Oversikt over metodar og teknikkar for å beskrive truslar

Mass Soldal Lund

SINTEF IKT

Kva er trusselmodellering?

- Trusselmodellering kan sjåast som to ting:
  - Metodar og teknikkar for å identifisere truslar
  - Metodar og teknikkar for å vise fram eit trusselbilete
    - dokumentasjon for seinare bruk
    - skape forståing som grunnlag for å take avgjerder
- Eg vil fokusere på det siste, mao. teknikkar for å teikne eit strukturert bilete av trusselsituasjonen

Dimensjonar

- Trusselmodelleringsteknikkar kan verte plassert i tilhøve til forskjellige dimensjonar
- Den viktigaste dimensjonen er kva som er fokus – kva for spørsmål er det ein svarar på
- Men viktige dimensjonar er òg
  - detaljnivå
  - teknologi/verksemd
  - kvalitativt/kvantitativt
  - aktivum/hending

Ulike fokus

- Trussel/-sårbarheitorientert
  - kva er dei tinga som kan få ting til å gå gale
  - ”eit nytt virus er oppdaga”
- Eventorientert
  - korleis kan noko gå gale
  - ”serveren er infisert – korleis kunne det gå til og kva kan det ført til?”
- Scenarioorientert
  - kva er det som kan gå gale
  - ”kva kan skje når vi går online?”

Kva er viktig når ein vel tilnærming

- Dokumentasjonen du endar opp med må innehalde den informasjonen du er ute etter når du nyttar han
  - har vi nok uttrykkskraft, detaljar, struktur?
- Dokumentasjonen eignar seg til å kommunisere trusselbilete til dei det skal kommuniserast til
  - er vi på riktig nivå i høve til detaljar og teknologi vs. verksemd

Eksempel: Sårbarheitsfokus

Overview

A privilege escalation vulnerability exists in the Mozilla `addSelectionListener` method. This may allow a remote attacker to execute arbitrary code.

I. Description

addSelectionListener

Web content can add a `SelectionListener` to the Selection object by using `addSelectionListener` method of the `nsISelectionPrivate` interface. This listener would be called when the user performs a "find" or "select all" command.

The problem

The notifications are created in a privileged context, which can be leveraged to execute arbitrary code. Mozilla Firefox and SeaMonkey are reported to be vulnerable.

II. Impact

By convincing a user to view a specially crafted HTML document (e.g., a web page, an HTML email message, or an HTML email attachment), an attacker may be able to execute arbitrary code with the privileges of the user.

Frå CERT

Eksempel: Trussel-fokus

Detailed Description

The shell-code in the Word document decrypts and drops the backdoor's file as CSRSE.EXE to the system's temporary folder and activates it.

After being run, the dropped file in its turn extracts and drops another file to the system. This file is dropped as WINGUIS.DLL to Windows System folder and its DoHook function is activated by the dropper. The dropper then deletes itself from the system.

The dropped DLL file is the main backdoor component. It traps several functions and modifies information that is passed to the user. As a result, the backdoor's file, startup key in the Registry, and process are not visible to the user.

The backdoor creates a startup key for its file in the Registry:

```
[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows]
"AppInit_DLLs" = "%WinSysDir%\winguis.dll"
```

- where %WinSysDir% represents the Windows System folder that by default has the name C:\Windows\System32\.

When active, the backdoor connects to a specified address in order to receive commands from a hacker. The backdoor allows the hacker to do any of the following on an infected computer:

- Create, read, write, delete and search for files and directories
- Access and modify the Registry
- Manipulate services
- Start and kill processes
- Take screenshots
- Enumerate open windows
- Create its own application window
- Get information about infected computer
- Lock, restart or shutdown Windows
- Create a pipe and read files from it
- Start a remote command shell
- Enumerate network resources

The backdoor also creates three empty SYS files in the \drivers\ subfolder of Windows System folder.

