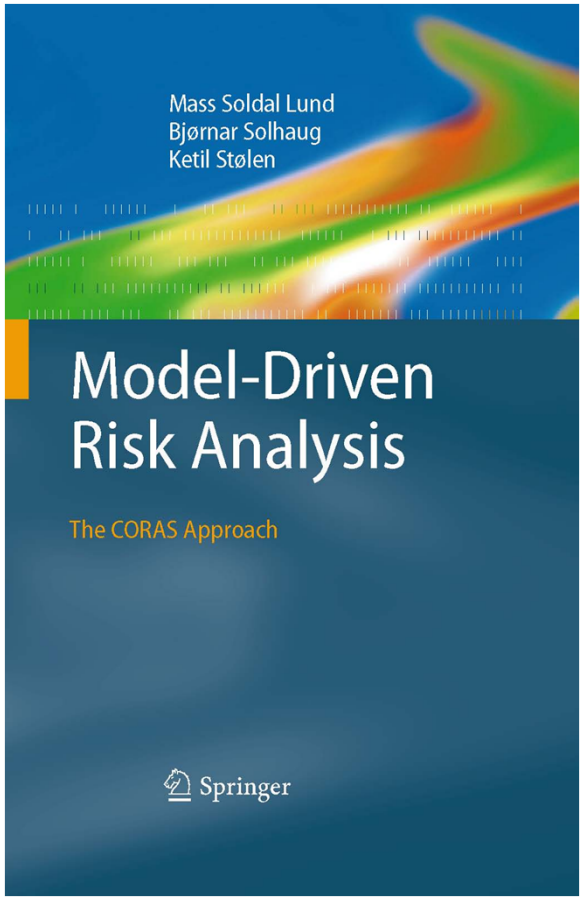
Install virus scanner

Treatment

Risk Analysis Using CORAS

Overview

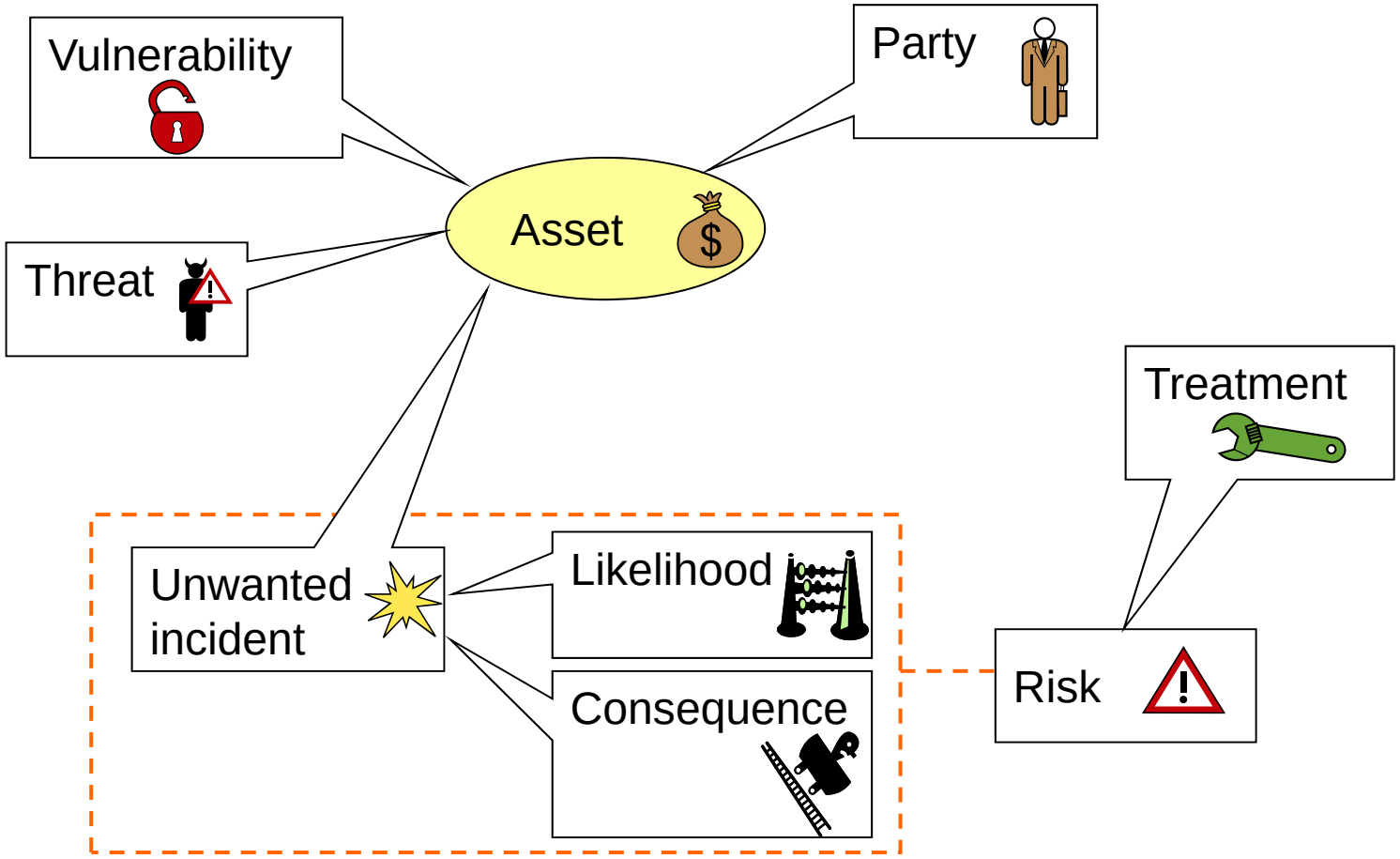
- What is CORAS?
- Main concepts
- Process of eight steps
- Risk modeling
- Semantics
- Calculus
- Tool support
- Further reading



