Model-Driven Risk Analysis
The CORAS Approach

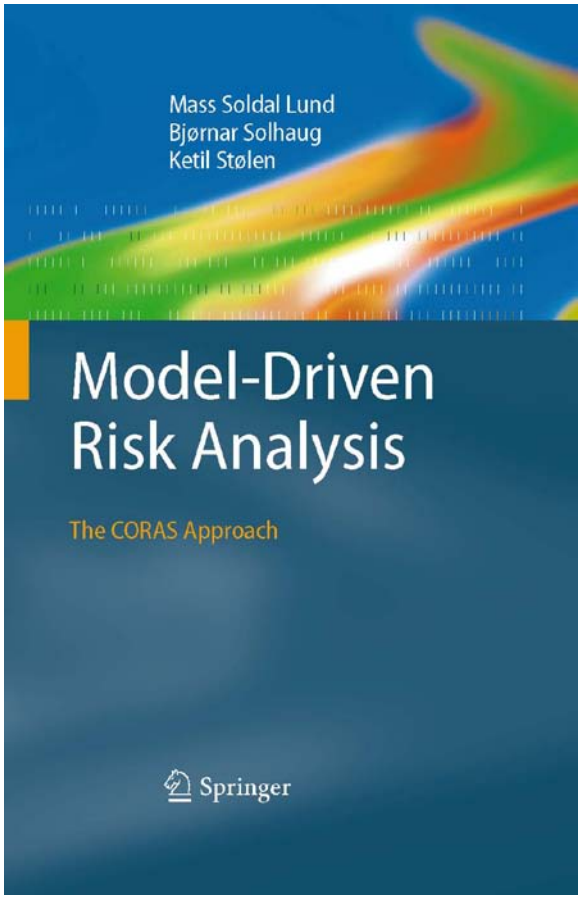
Bjørnar Solhaug

AF Security

18 February, 2011

Oversikt

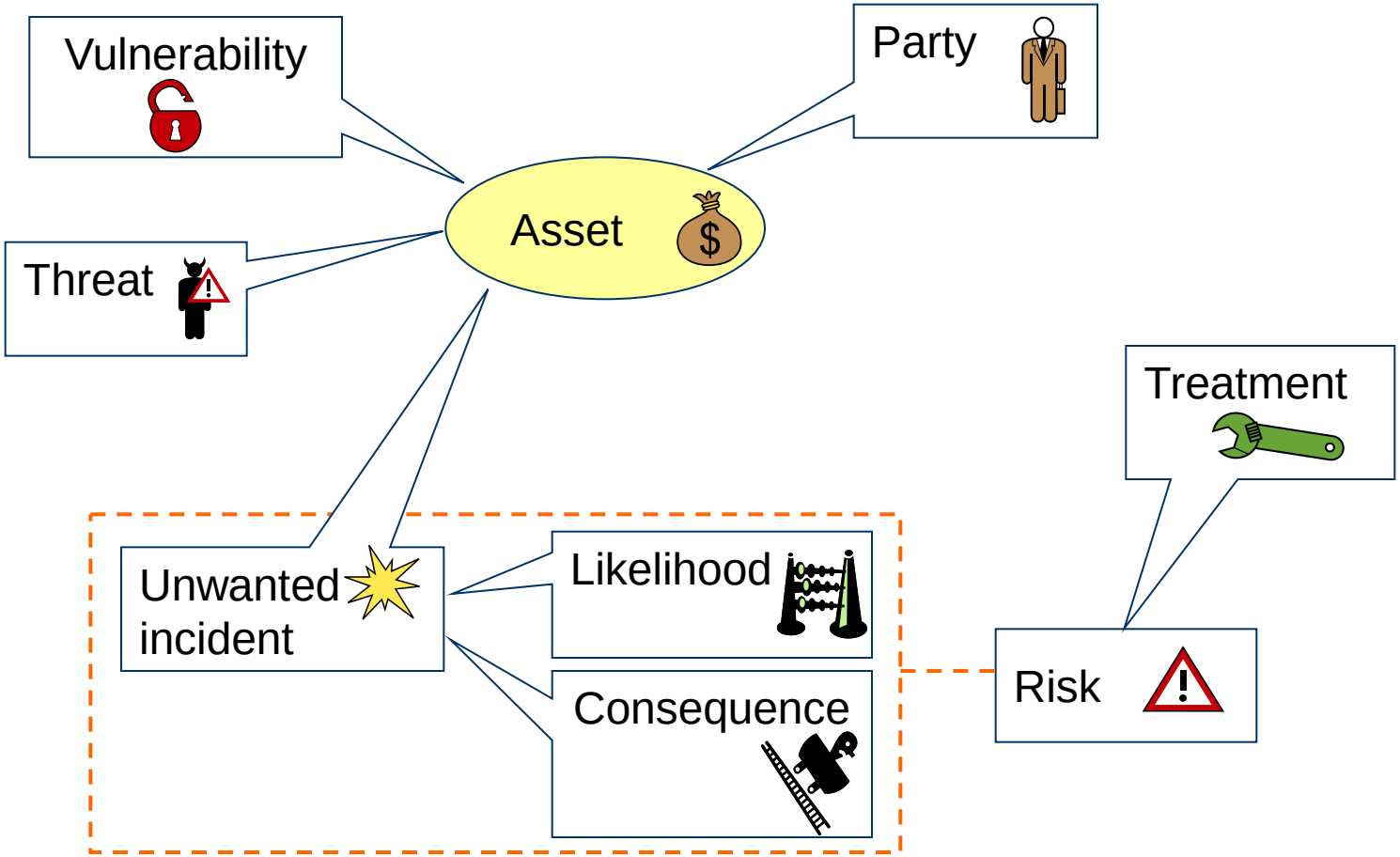
- What is CORAS?
- Central concepts
- The risk analysis process
- Risk modeling
- Semantics
- Tool support
- Summary



