A contract-oriented view on threat modelling

Ketil Stølen
SINTEF ICT and University of Oslo

Joint work with
Gyrd Brændeland, Heidi Dahl, Olav Ligaarden

FLACOS
Malta, November 27, 2008
Motivation

- How to modularize threat modelling
- How to deal with mutual dependencies in threat modeling of complex systems
- We need a notion of contract at the abstraction level of threat models
Problem of risk analysis

- Systems
  - are complex
  - mutually dependent
  - cross national borders
  - are continuously updated

- You never have full access to all documentation

- And, if you had, there would just be too much of it
There is only one way forward

- We need a reductionistic approach to risk analysis
  - Decomposing analyses into smaller parts
  - Composing (already completed) analyses into an overall risk picture

- Methodological reductionism is the idea that developing an understanding of a complex system's constituent parts (and their interactions) is the best way to develop an understanding of the system as a whole
Reductionistic approach to the modeling of threat scenarios

- I will illustrate the approach on CORAS

CORAS is
- a method for model-driven security risk analysis
- a graphical language
  - for structured brainstorming and analysis
  - semantics defined as schematic translation of diagrams into English
- a tool

- You may do likewise with your favorite threat scenario modeling language – (or your favorite risk table)
Approach

- Extend the graphical CORAS language to cope with context dependencies
  - We refer to the extended language as **Dependent CORAS**
- Update the semantics of the CORAS language to deal with context dependencies
- Define rules to reason about context dependencies
- Define rules for simplifying composed scenarios
One Step Back: What is Security Risk Analysis?
The CORAS security risk modeling language

- Human threat (accidental)
- Non-human threat
- Human threat (deliberate)
- Vulnerability
- Threat scenario
- Treatment
- Unwanted incident
- Asset
Threat Diagram

- **Threat**: Hacker
- **Threat scenario**: Power supply in Norway breaks down
- **Unwanted incident**: Blackout in Norway
- **Critical asset**: Power production in Norway

- **Events**:
  - Power supply in Sweden breaks down [1:5 years]
  - Power supply in Norway breaks down [1:100 years]
Semantics: Translation into English

Vertices
- "Hacker” is a deliberate threat.
- Threat scenario "Power supply in Norway breaks down” occurs with undefined likelihood.
- Threat scenario "Power supply in Sweden breaks down” occurs with likelihood ”1:5 years”.
- Unwanted incident "Blackout in Norway” occurs with likelihood ”3:100 years”.
- ”Power production in Norway” is an asset.

Relations
- Hacker initiates "Power supply in Norway breaks down” with likelihood ”1:100” years.
- ”Power supply in Norway breaks down” leads to "Blackout in Norway” with conditional likelihood ”1.0”.
- ”Power supply in Sweden breaks down” leads to "Blackout in Norway” with conditional likelihood ”0.1”.
- ”Power supply in Norway breaks down” impacts "Power production in Norway” with consequence ”critical”.

Checking Likelihoods

Power supply in Sweden breaks down [1:5 years]

Power supply in Norway breaks down [1:100 years] * 0.1 = [1:50 years]

[1:5 years] * 0.1 = [1:50 years]

[1:100 years] + [1:50 years] = [3:100 years]

Blackout in Norway [3:100 years]

Critical Power production in Norway
Power supply in Norway breaks down
[3:100 years]

Power supply in Sweden breaks down
[1:5 years]

Hacker
[1:100 years]

Norwegian Power Supply

Power supply in Norway breaks down
1.0

Blackout in Norway
[3:100 years]

Target Scenario

Critical

Power production in Norway

Context Scenario

ICT
Semantics of Dependent Diagram

- \( [[[C \triangleright T]]] := \)
- \( [[[T]]] \
  \text{assuming} \
  [[[C]]] \
  \text{to the extent there are explicit dependencies} \)

Norwegian Power Supply

- Hacker
  - [1:100 years]

- Power supply in Norway breaks down
  - [1:5 years]