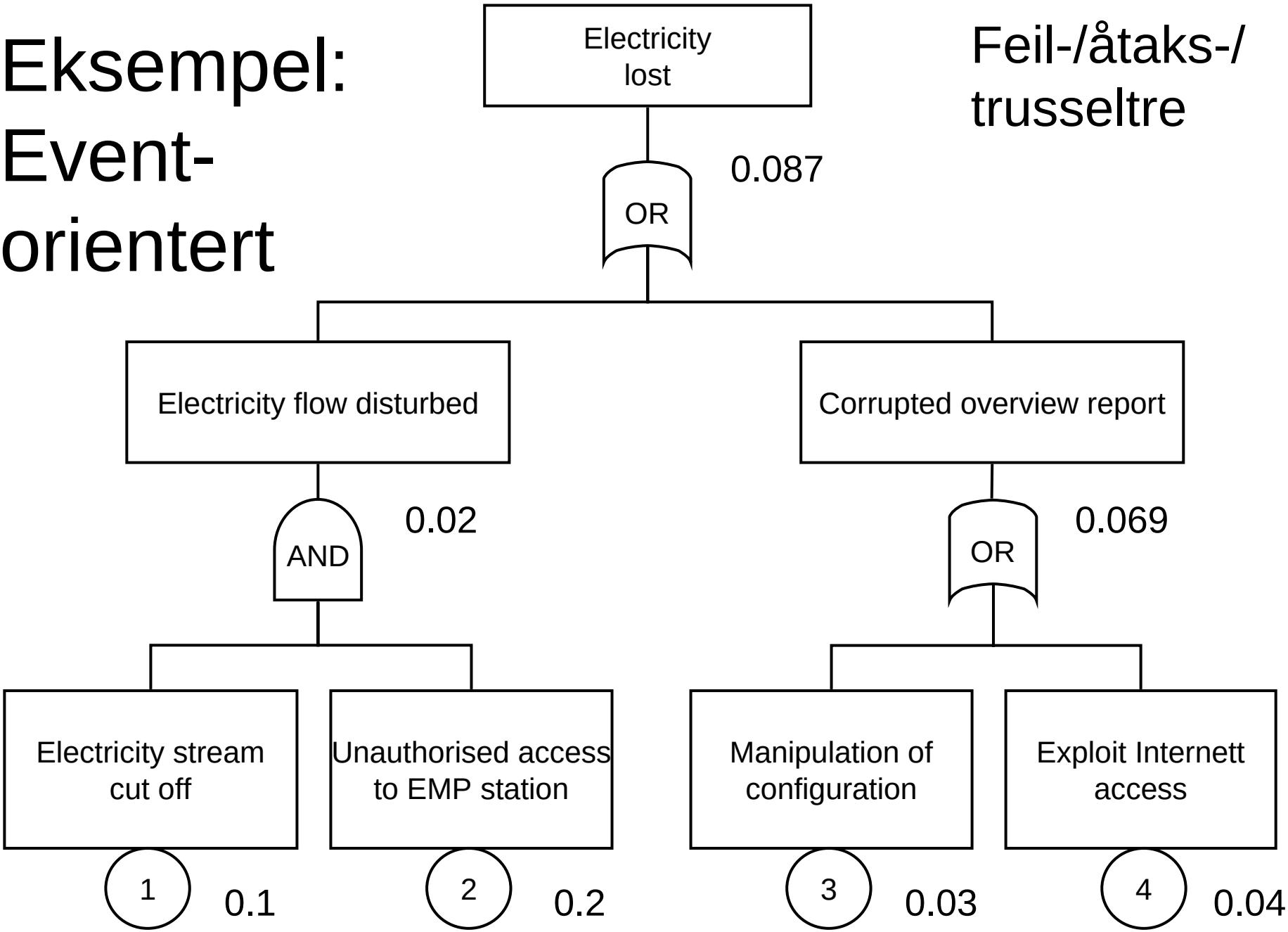
Frå F-Secure

Trussel- og sårbarheitsfokus

- Kva er dei tinga som kan få ting til å gå gale?
- Teknologi- og detaljorientert
- Viktig for arbeid med praktisk sikkerheit
- Men ikkje eigna for oversikt over trusselbilete
- Eller avgjerder på verksemdnivå

