Security analysis — basic notions and ideas

September 28, 2007

Ketil Stølen, SINTEF & UiO

Acknowledgements

- The lectures on security analysis is the result of joint work with a number of current and past colleagues at SINTEF; in particular:
  - Ida Hogganvik, Mass Soldal Lund, Fredrik Vraalsen, Heidi Dahl

- The initial version of CORAS was jointly developed by the 11 partner in the CORAS project

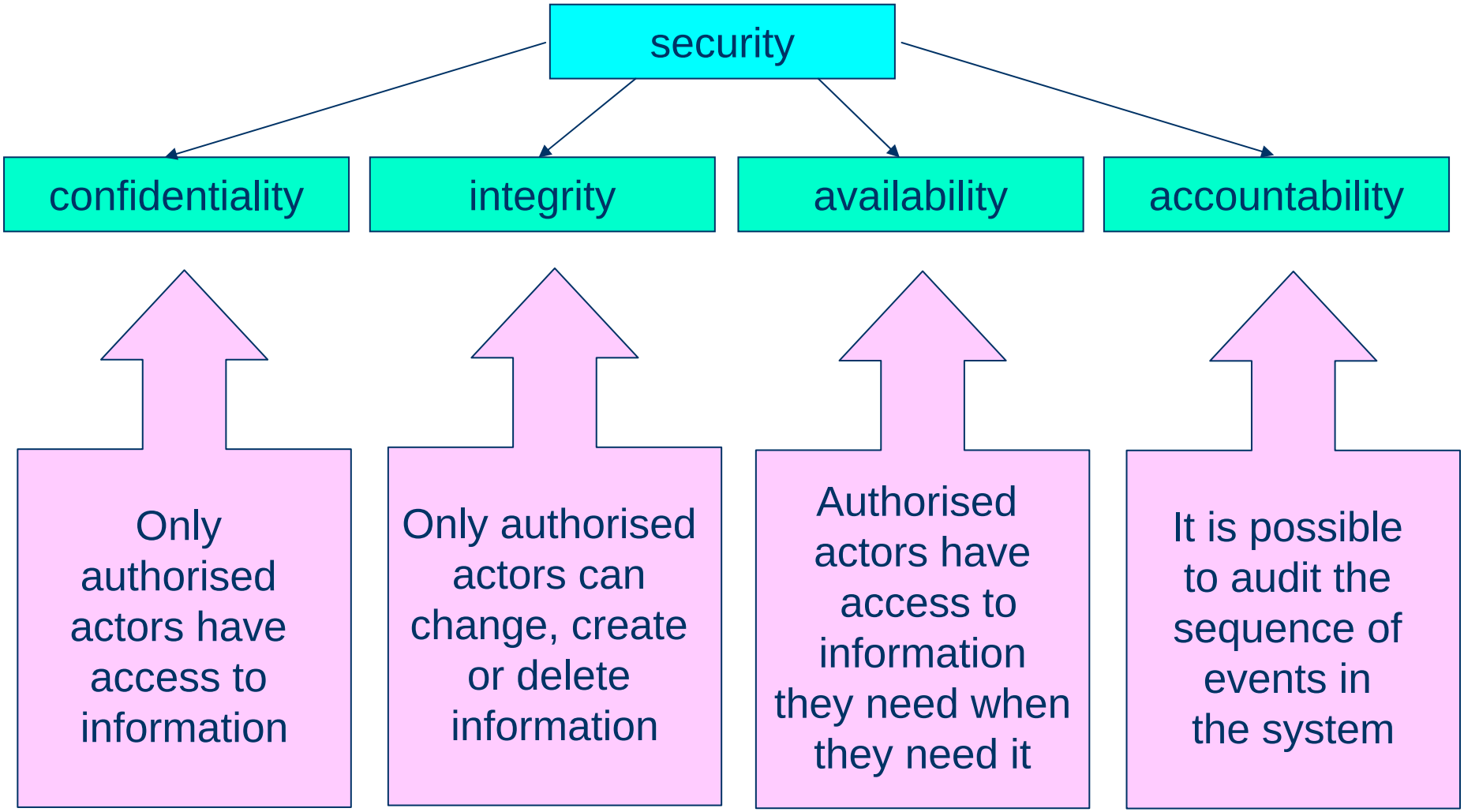
Objectives for the three lectures on security analysis

- Classify security concepts
- Introduce, motivate and explain a basic apparatus for risk management in general and risk analysis in particular
- Relate risk management to system development
- Describe the different processes that risk management involve
- Motivate and illustrate model based security analysis
- Demonstrate the use of risk analysis techniques

What is security analysis?