- Power supply in Sweden breaks down
  - [1:5 years]

Blackout in Norway
- [3:100 years]

Critical
- Power production in Norway
Independence of Context

\[ C \perp T \] : T is independent of C if there are no paths from C to T

[Diagram showing the Independence of Context with nodes and edges labeled accordingly.]
Rule of Independence

\[ C \triangleright T \quad C \bowtie T'' \quad T' \bowtie T'' \quad \triangleright T'' \]

- Power supply in Sweden breaks down [1:5 years]
- Blackout in Norway [3:100 years]

Norwegian Power Supply

Hacker [1:100 years]

Power supply in Norway breaks down

Power production in Norway

0.1

1.0

critical
Modus Ponens

\[ \frac{C \downarrow T \quad \downarrow C}{\downarrow T} \]

- Power supply in Sweden breaks down [1:5 years]
- 0.1
- Blackout in Norway [3:100 years]
- Power production in Norway

Norwegian Power Supply

Hacker [1:100 years]

Power supply in Norway breaks down 1.0 critical

SINTEF ICT
Applying the Deduction Rules

Norwegian Power Supply

- Power supply in Norway breaks down [1:100 years]
- Hacker [1:100 years] -> 0.1
- Power supply in Norway breaks down
- Blackout in Norway [3:100 years]
- Critical Power production in Norway

Swedish Power Supply

- Power supply in Sweden breaks down [1:100 years]
- Operator error [1:5 years] -> 0.1
- Power supply in Sweden breaks down
- Blackout in Sweden [21:100 years]
- Critical Power production in Sweden
The Combined Diagram

Norwegian and Swedish Power Supply

- Hacker [1:100 years]
- Operator error [1:5 years]

Power supply in Norway breaks down [1:100 years] -> Blackout in Norway [3:100 years] 1.0

Power supply in Sweden breaks down [1:5 years] -> Blackout in Sweden [21:100 years] 1.0

Critical Power production in Norway

Critical Power production in Sweden
Horizontal Composition

- High export from area [1:1years]
  - High load on transmission corridor
  - Protection failure
  - Transmission line outage [1:1year]
  - Grid overload causes multiple outages in export area [1:10years]

- Grid overload leads to grid overload in Norway [1:10years]
Blackout in southern Sweden and Norway

- Power market
  - Lack of rain in Norway [1:5years]
  - Lack of rain in Sweden [1:5years]
  - Operator error
  - Hacker
  - Low hydro availability [1:5years]
  - Reduced nuclear availability [1:20years]

High export leads to grid overload in Norway [1:10years]

Grid overload causes multiple outages [1:10years]

Failed area protection [1:20years]

Outage of two or more transmission lines in the north/south corridor [1:1years]

Failed load shedding [1:10years]

High load on transmission corridor

Grid overload causes multiple outages [1:10years]

Failed area protection [1:10years]

Blackout in southern Sweden [1:20years]

Minor export area blackout in Norway [1:20years]

Power production in Sweden

Power production in Norway

Minor area blackout [1:20years]

Outage of two or more transmission lines in the north/south corridor [1:1years]

Failed load shedding [1:10years]

High load on transmission corridor

Grid overload causes multiple outages [1:10years]

Failed area protection [1:10years]

Blackout in southern Sweden [1:20years]

Minor export area blackout in Norway [1:20years]

Power production in Sweden

Minor area blackout [1:20years]
Horizontal Composition

- Grid overload causes multiple outages [1:10 years]
- Failed area protection
- Total area blackout [1:20 years]

Critical
Blackout in southern Sweden and Norway

- Lack of rain in Norway [1:5years]
- Low hydro availability in Norway [1:5years]
- Hacker
- Low load on transmission corridor [1:10years]
- Outage of two or more transmission lines in the north/south corridor [1:1year]
- Reduced nuclear availability in Sweden [1:20years]
- Low hydro availability in Sweden [1:5years]
- Operator error
- Power production in Sweden
- Power market