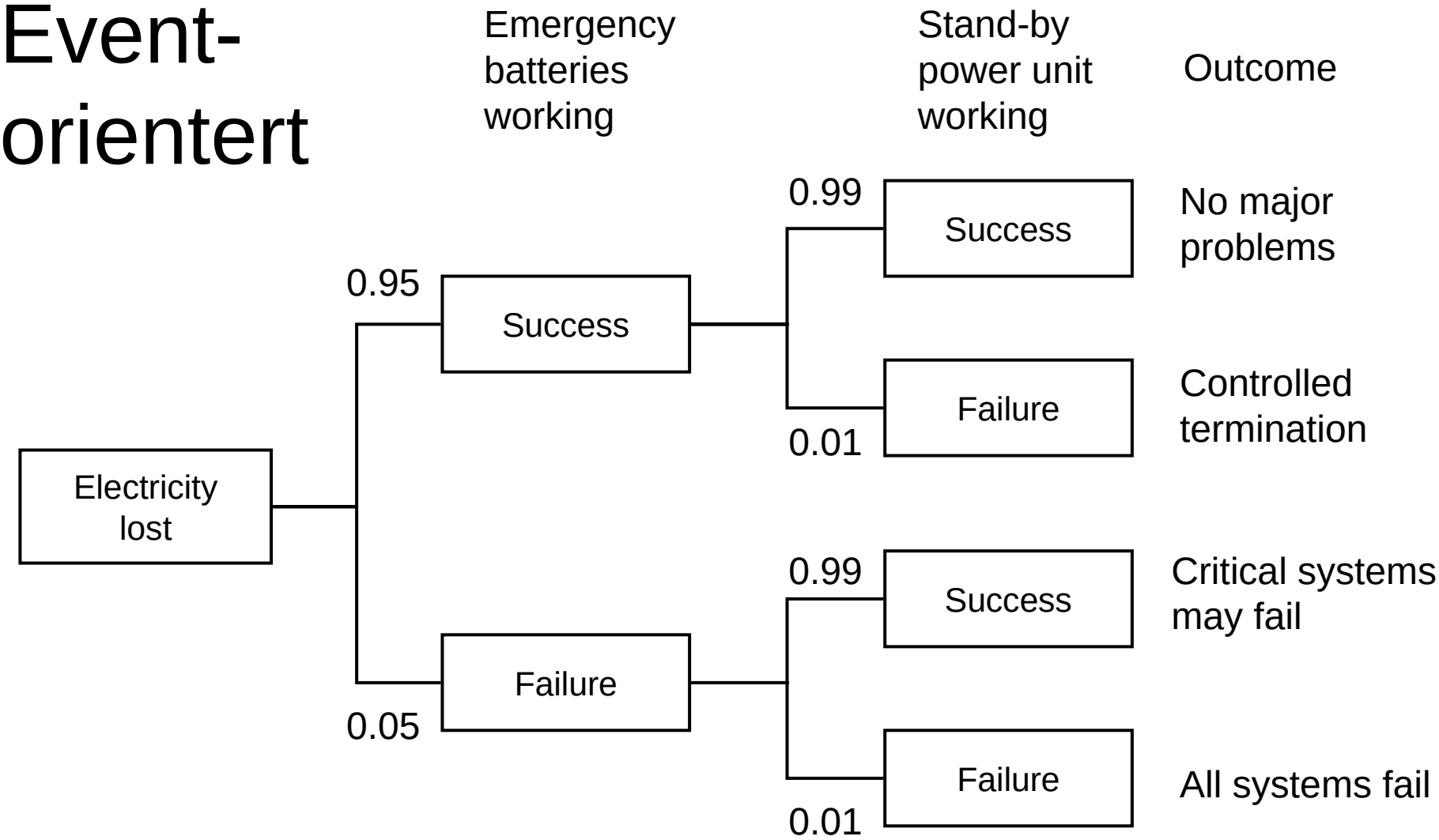
Eksempel: Event-orientert

Feil-/åtaks-/ trusseltre



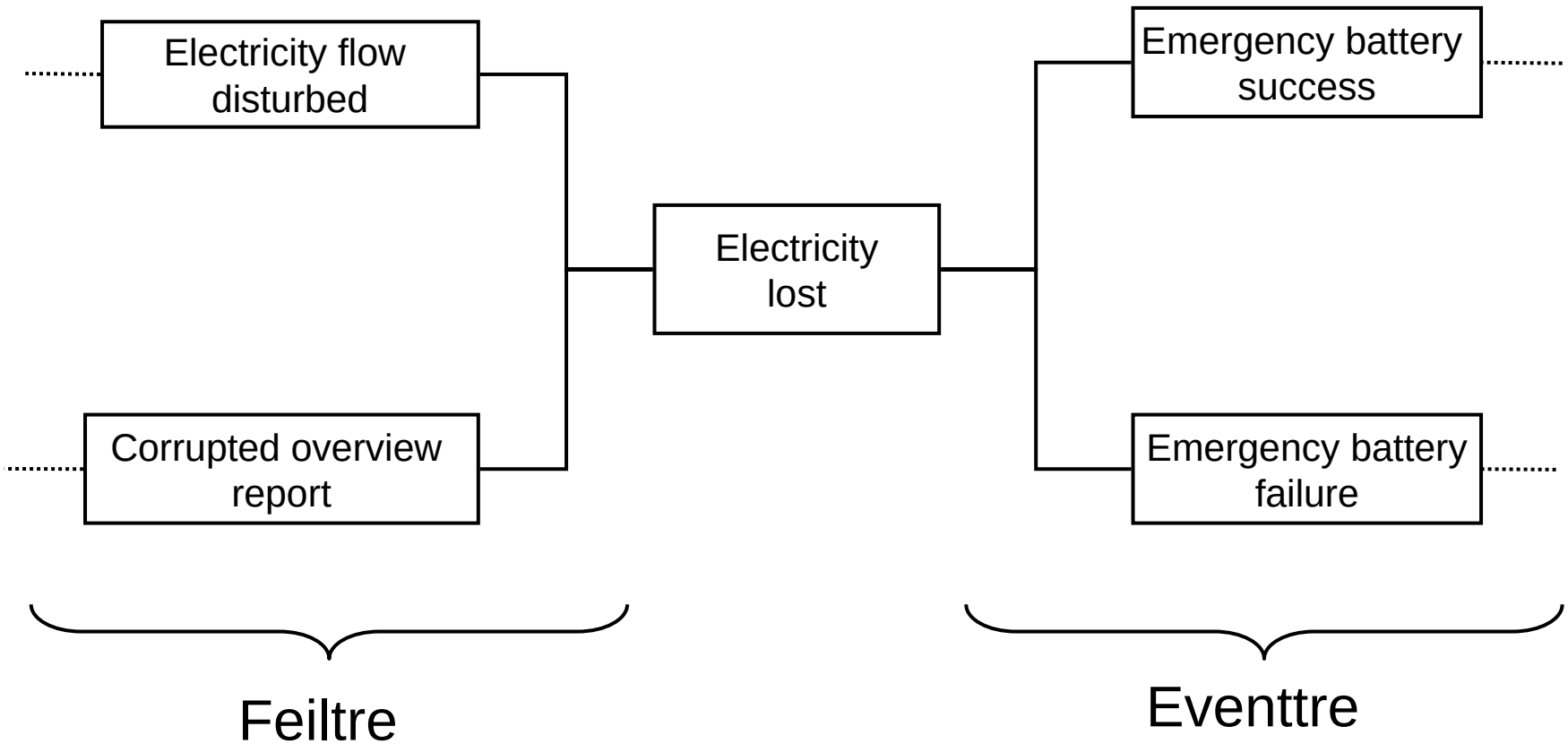
Eksempel: Event-orientert

Eventtre



Eksempel: Event-orientert

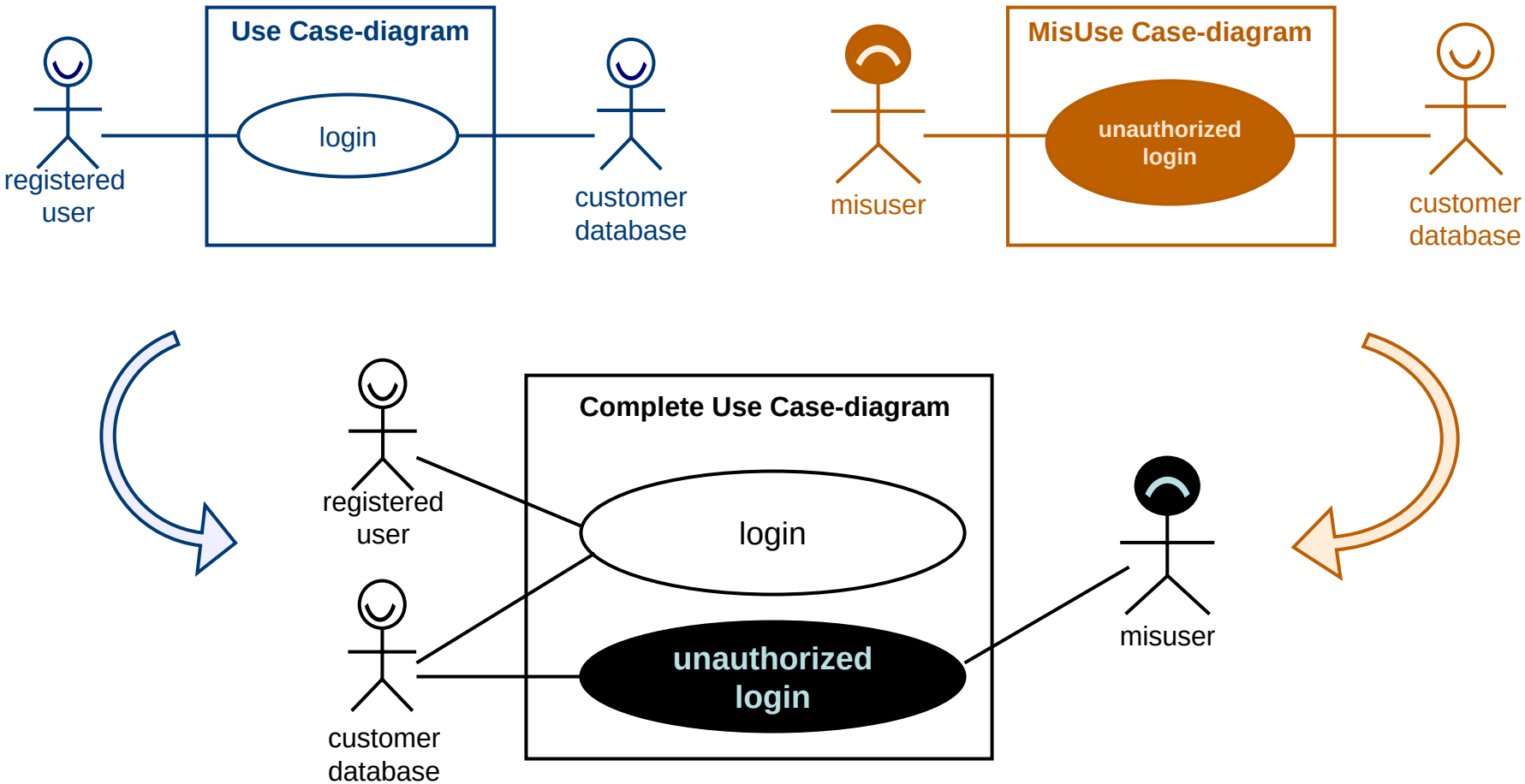
Cause-Consequence diagram



Eventfokus

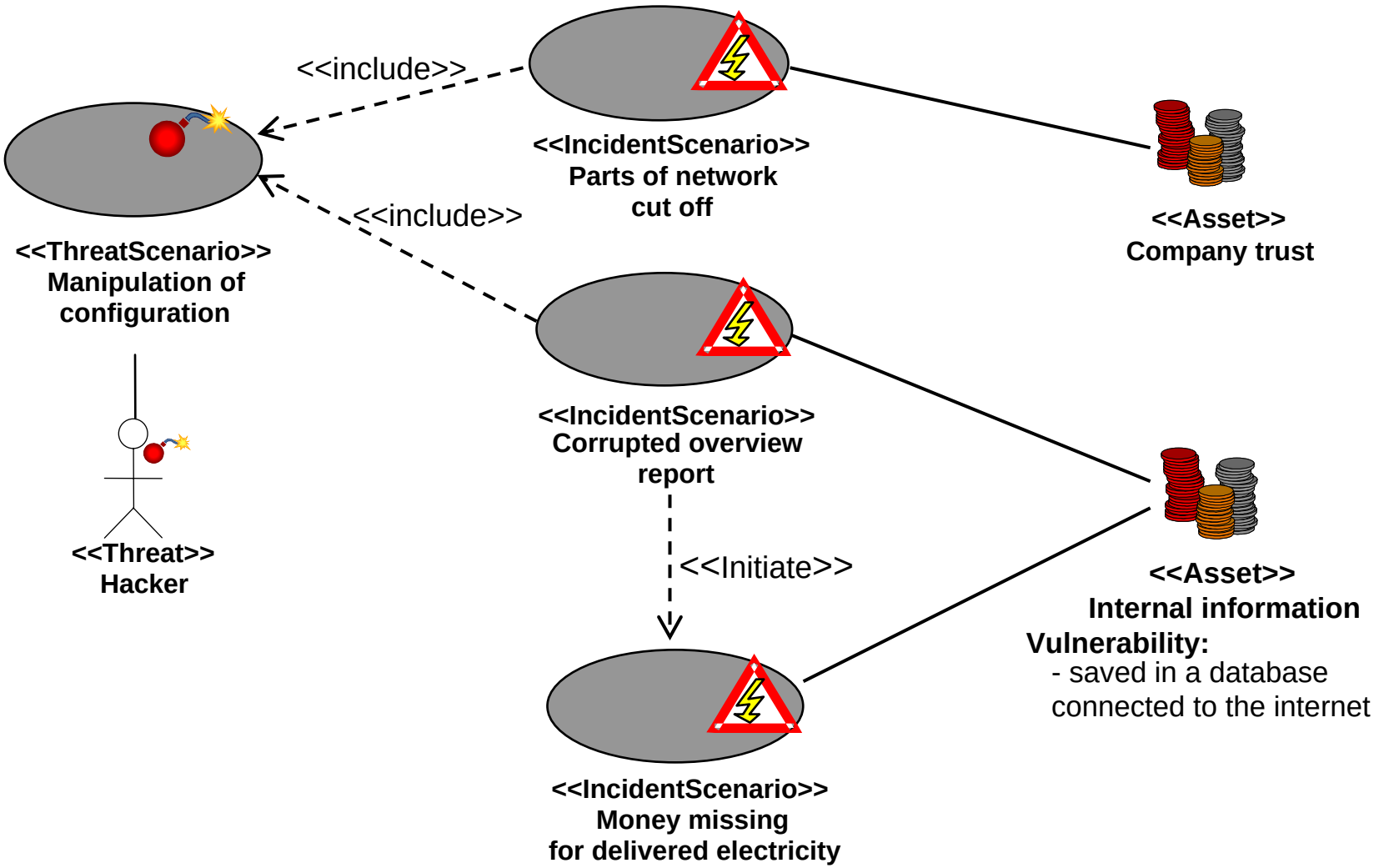
- Korleis kan noko gå gale?
- Analyse av einskilhendingar
  - kva må til for at ei uønskt hending skal skje
  - kva er konsekvensen av ei uønskt hending
- Teknologi- og detaljorientert