- Security analysis is a specialized form of risk analysis focusing on security risks

What is security?



What is risk analysis?

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

Note: Security is more than technology

- From a technical standpoint, security solutions are available – but what good is security if no one can use the systems?

- Security requires more than technical understanding
- Security problems are often of non-technical origin
- A sound security evaluation requires a uniform description of the system as a whole
  - how it is used, the surrounding organisation, etc.

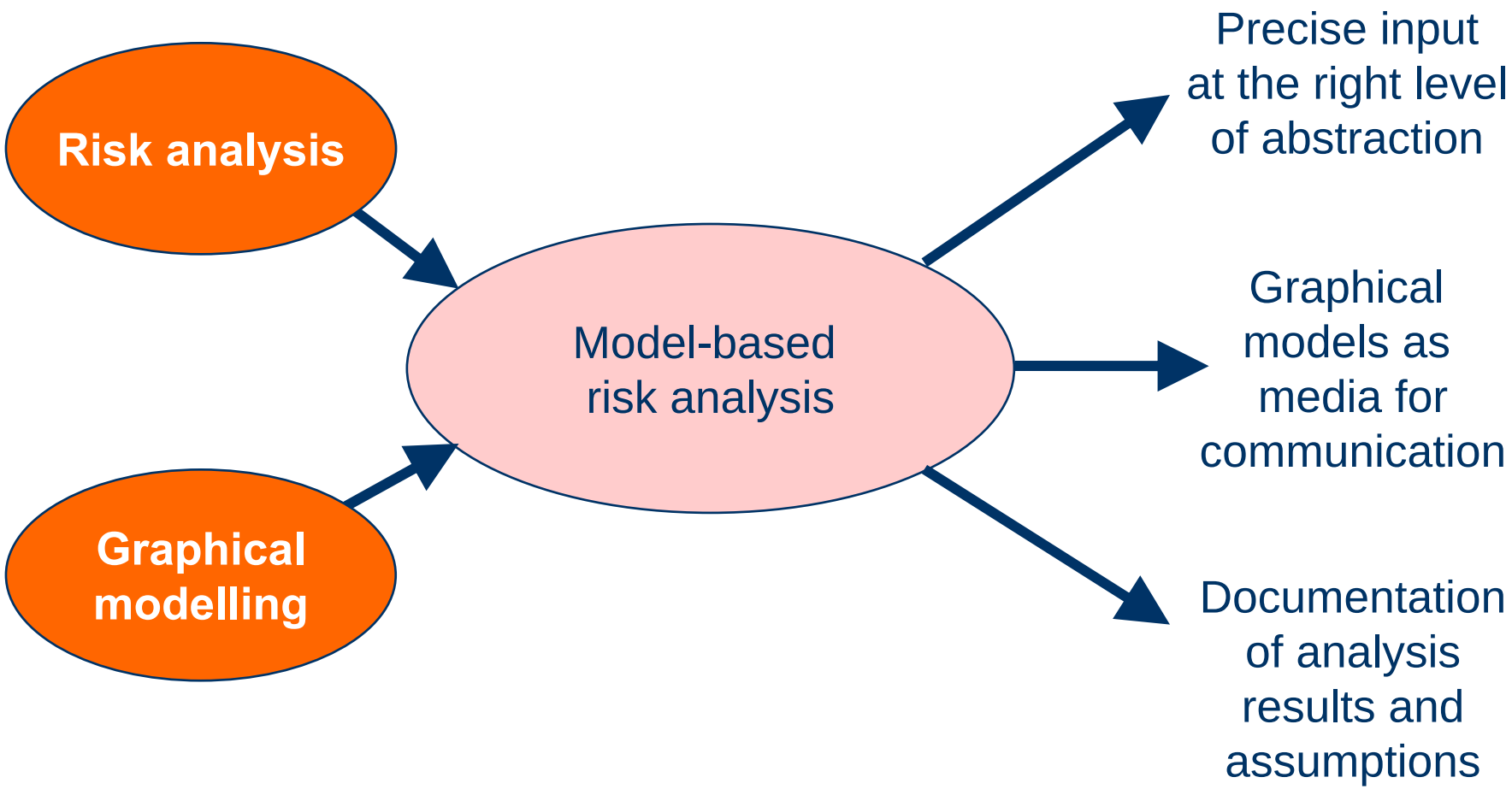
Security – part of system development

- Security is traditionally added as an “afterthought”
  - Solutions often reactive rather than proactive
  - Security issues often solved in isolation
  - Costly redesign
  - Security not completely integrated
- Requirements analysis and risk analysis are two sides of the same coin and should be integrated
  - Focus on desired and undesired behaviour, respectively