What is CORAS?

- CORAS consists of three tightly integrated parts
  - A method for risk analysis
  - A language for risk modeling
  - A tool to support the risk analysis process
- A stepwise, structured and systematic process
  - Asses-driven
  - Concrete tasks with practical guidelines
  - Model-driven
    - Models as basis for and input to analysis tasks
    - Models for documentation of results
- Based on internationally established standards

Central Concepts



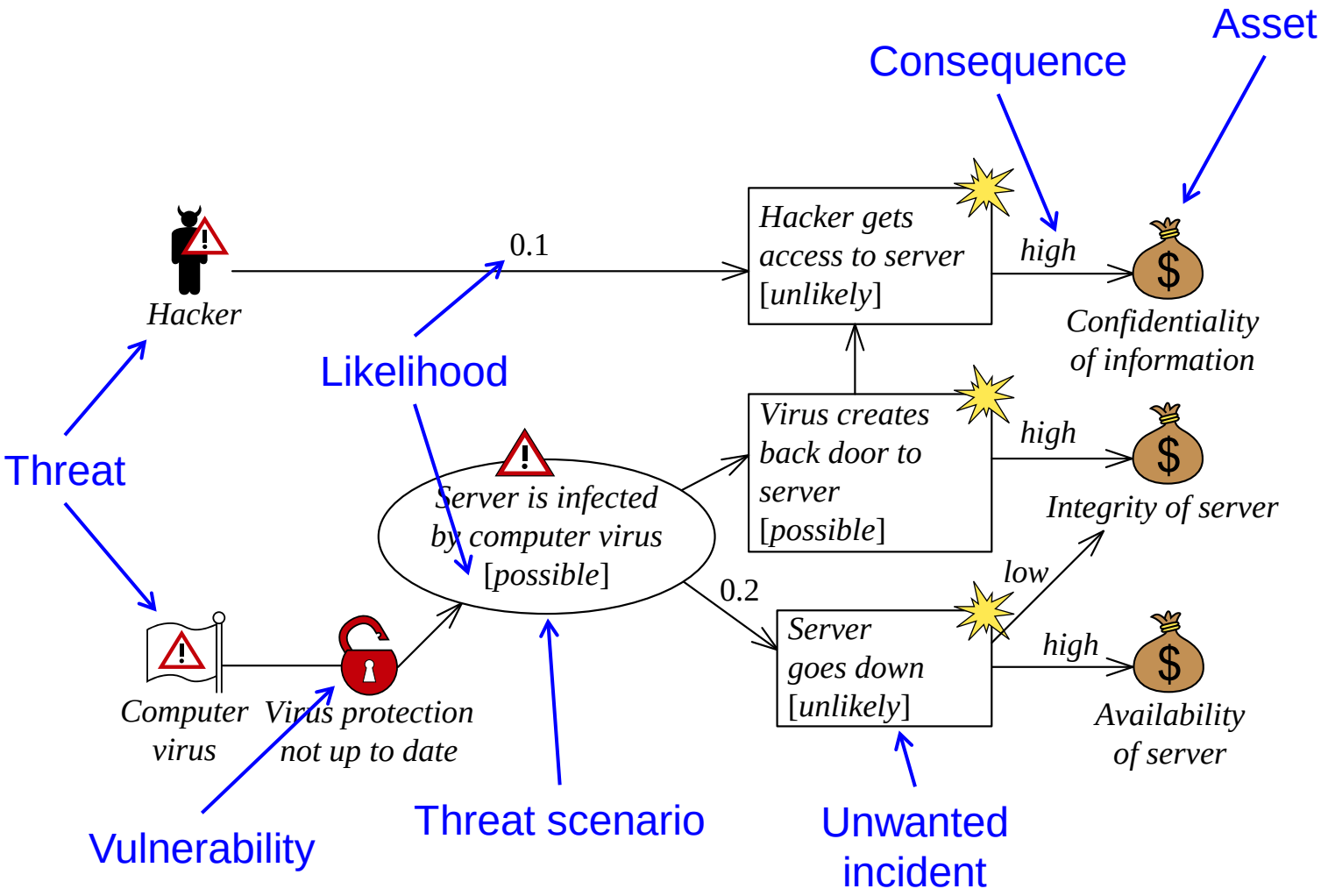
The Risk Analysis Process – 8 Steps

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	Context establishment
5. Risk identification using threat diagrams 6. Risk estimation using threat diagrams 7. Risk evaluation using risk diagrams	Risk analysis