- Gjev godt bilete av hendingar, men eignar seg mindre bra for større trusselbilete
- Eignar seg til både kvalitativ og kvantitativ analyse

Eksempel: Scenariofokus



Eksempel: Scenariofokus

CORAS trusseldiagram



Scenariofokus

- Kva er det som kan gå gale?
- Fokus på trusseloppførsel og avhengigheiter mellom trusselscenario
- Verksemdorientert
- Eigna for å lage oversiktsbilete av trusselsituasjonen
- Og kommunisere samanhengar mellom trussler

Oppsummering

- Trussel- og sårbarheitorientert
  - strukturert tekst
  - databasar
- Eventorientert
  - Feil-/åtaks-/trusseltre
  - Eventtre
  - Cause-Consequence diagrams
- Scenarioorientert
  - Misuse cases
  - CORAS trusseldiagram

Referansar

- Ian Alexander. Misuse cases: Use cases with hostile intent. *IEEE Software*, 20(1):58-66, 2003.
- Folker den Braber, Mass Soldal Lund, Ketil Stølen. *Using the CORAS threat modelling language to document threat scenarios for several Microsoft relevant technologies*. Technical report STF90 A04057, SINTEF ICT, July 2004.
- CERT. *Vulnerabilities & Fixes.* http://www.cert.org/nav/index_red.html
- F-Secure. *Security Information Center.* http://www.f-secure.com/virus-info/
- Michael Howard, David LeBlanc. *Writing secure code, 2nd ed.* Microsoft press, 2003.
- Marvin Rausand. *Risikoanalyse, veiledning til NS 5814*, Tapir, 1991.
- Richard M. Robinson *et al. Risk & Reliability, An introductory text, 5th ed.*
- Bruce Scheiner. *Secrets & lies: digital security in a networked world.* John Wiley & Sons, 2004.