- High import from Sweden [1:5years]
- High export leads to grid overload in Norway [1:10years]
- Blackout in southern Sweden [1:20years]
- Minor area blackout [1:20years]
- Minor export area blackout in Norway [1:10years]

- Grid overload causes multiple outages [1:10years]
- Total area blackout [1:20years]
- Failed area protection
- Failed load shedding [1:10years]
- Reduced load on transmission corridor [1:10years]
- High load on transmission corridor [1:10years]
- High load on transmission corridor [1:10years]

- Power production in Norway
- Power production in Sweden

- High load on transmission corridor [1:10years]
Horizontal Composition

- Blackout in southern Sweden [1:20 years]
- Total area blackout [1:20 years]
- Total area blackout in southern Sweden and Norway [1:100 years]

0.2, 0.2, 0.1
Blackout in southern Sweden and Norway

- Power market
  - Lack of rain in Norway
    - Low hydro availability [1:5years]
      - High import from Sweden [1:5years]
        - High load on transmission corridor
          - Grid overload causes multiple outages [1:10years]
            - Failed area protection
              - Failed load shedding
                - Outage of two or more transmission lines in the north/south corridor [1:1year]
                  - Reduced nuclear availability [1:20years]
                    - Low hydro availability [1:5years]
                      - Capacity shortage [1:4years]
                        - Unstable network [1:10years]
                          - Minor export area blackout [1:20years]
                            - Total area blackout in southern Sweden and Norway [1:100years]

- Hacker
  - Operator error
    - Interface bottleneck
      - Low hydro availability [1:5years]
        - High export leads to grid overload in Norway [1:10years]
          - Total area blackout in Norway [1:10years]

- Power market
  - Power production in Norway
    - Power production in Sweden
      - Minor area blackout [1:20years]
        - Reduced nuclear availability [1:20years]
          - Low hydro availability [1:5years]
            - Outage of two or more transmission lines in the north/south corridor [1:1year]
              - Unstable network [1:10years]
Asset Composition

Total area blackout in southern Sweden and Norway [1:100 years]

Critical

Power production in Norway

Critical

Power production in Sweden

Critical

Total area blackout in southern Sweden and Norway [1:100 years]

Critical

Power production in Norway and Sweden
Blackout in southern Sweden and Norway

- Power market
- Low hydro availability in Norway [1:5 years]
- High import from Sweden [1:5 years]
- High load on transmission corridor
- Grid overload causes multiple outages [1:10 years]
- Total area blackout in Norway [1:20 years]
- Power production in Norway
- Power production in southern Sweden and Norway [1:100 years]
- Total area blackout in southern Sweden and Norway [1:100 years]

- Hacker
- Operator error
- Outage of two or more transmission lines in the north/south corridor [1:1 year]
- Failed load shedding
- Failed area protection
- Minor area blackout in Norway [1:20 years]

- Reduced nuclear availability [1:20 years]
- Low hydro availability in Sweden [1:5 years]
- Capacity shortage [1:4 years]
- Unstable network [1:10 years]

- Interface bottleneck
- Power production in Sweden
Vertical Composition

- Reduced nuclear availability [1:20 years]
- Low hydro availability [1:5 years]
- Low energy availability [1:4 years]
Blackout in southern Sweden and Norway

Power market

Lack of rain in Norway

Lack of rain in Sweden

High export leads to grid overload in Norway [1:10years]

High import from Sweden [1:5years]

Low hydro availability [1:5years]

High load on transmission corridor

Failed area protection

Failed load shedding

Outage of two or more transmission lines in the north/south corridor [1:1year]

Interface bottleneck

Total area blackout [1:20years]

Power production in Norway

High export leads to grid overload in Norway [1:10years]

Power production in Norway

Minor export area blackout in Norway [1:20years]

Power production in Sweden

Total area blackout in southern Sweden and Norway [1:100years]

Low hydro availability [1:5years]

Low energy availability [1:4years]

Capacity shortage [1:4years]