8. Risk treatment using treatment diagrams	Risk treatment

Risk modeling

- The CORAS language consists of five kinds of diagrams
  - Asset diagrams
  - Threat diagrams
  - Risk diagrams
  - Treatment diagrams
  - Treatment overview diagrams
- Each kind of diagram supports specific steps of the risk analysis process
- Three further kinds of diagram for specific needs
  - High-level CORAS diagrams
  - Dependent CORAS diagrams
  - Legal CORAS diagrams

Example: Threat diagram

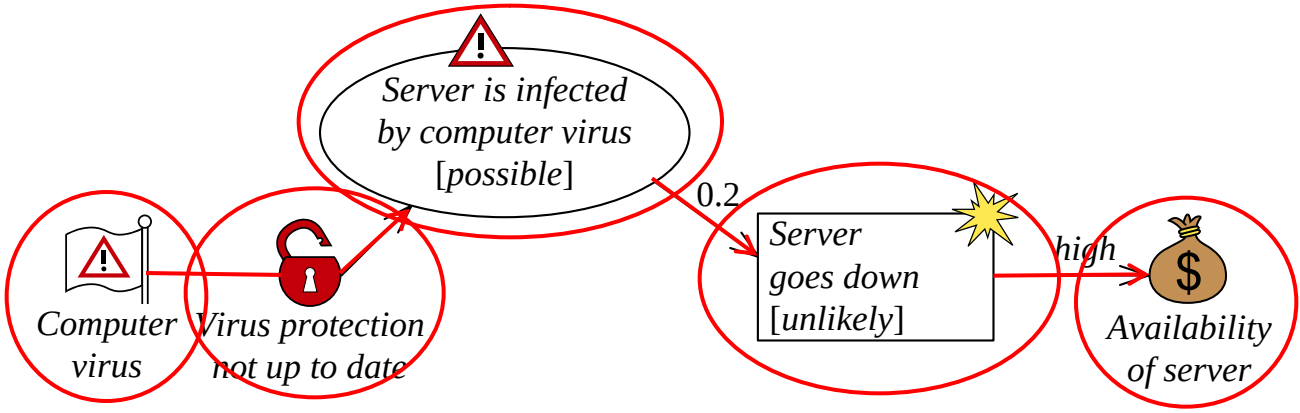


Semantics

- 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*.

Rules for Likelihood Calculation

Format of rules: $\dfrac{R_1 \quad R_2 \quad \ldots \; R_i}{C}$

Relation: $\dfrac{v_1(P_1) \quad v_1 \overset{P_2}{\rightarrow} v_2}{(v_1 \sqcap\!| \; v_2)(P_1 \cdot P_2)}$