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



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

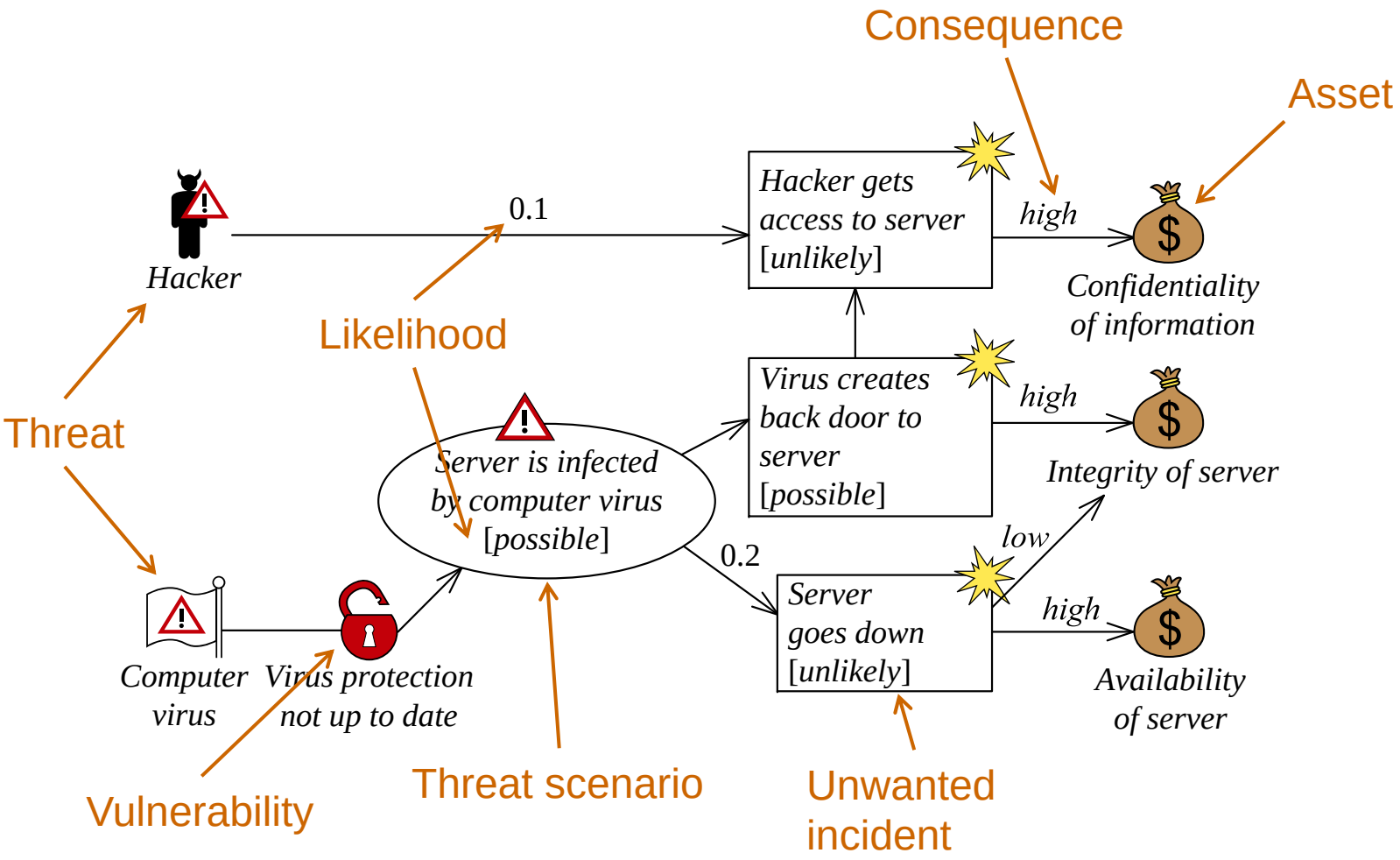
Process of Eight Steps

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	Establish context
5. Risk identification using threat diagrams 6. Risk estimation using threat diagrams 7. Risk evaluation using risk diagrams	Assess risk
8. Risk treatment using treatment diagrams	Treat risk