Unstable network [1:10years]

Operator error

Hacker

High import from Sweden [1:5years]

High load on transmission corridor

Grid overload causes multiple outages [1:10years]

Total area blackout [1:20years]

Failed area protection

Minor area blackout [1:20years]
Horizontal Composition

- Low energy availability [1:4 years]
- Capacity shortage [1:4 years]
- Unstable network [1:10 years]

- High load in combination with extreme demand in Southern Sweden [1:10 years]
Blackout in southern Sweden and Norway

- Power market
- Lack of rain in Norway [1:5years]
- Hacker
- Operator error
- Lack of rain in Sweden
- Interface bottleneck
- Outage of two or more transmission lines in the north/south corridor [1:1year]
- High load in combination with extreme demand in Southern Sweden [1:10years]
- High import from Sweden [1:5years]
- High load on transmission corridor
- Grid overload causes multiple outages [1:10years]
- Failed area protection
- Failed load shedding
- High export leads to grid overload in Norway [1:10years]
- Low hydro availability [1:5years]
- Total area blackout in southern Sweden and Norway [1:100years]
- Total area blackout in Norway [1:20years]
- Minor area blackout [1:20years]
- Minor export area blackout in Norway [1:20years]
- High load on transmission corridor
- Power market
- Power production in Norway
- Power production in Norway and Sweden
- Power production in Sweden

Events:
- High export leads to grid overload in Norway [1:10years]
- Total area blackout in Norway [1:20years]
- Minor area blackout [1:20years]
- Total area blackout in southern Sweden and Norway [1:100years]
- Minor export area blackout in Norway [1:20years]
- Grid overload causes multiple outages [1:10years]
- Failed area protection
- Failed load shedding
- High load in combination with extreme demand in Southern Sweden [1:10years]
- High import from Sweden [1:5years]
- Low hydro availability [1:5years]
- Lack of rain in Norway [1:5years]
- Hacker
- Operator error
- Lack of rain in Sweden
- Interface bottleneck
- Outage of two or more transmission lines in the north/south corridor [1:1year]
Horizontal & Asset Composition

Minor export area blackout in Norway [1:20years]

Minor area blackout [1:20years]

Power production in Norway

Power production in Sweden

Power production in Norway and Sweden

Minor area blackout [1:20years]

Power production in Sweden
Blackout in southern Sweden and Norway

- Power market
  - Power production in Norway and Sweden
  - High export leads to grid overload in Norway [1:10 years]
  - High import from Sweden [1:5 years]
  - Power production in Norway and Sweden
  - High load on transmission corridor
  - Failed load shedding
  - Failed area protection
  - Multiple area blackout [1:50 years]

- Lack of rain in Norway [1:5 years]
  - Low hydro availability
  - Power production in Norway
  - Total area blackout in Norway [1:20 years]
  - Grid overload causes multiple outages [1:10 years]

- Hacker
  - Outage of two or more transmission lines in the north/south corridor [1:1 year]
  - Failed area protection
  - Total area blackout in southern Sweden and Norway [1:100 years]

- Operator error
  - Interface bottleneck
  - Failed area protection
  - Minor area blackout [1:20 years]

- Lack of rain in Sweden [1:10 years]
  - Power production in Sweden
  - Power production in Norway
  - High export leads to grid overload in Norway [1:10 years]
  - High import from Sweden [1:5 years]
  - Power production in Norway and Sweden
  - High load on transmission corridor
  - Failed load shedding
  - Failed area protection
  - Multiple area blackout [1:50 years]
Conclusions

We have
- argued the need for a reductionistic approach to risk analysis
- outlined a generic strategy to facilitate modular threat modelling
- illustrated the generic strategy on the CORAS language

- **Downloads**
  - The CORAS diagram editor
  - The CORAS icons (Visio stencil, PNG, SVG)

- **Publications**:
Questions?

Ketil Stølen
SINTEF ICT and University of Oslo

Ketil.Stolen@sintef.no