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

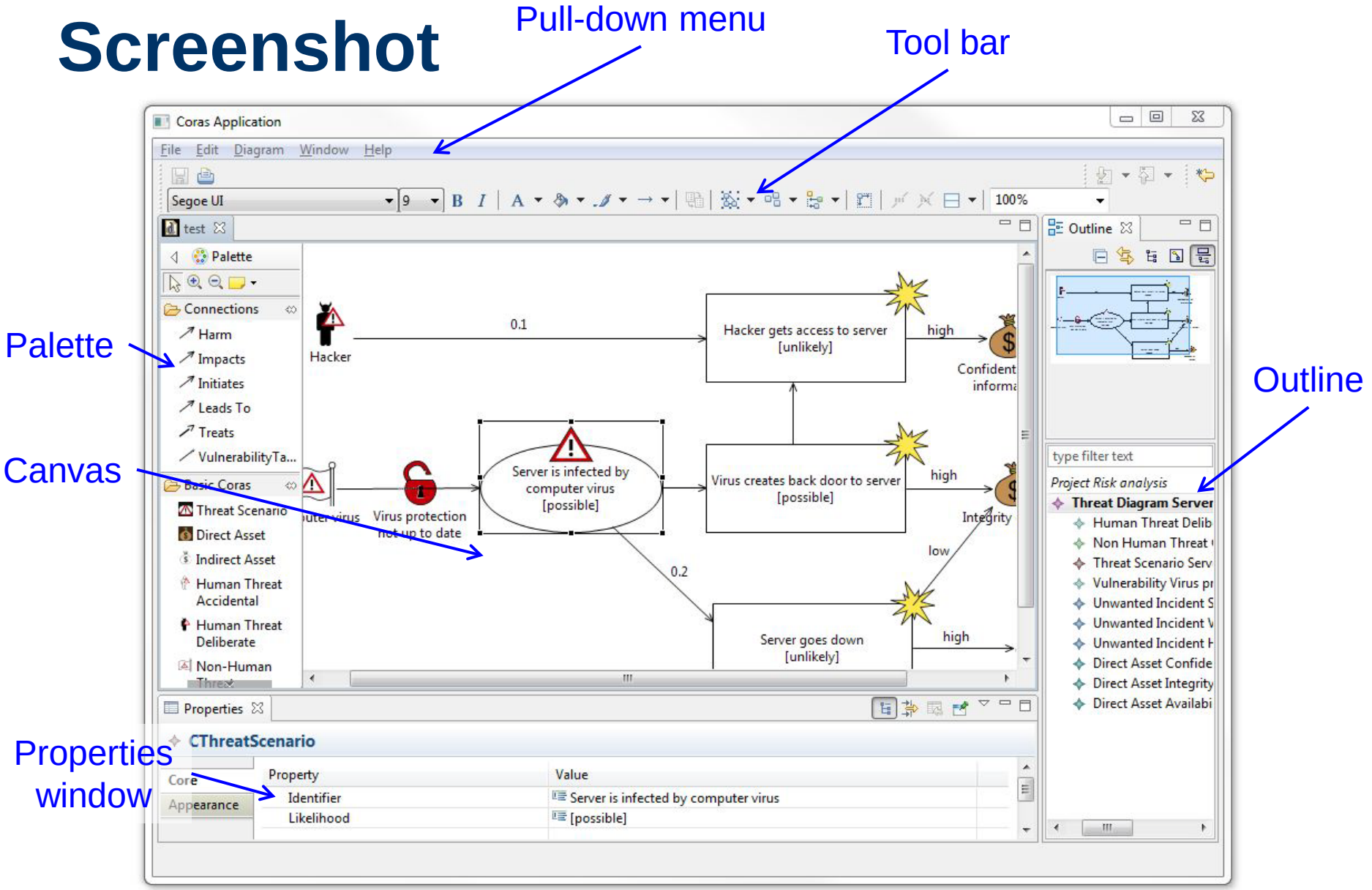
Statistically independent: $\dfrac{v_1(P_1) \quad v_2(P_2)}{(v_1 \sqcup v_2)(P_1 + P_2 - P_1 \cdot P_2)}$

Soundness theorem: $[[R_1]] \wedge [[R_2]] \wedge \ldots \wedge [[R_i]] \Rightarrow [[C]]$

Tool Support

- The CORAS tool is a diagram editor
- Support for making all kinds of CORAS diagrams
- Design for on-the-fly modeling during structured brainstorming at analysis workshops
- Ensures syntactically correct diagrams
- Used during all steps of the risk analysis
  - Input to the various tasks
  - Gathering and structuring of information during the tasks
  - Documentation of analysis results
- Available for 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 informa
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]

Summary

- CORAS consists of three parts
  - Method
  - Language
  - Tool
- Model-driven and asset-driven
- Concrete guidelines for how to conduct risk analysis in practice
- Based on a well-established and precisely defined conceptual framework
- Based on internationally established standards

- Book: http://www.springer.com/computer/swe/book/978-3-642-12322-1
- Home page: http://coras.sourceforge.net/