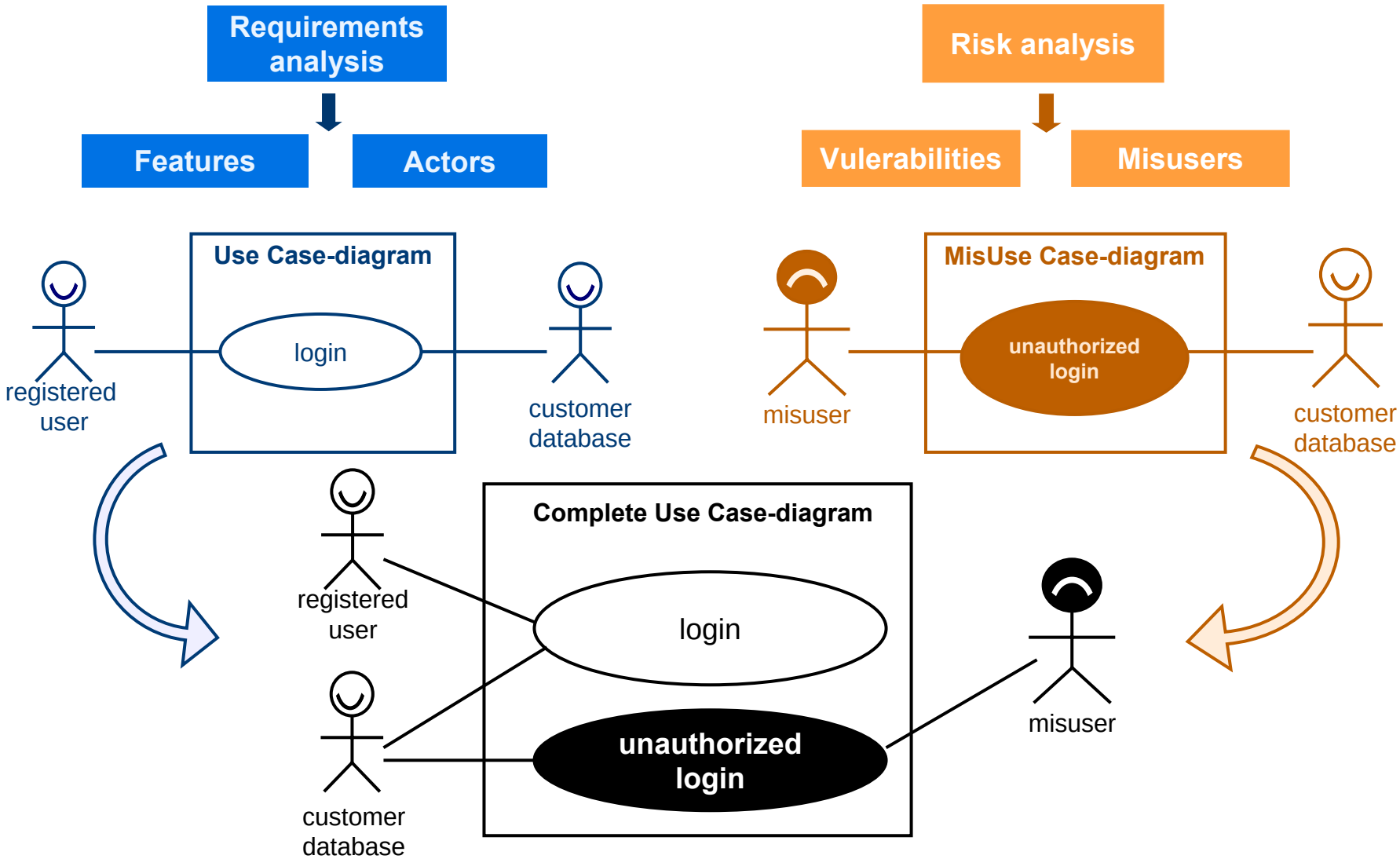
In what way relates security to

- safety
- reliability
- dependability
- maintainability
- data protection
- privacy
- trustworthy
- trust
- public key infrastructure based on trusted third party
- authentication and authorization