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

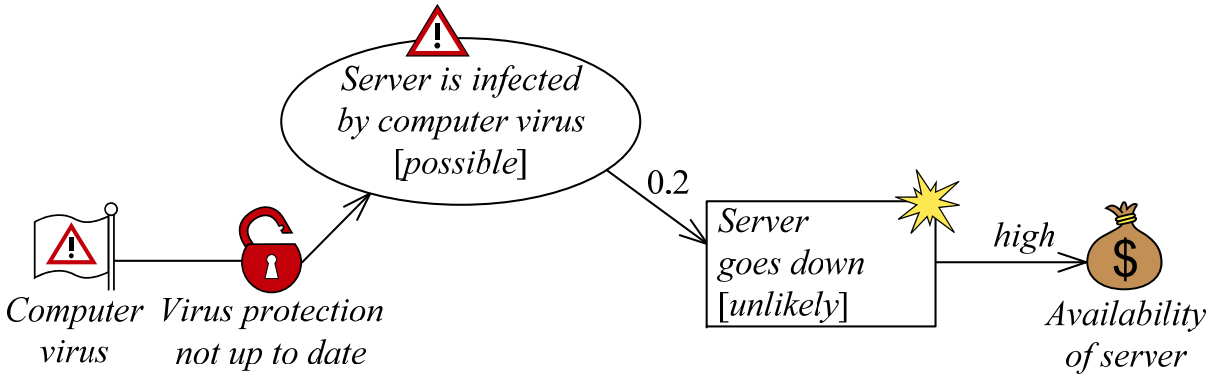


Semantics

- 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 $\dfrac{v_1(P_1) \quad v_1 \xrightarrow{P_2} v_2}{(v_1 \sqcap\!| \, v_2)(P_1 \cdot P_2)}$

- Mutually exclusive vertices $\dfrac{v_1(P_1) \quad v_2(P_2)}{(v_1 \sqcup v_2)(P_1 + P_2)}$

- Statistically independent vertices $\dfrac{v_1(P_1) \quad v_2(P_2)}{(v_1 \sqcup v_2)(P_1 + P_2 - P_1 \cdot P_2)}$

