Security analysis: The CORAS Approach

October 15, 2010

Ketil Stølen, SINTEF & UiO
What is CORAS?

- The CORAS process
  - A process for security risk analysis
- The CORAS language (diagrams)
  - A graphical language that supports the analysis process
  - Basis for communication, documentation and analysis
- The CORAS semantics
  - A schematic translation of any CORAS diagram into English
- The CORAS calculus
  - A set of rules for reasoning about diagrams
- The CORAS editor
  - A computerized tool supporting the drawing of diagrams
- The CORAS guideline
  - A guideline for best use of the language within the process
The CORAS process
The CORAS process

Risk analysis process based on the standard ISO 31000: Risk Management – Principles and Guidelines
Context identification

- Characterise target of analysis
  - What is the focus and scope of the analysis?
- Identify and value assets
  - Asset-driven risk analysis process
  - Business oriented, e.g. availability of services generating revenue
- Specify risk evaluation criteria
  - What losses can the client tolerate?
  - Similar to requirements in system development
Risk identification

- Identify threats to assets through structured brainstorming
  - Involves decision makers, users, developers, domain experts, risk analysis experts, etc. (typically 5-7 people)

- Identify vulnerabilities of assets
  - Questionnaires and checklists

**Equipment physical security**
- Is equipment properly physically protected against unauthorised access to data or loss of data?
- Are power supplies handled in a manner that prevents loss of data and ensures availability?
- …
Risk evaluation

- We cannot eliminate all risks
- Determine which risks need treatment
  - We need to know how serious they are so we can prioritise

- Risk level is determined based on analysis of the frequency and consequence of the unwanted incident
  - Quantitative values: e.g., loss of 1M€, 25% chance per year
  - Qualitative values: e.g., high, medium, low
Risk treatment

- Identify treatments for unaccepted risks
- Evaluate and prioritise different treatments
Elements of security risk analysis

- Identify Context
- Identify Risks
- Estimate Risk Level
- Evaluate Risks
- Treat Risks

**Context**

- Vulnerability
- Threat

**Target**

- Asset
- Unwanted Incident

**Treatment**

- Frequency
- Consequence
- Risk
The CORAS language (diagrams)
The CORAS security risk modeling language

- Key symbols:
The CORAS diagrams

- **Asset diagrams**
  Describes the focus of the analysis

- **Threat diagrams**
  Describes scenarios which may cause harm to the assets

- **Risk diagrams**
  Summarises the risks presented in threat diagrams

- **Treatment diagrams**
  Adds proposed treatments to threat diagrams

- **Treatment overview diagrams**
  Adds proposed treatments to risk diagrams
Identifying and documenting assets

- **Asset:** *Something to which a party assigns value and hence for which the party requires protection*
- The client specifies its assets and risk acceptance levels
- Difficult, - faults may jeopardize the whole analysis
  - wrong focus
  - wrong level of details

![Diagram with Analysis client, Product information, Budget, and Business contracts]
Identifying and documenting assets

- One may also specify other interested parties than the client
  - Different parties may have different assets
  - Two parties may assign value to the same parts or aspects (e.g. confidentiality), but possibly with different priority (asset value) and different protection requirements

- Possible to specify how assets can depend on other assets
  - company reputation
  - income

Harm to Confidentiality may result in harm to Data protection
Identifying and documenting threats and unwanted incidents in threat diagrams

- **Threat:** A potential cause of an unwanted incident
- **Unwanted incident:** An event that harms or reduces the value of an asset

<table>
<thead>
<tr>
<th>Threat</th>
<th>Unwanted incident</th>
<th>Asset damaged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>Virus attack makes information unavailable</td>
<td>Business contracts</td>
</tr>
<tr>
<td>Virus</td>
<td>Virus attack makes information unavailable</td>
<td>Product information</td>
</tr>
<tr>
<td>Employee</td>
<td>Product information is accidentally published on the web</td>
<td>Product information</td>
</tr>
<tr>
<td>Insider</td>
<td>Competitor receives confidential information</td>
<td>Product information</td>
</tr>
<tr>
<td>Insider</td>
<td>Competitor receives confidential information</td>
<td>Budget</td>
</tr>
</tbody>
</table>
Identifying and documenting vulnerabilities and threat scenarios

- **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

- **Threat scenario**: A chain or series of events that is initiated by a threat and that may lead to an unwanted incident

- Forces the participants to specify “why” incidents can happen (vulnerabilities) and “how” (threat scenarios)

- Impossible or wrong paths are likely to be discovered
Identifying and documenting likelihoods and consequences

- **Likelihood**: *The frequency or probability of something to occur*
- **Consequence**: *The impact of an unwanted incident on an asset in terms of harm or reduced asset value*
- Capturing the rationale for the likelihood estimates
Documenting risks

- **Risk**: The likelihood of an unwanted incident and its consequence for a specific asset
- Compared to the party’s risk acceptance levels
- Acceptable and non-acceptable risks are shown in a risk diagram
  - decision makers
  - planning treatments
  - communicating risks
Identifying and documenting risk treatments

- Risks that are **unacceptable** are evaluated to identify appropriate treatments
- Risks that are **acceptable** can be removed from the diagram
Identifying and documenting risk treatments

**Risk treatment**: An appropriate measure to reduce risk level

- Treatments are added where they should have effect
Example CORAS diagrams
Example asset diagram

- **Party**
  - Company

- **Indirect asset**
  - Company’s reputation

- **Harm relation**
  - Integrity of server [high]
  - Confidentiality of information [critical]
  - Availability of server [critical]

- **Asset**
Example threat diagram

- Hacker
- Initiates relation
- Unwanted incident
- Consequence
- Hacker gets access to server
- [unlikely]
- Confidentiality of information
- High
- Virus creates back door to server
- [possible]
- Integrity of server
- High
- Server is infected by computer virus
- [possible]
- Server goes down
- [unlikely]
- Availability of server
- High
- Vulnerability
- Threat
- Leads-to relation
- Low
- Threat scenario
- Influence
- Virus protection not up to date
- Impacts relation
- Computer virus
- Low
Example risk diagram

HA: Hacker gets access to server [unacceptable]

VB: Virus creates back door to server [unacceptable]

SD1: Server goes down [unacceptable]

SD2: Server goes down [acceptable]

Confidentiality of information

Integrity of server

Availability of server

Risk

Risk level

Hacker

Leads-to relation

Computer virus

Initiates relation

Roles and relationships in the risk diagram:

- **Hacker**: Represents an external threat that gains access to the server.
- **Virus**: Represents an internal threat that creates a back door to the server.
- **Server**: Represents the target of the risk assessment.
- **Confidentiality of Information**: Indicates a loss of confidentiality.
- **Integrity of Server**: Indicates a loss of integrity.
- **Availability of Server**: Indicates an unavailability of the server.

The diagram illustrates the flow of risk from an external hacker, through the installation of a virus, leading to the server being compromised and potentially going down, impacting confidentiality, integrity, and availability.
Example treatment diagram
Example treatment overview diagram

ICT

Exam

p

Overview

diagram
The CORAS semantics
Building a threat diagram (1)
Building a threat diagram (2)

Unwanted incident

Corruption of data

Data integrity

Employee

Initiates relation

Impacts relation
Building a threat diagram (3)
Building a threat diagram (4)

How do we interpret this diagram?
How do we interpret CORAS diagrams?

In order to answer this question, we have

- Formulated a textual syntax
  - Defined by Extended BNF grammars
- Defined a structured semantics
  - STEP 1: Translation of a diagram into its textual representation
  - STEP 2: Translation of the textual representation into its meaning as a paragraph in English
Success criteria we defined for the CORAS semantics

- The semantics should be modular
- The translation should be easy to perform
- The resulting English sentences should be easily understandable
- The translation should be possible to automate
- It should be possible to translate any diagram
Semantics of the impact relation

\[ \text{[[ ui ]] := Unwanted incident } ui \text{ occurs with undefined likelihood.} \]
\[ \text{[[ a ]] := a is a direct asset.} \]
\[ \text{[[ ui } \xrightarrow{c} a \text{ ]] := } ui \text{ impacts } a \text{ [[ c ]].} \]
\[ \text{[[ c ]] := with consequence } c \text{.} \]
Semantics of the initiate relation

[[ ts(l₁) ]] := Threat scenario ts occurs [[ l₁ ]].
[[ ui(l₂) ]] := Unwanted incident ui occurs [[ l₂ ]].

[[ v ]] := vulnerability v
[[ l ]] := with likelihood l

[[ ts \xrightarrow[v]{l₃} ui ]] := ts leads to ui with [[ l₃ ]], due to [[ v ]].
An example

Threat scenario *Servers infected by malicious code* occurs with likelihood *1 per 10 years*.

Threat scenario *Malicious code traffic jams network* occurs with likelihood *1 per year*.

Threat scenario *Application servers malfunctioning* occurs with likelihood *1 per 5 years*.

*Servers infected by malicious code* leads to *Application servers malfunctioning* with likelihood *0.5*.

*Malicious code traffic jams network* leads to *Application servers malfunctioning* with likelihood *0.1*. 
The CORAS calculus
Initiates rule

- For threat $t$ and scenario/incident $e$ related by the initiates relation, we have:

$$
\frac{t \xrightarrow{p} e}{(t \sqcap\downarrow e)(p)}
$$

- $t \sqcap\downarrow e$ can be understood as the instances of scenario/incident $e$ that are initiated by threat $t$, in other words $t \sqcap\downarrow e$ is a subset of $e$
Leads-to rule

- For the scenarios/incidents \( e_1 \) and \( e_2 \) related by the leads-to relation, we have:

\[
\frac{e_1(p) \quad e_1 \overset{l}{\rightarrow} e_2}{(e_1 \sqcap e_2)(p \cdot l)}
\]

- \( e_1 \sqcap e_2 \) can be understood as the subset of the scenarios/incidents \( e_2 \) that are preceded by \( e_1 \); note that this means that \( \sqcap \) is not commutative.
Mutually exclusive vertices rule

- If the scenarios/incidents $e_1$ and $e_2$ are mutually exclusive, we have:

$$\frac{e_1(p_1) \cdot e_2(p_2)}{(e_1 \sqcup e_2)(p_1 + p_2)}$$

- $e_1 \sqcup e_2$ denotes all instances of $e_1$ and $e_2$
Independent vertices rule

- If the scenarios/incidents $e_1$ and $e_2$ are statistically independent, we have:

$$
\frac{e_1(p_1) \cdot e_2(p_2)}{(e_1 \biguplus e_2)(p_1 + p_2 - p_1 \cdot p_2)}
$$
Consistency checking of likelihoods

1 per 10 years x 0.5 = 1 per 20 years = 0.05
1 per year x 0.1 = 1 per 10 years = 0.1

Given that the events are statistically independent, we may calculate a minimum for the end node: 

$$1 - (1 - 0.05)(1 - 0.1) = 0.145$$

1 per 5 years = 0.2 > 0.145

If the events had been mutually exclusive the minimum would have been 0.05 + 0.1 = 0.15
The CORAS editor
Getting Started

- **Installation**
  - Make sure you have Java installed.
  - Create a suitable folder, e.g. C:\CORAS-TOOL. In the following we refer to this as <Your folder>.
  - Extract the zip-file corastool_deployment.zip into <Your folder>.

- **Starting the CORAS tool**
  - Go to the folder <Your folder>\eclipse and double click on Coras.exe.
  - You are now ready to use the CORAS tool.