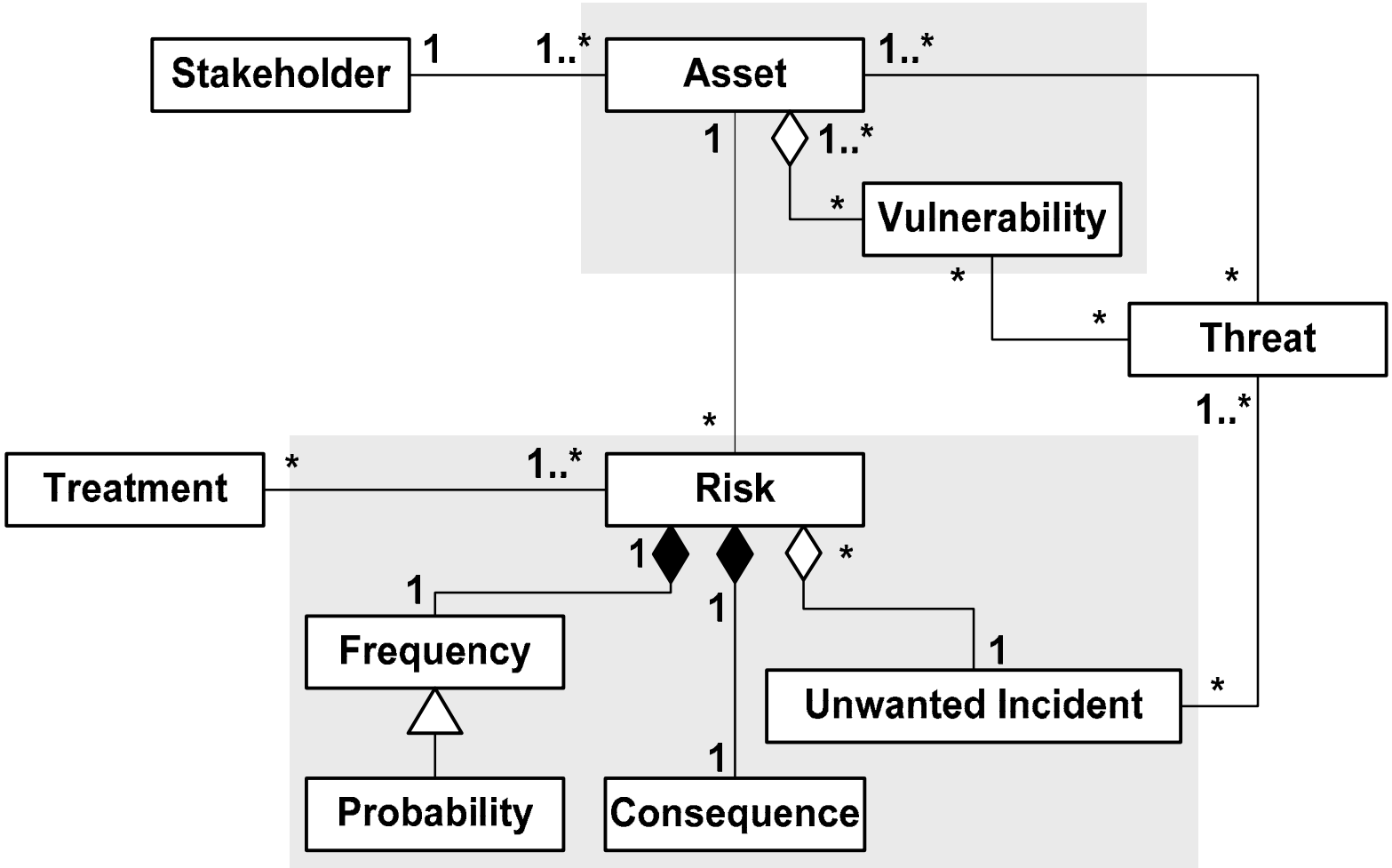
Model-based risk analysis



Model-based risk analysis

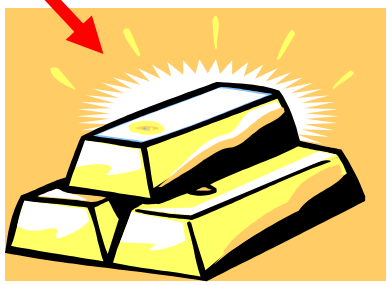


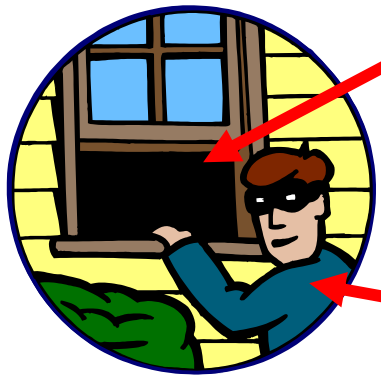
Conceptual model for risk analysis



Terms

asset, something of value





vulnerability

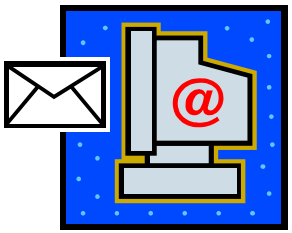
threat

reduced security risk

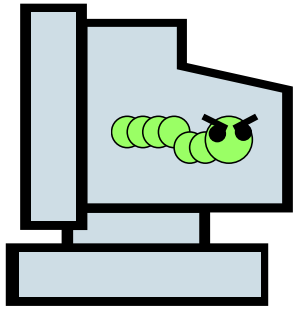