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: $v([p_i, p_j])$

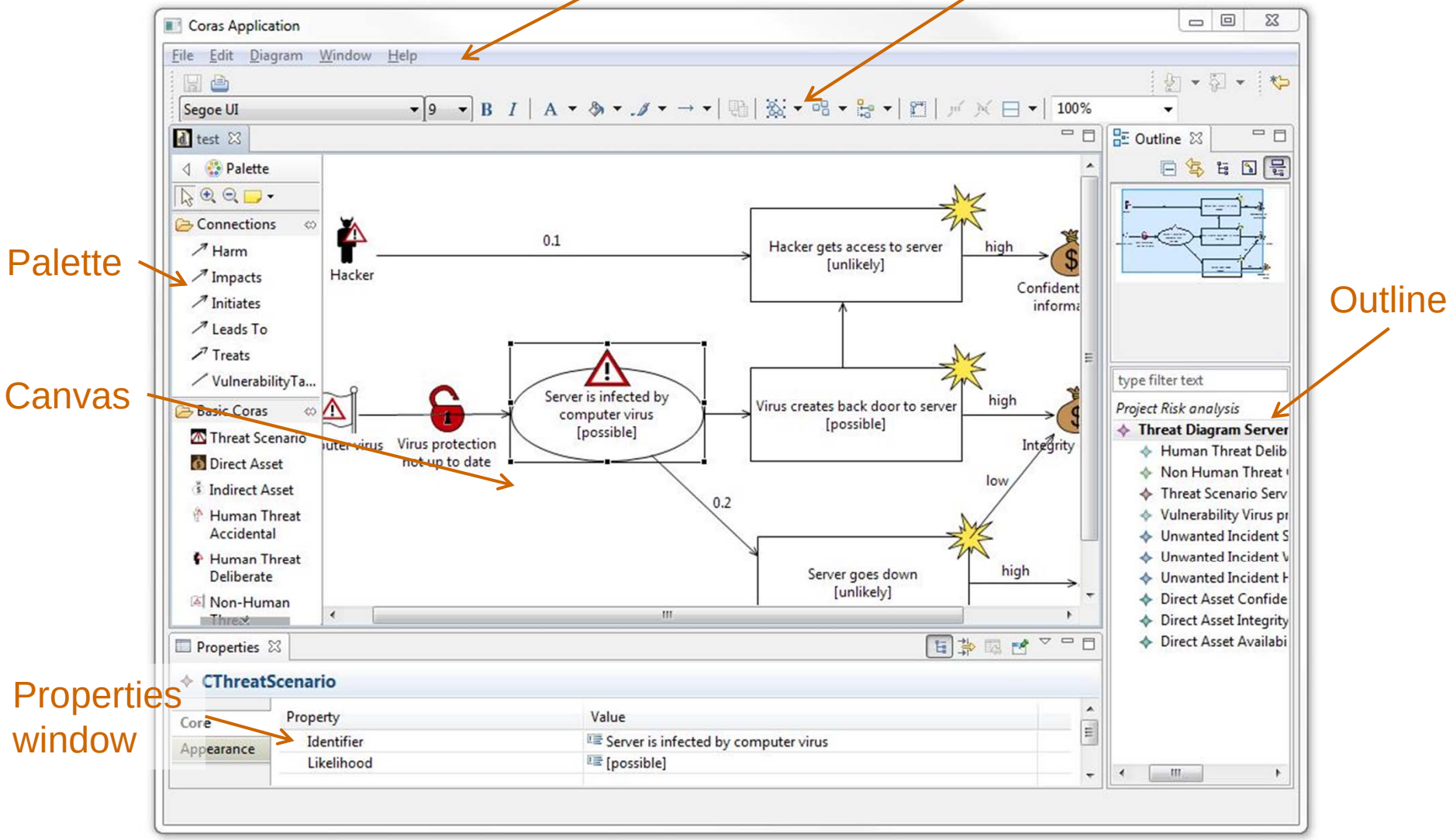
Calculated interval: $v([p'_i, p'_j])$

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
- Download: http://coras.sourceforge.net/

Screenshot


Pull-down menu
Tool bar
Palette
Canvas
Outline
Properties window
Coras Application
File Edit Diagram Window Help
Segoe UI
9
100%
test
Palette
Connections
Harm
Impacts
Initiates
Leads To
Treats
VulnerabilityTa...
Basic Coras
Threat Scenario
Direct Asset
Indirect Asset
Human Threat Accidental
Human Threat Deliberate
Non-Human
Hacker
0.1
Hacker gets access to server [unlikely]
high
Confident
Server is infected by computer virus [possible]
Virus protection not up to date
Virus creates back door to server [possible]
high
Integrity
low
0.2
Server goes down [unlikely]
high
Outline
type filter text
Project Risk analysis
Threat Diagram Server
Human Threat Delib
Non Human Threat
Threat Scenario Serv
Vulnerability Virus pr
Unwanted Incident S
Unwanted Incident V
Unwanted Incident H
Direct Asset Confide
Direct Asset Integrity
Direct Asset Availabi
Properties
CThreatScenario
Core
Appearance
Property
Value
Identifier
Server is infected by computer virus
Likelihood
[possible]

Further Reading

- Book:
  - www.springer.com/computer/swe/book/978-3-642-12322-1
  - Some chapters may be downloaded for free, including Chapter 3 which gives a Guided Tour of CORAS
- Tool:
  - http://coras.sourceforge.net/
  - Open source
- Formal semantics:
  - Gyrd Brændeland, Atle Refsdal, Ketil Stølen. Modular analysis and modelling of risk scenarios with dependencies. Journal of Systems and Software, volume 83, pages 1995-2013, Elsevier, 2010.