Risk with respect to security

need to introduce security mechanisms

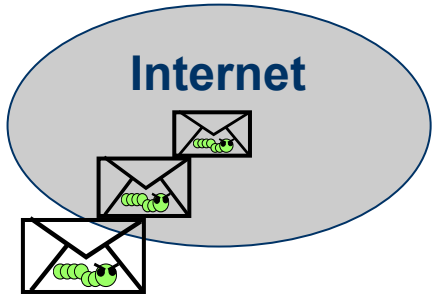
Terms

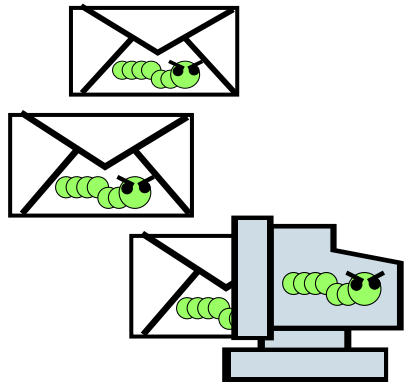


Computer running Outlook



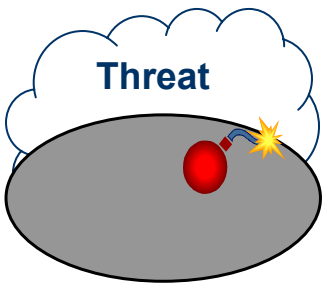
Infected PC

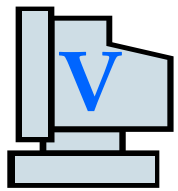




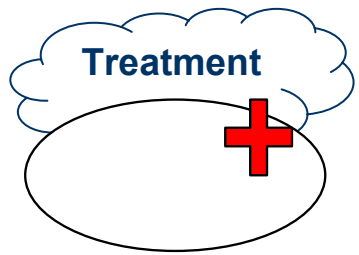
- Infected twice per year
- Infected mail send to all contacts

Worm





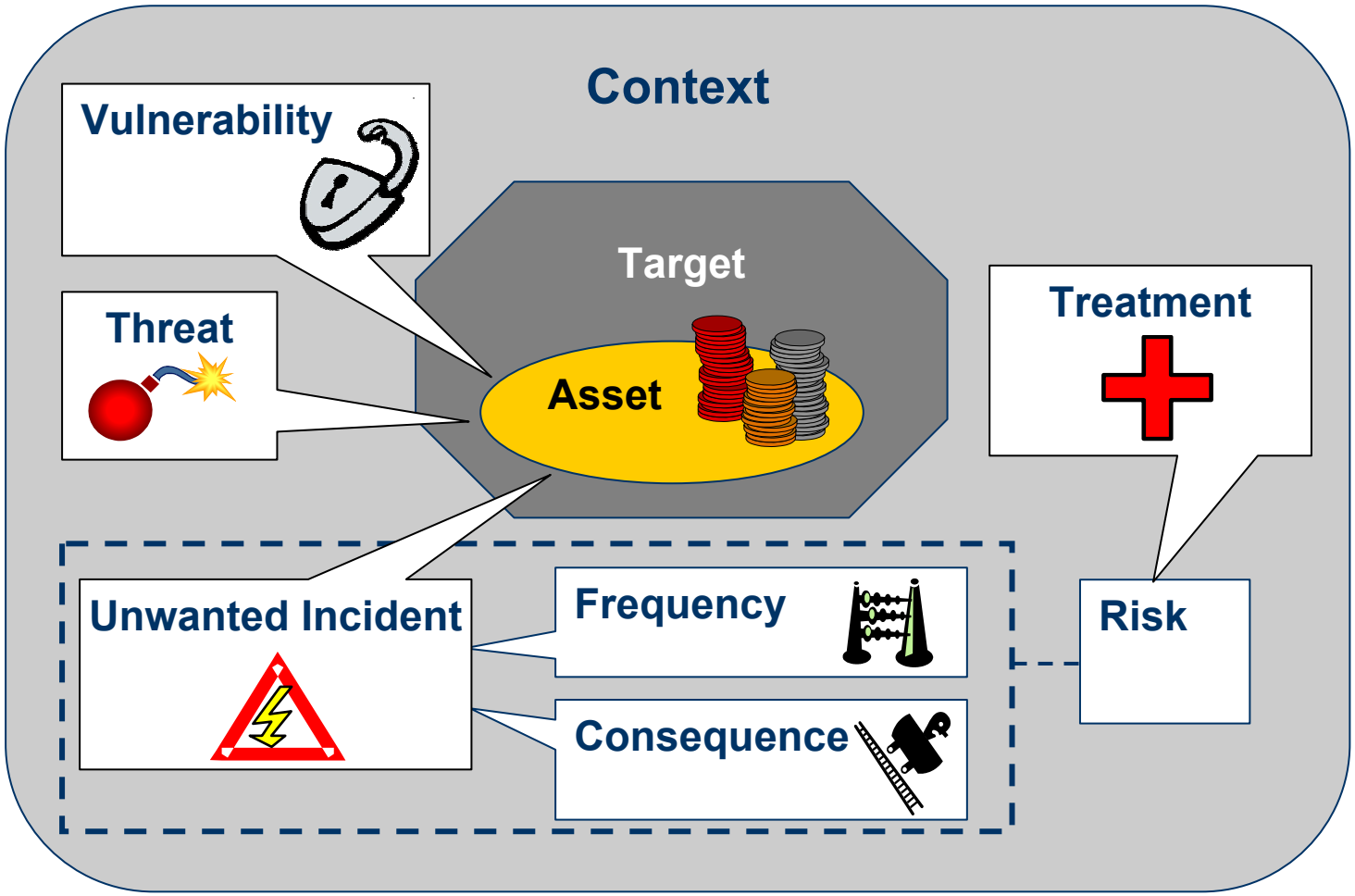
Install virus scanner



Oversettelse av terminologi

asset	aktivum (noe med verdi)
threat	trussel
unwanted incident	uønsket hendelse
risk	risiko
vulnerability	sårbarhet
consequence	konsekvens
probability	sannsynlighet
frequency	frekvens/hyppighet
treatment	behandling

Elements of risk analysis



CORAS background

- Research and technological development project under the Information Society Technologies (IST) Programme
- January 2001 -> July 2003
- 11 partners from 4 European countries

- Goal: Develop an improved methodology for precise, unambiguous, and efficient risk analysis of security critical IT systems

The need for a language

- Security analysis
  - Structured brainstorming:
    - a step-wise walk through of the analysis object to identify potential threats, vulnerabilities, unwanted incidents, risks.
  - Participants:
    - developers, users, decision makers etc.
    - have thorough knowledge of the analysis object (different parts)
    - often no experience with security analysis
    - often not used to communicate with each other
  - We need a way of supporting the analysis process and documenting findings

The need for a language

- Why is documenting a security analysis important?
  - Documentation is used ***during*** the analysis to:
    - support the process
    - share and communicate information
    - achieve a common understanding of the target of analysis
  - Documentation is used ***after*** the analysis to:
    - demonstrate that the process was conducted properly
    - provide evidence for a systematic approach
    - keep a record of risks and develop the organization's knowledge base
    - provide the decision makers with a risk management plan
    - facilitate continuous monitoring and review

The need for a language

- Traditional documentation methods in risk analysis are often only based on text and tables
- We believe graphical models are more useful in structured brainstorming:
  - suitable for capturing information “on-the-fly”
  - understandable for people without technical background
  - can quickly give the reader an overview of the risk picture

Our approach:
the CORAS security risk modeling language

- Specifies a common security risk picture for the object analyzed:
  - shows potential unwanted incidents, threats, vulnerabilities
  - supports estimation of risks (how often may the risk occur and how serious is it?)
- Developed iteratively in the SECURIS project based on:
  - experiences from field trials
  - results from empirical experiments

- Key symbols: