GraMSec 2014

Graphical Models for Security: Overview, Challenges and Recommendations

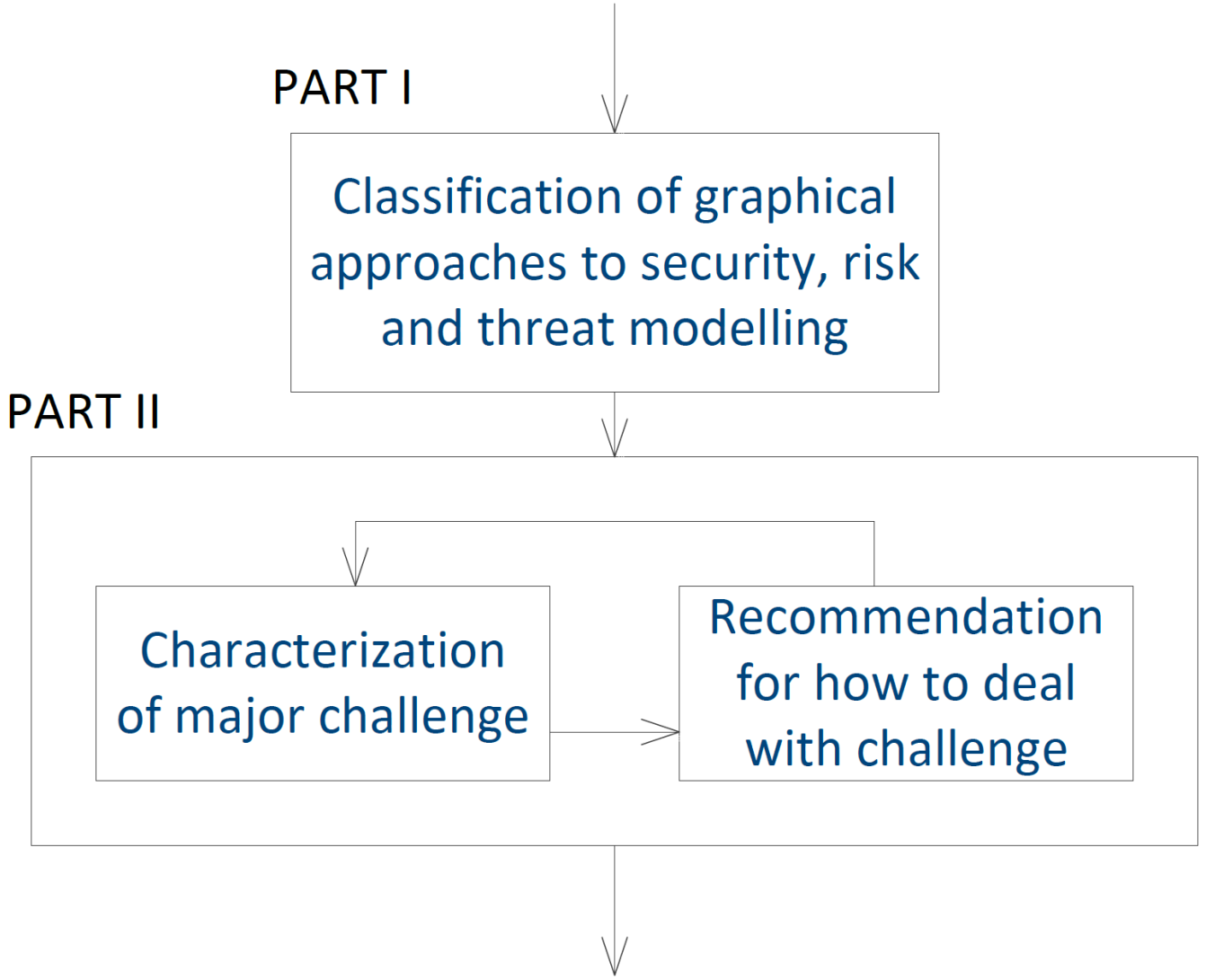
Ketil Stølen, SINTEF and University of Oslo

Grenoble, April 12, 2014

This talk aims to provide

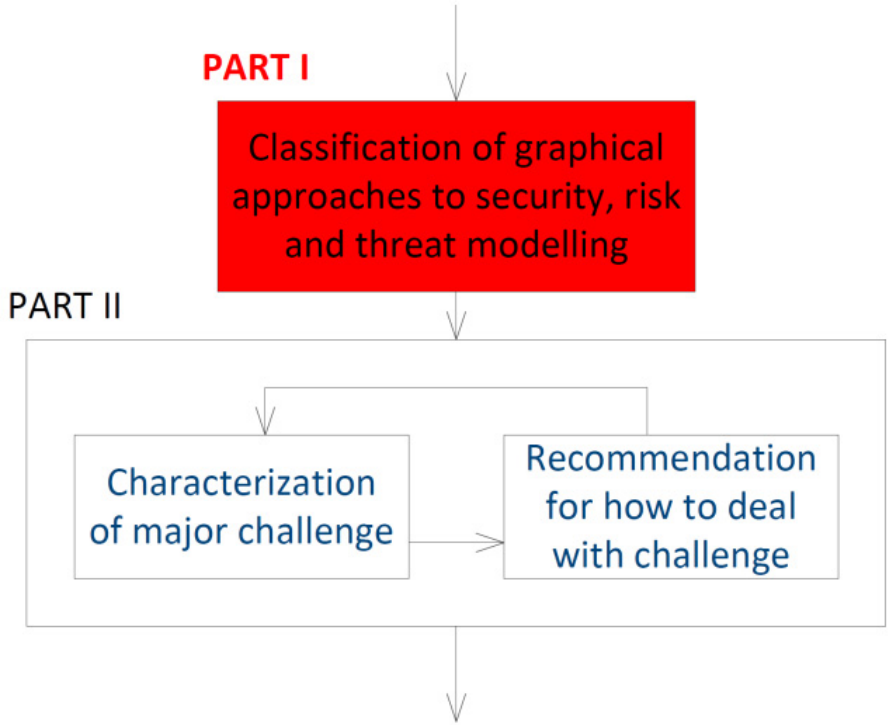
- A classification of graphical approaches to security, risk and threat modelling
- A characterization of major challenges within graphical modelling with particular focus on security, risk and threats
- Recommendations for how to deal with these challenges

Structure of talk



Part I

Classification of graphical approaches to security, risk and threat modelling



Why are you interested in graphical models for security?

What is a graphical model?

One proposal

Graphical models are a marriage between probability theory and graph theory. They provide a natural tool for dealing with two problems that occur throughout applied mathematics and engineering -- uncertainty and complexity …

From preface of Learning In Graphical Models by Michael I. Jordan

One proposal

Graphical model[illegible] marriage[illegible]ween probability theory and graph theory. They provide a natu[illegible]de[illegible]wo problems that occur throughout applied mathematics and e[illegible]certainty and complexity …

From preface of Learning In Graphical Models by Michael I. Jordan

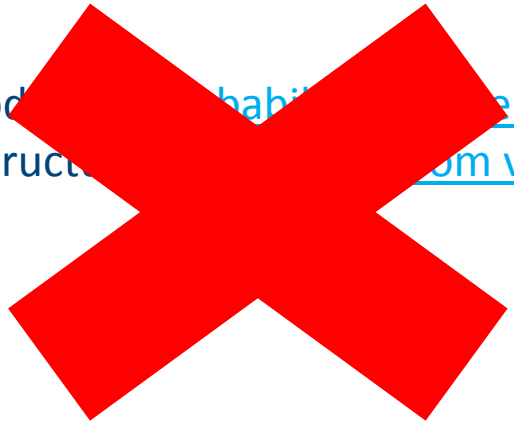
Too Narrow!

Wikipedia says

A graphical model is a probabilistic model for which a graph denotes the conditional dependence structure between random variables

Wikipedia says

A graphical mod habil el for which a graph denotes the conditional dependence struct om variables



Too Narrow!

What makes textual representations different from graphical?

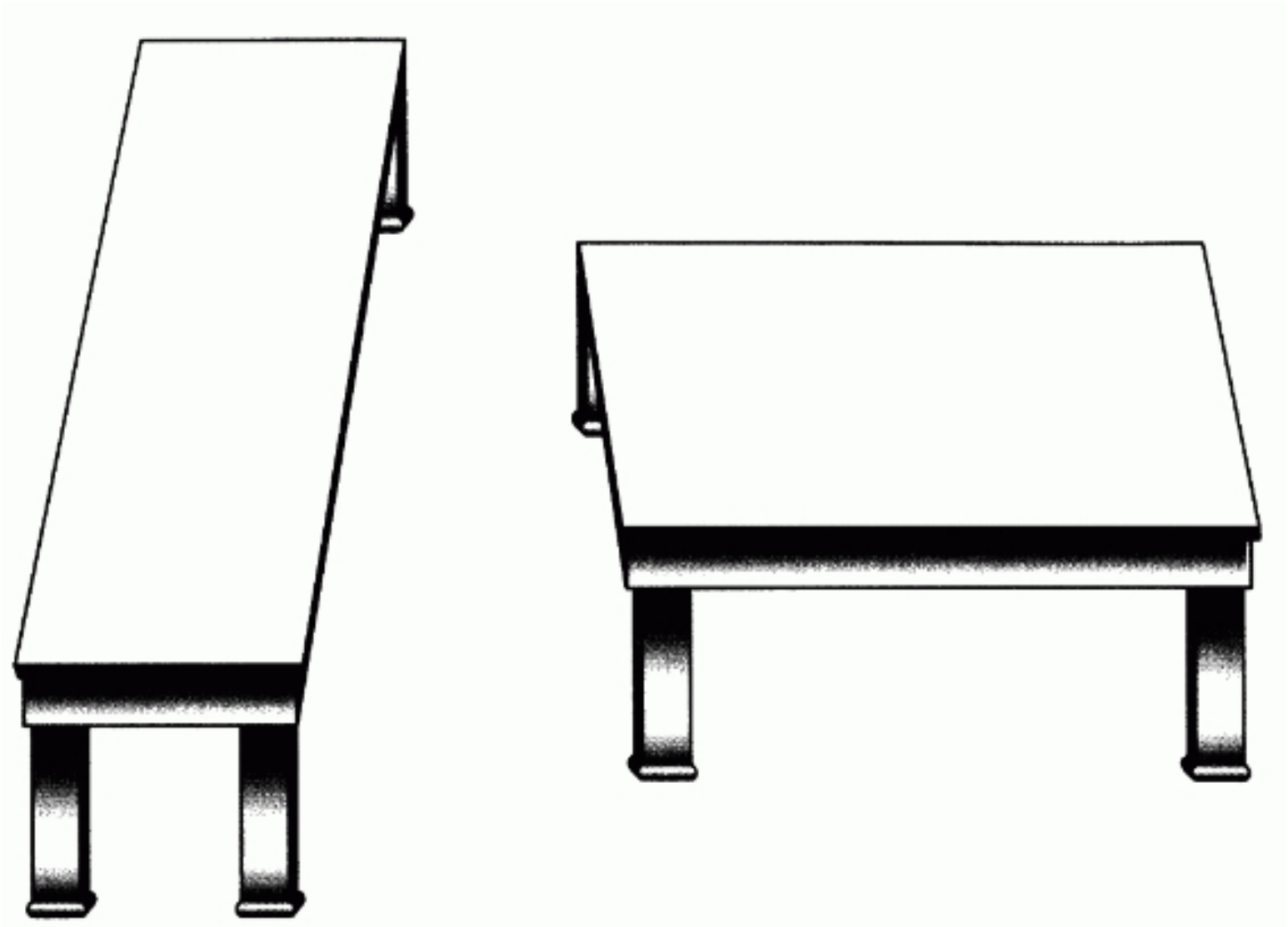
- Textual representations are ***one-dimensional***
- Graphical representations are ***two-dimensional***

Definition of a graphical model

A representation in which information is indexed by two-dimensional location

J.H Larkin & H.A. Simon:1987

What is a good graphical model?



From R.N.Shepard:90

It does matter!

Research in diagrammatic reasoning shows that the form of representations has an equal, if not greater, influence on cognitive effectiveness as their content

D.L. Moody:2009

What is security?

- OR more specific: What is **cybersecurity**?

Information security

Preservation of confidentiality, integrity and availability of information

ISO/IEC 17799:2005

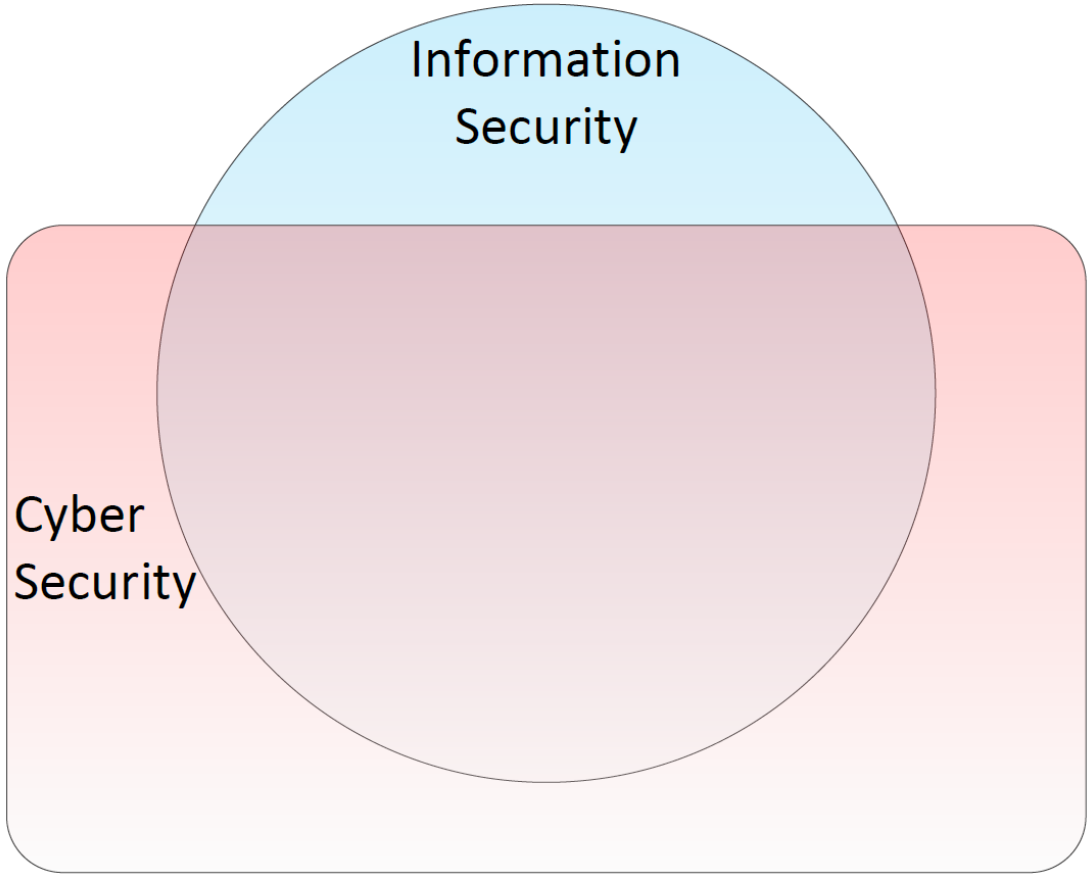
From information security to cyber security: Step 1

- Prevention of **cyber** incidents with respect to the confidentiality, integrity and availability of information

From information security to cyber security: Step 2

- Prevention of **cyber** incidents with respect to the confidentiality, integrity and availability of information **and infrastructure**

Information security vs cyber security, summarised



What kind of approaches for graphical modelling are there?

- Software engineering
  - Flow-charts
  - Entity-relation diagrams
  - Use-case diagrams
  - State-machines
  - Activity diagrams
  - Sequence diagrams
- Statistics/risk analysis
  - Tables
  - Trees
  - Graphs

What kind of approaches for graphical modelling **of security** are there?

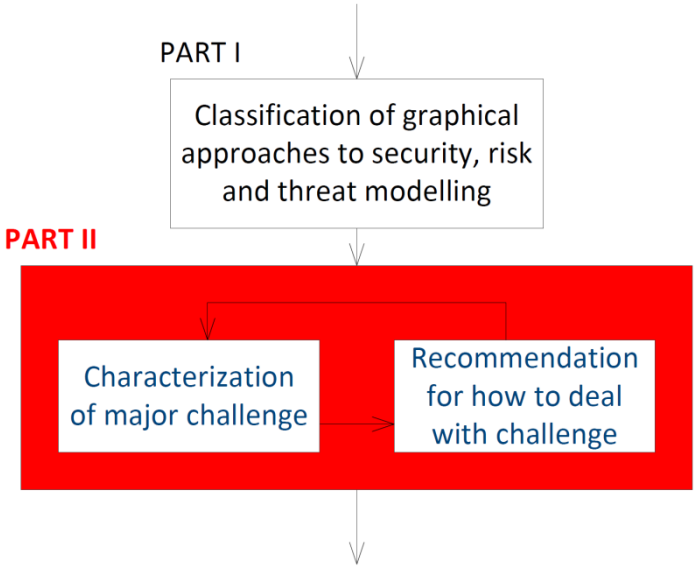
- Software engineering
  - Flow-charts → **Security flow-charts** (*M.Abi-Antoun et al:2007*)
  - Entity-relation diagrams → **Secure UML** (*T.Lodderstedt et al:2002*)
  - Use-case diagrams → **Misuse-case diagrams** (*G.Sindre et al:2000*)
  - State-machines → **Bell–LaPadula** (*W.Caelli et al:1994*)
  - Activity diagrams → **UMLSec** (*J.Jürjens:2004*)
  - Sequence diagrams → **Deontic STAIRS** (*B.Solhaug:2009*)
- Statistics/risk analysis
  - Tables → **DREAD tables** (*MICROSOFT:2003*)
  - Trees → **Attack trees** (*B.Schneier:1999*)
  - Graphs → **CORAS threat diagrams** (*M.S.Lund et al:2011*)

What makes graphical models for security **special**?

- Misbehaviour
- Human intensions
- Capabilities
- Defences
- Vulnerabilities
- Soft as opposed to hard constraints

Part II

- Major challenges within graphical modelling with particular focus on security, risk and threats
- Recommendations for how to deal with these challenges

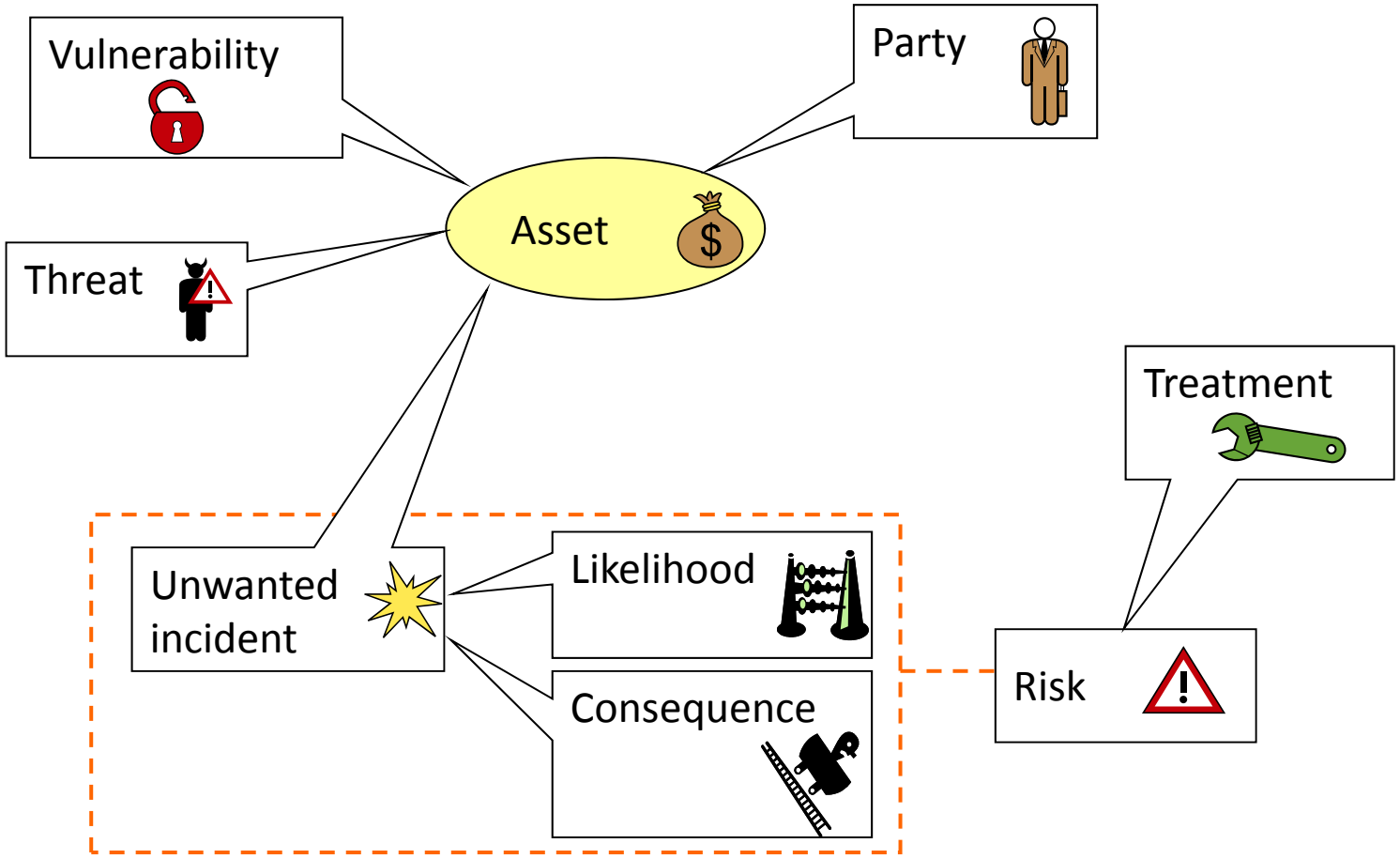


Seven iterations

1. Relationship to ontology
2. The number of symbols
3. What kind of symbols
4. Semantics
5. Documenting consequence
6. Documenting likelihood
7. Documenting risk

Challenge 1: Relationship to ontology

Ontology for risk modelling



Make sure to avoid

- Construct deficit
- Construct overload
- Construct redundancy
- Construct excess

Challenge 2: The number of symbols?

The amount of information that is transmitted by a human being along one dimension is seven, plus or minus two

(G.A. Miller:1956)

Most humans cannot reliably transmit more than

- 6 pitches (tones)
- 5 levels of loudness
- 4 tastes of salt intensities
- 10 visual positions (short exposure)
- 5 sizes of squares
- 6 levels of brightness

Fix: Use several dimensions!

Challenge 3: What kind of symbols

(D.L.Moody:2009) recommends amongst others

- Different symbols should be clearly distinguishable
- Use visual representations suggesting their meaning
- Include explicit mechanisms to deal with complexity
- Include explicit mechanisms to support integration
- Use the full range of capacities of visual variables

Be aware of the theory of gestalt psychology

- Law of proximity
- Law of similarity
- Law of closure
- Law of symmetry
- Law of common fate
- Law of continuity
- Law of good gestalt
- Law of past experience

Challenge 4: Semantics

What is a semantics?

Why do we bother to define semantics?

- You need more than one semantics
- Start by defining a natural language semantics
- Make sure the semantics works for incomplete diagrams
- Be careful with hidden constraints
- The ability to capture inconsistencies is often a good thing

Challenge 5: Documenting consequence

When I was young and stupid I measured any loss, impact or consequence in monetary value

That's not a good idea!

Fix

- Define assets carefully
- Decompose or try to avoid fluffy assets
- Define concrete scales for each asset

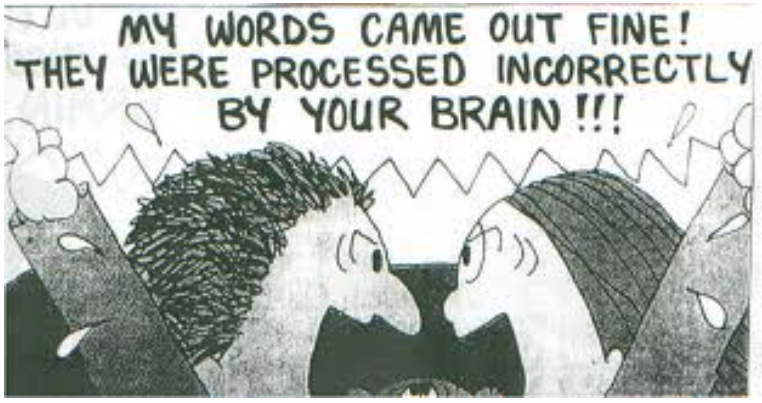
Challenge 6: Documenting likelihood

Bad communication: Probability (G. Gigerenzer:2002)

- "30-50% probability for sexual problems if you take for Prozac" means ...
  - of 10 times you have sex, you will get problems in 3-5?
  - of 10 patients, 3-5 will get problems?
  - ...

Bad communication: Probability

- Implicit reference – invites missunderstandings
- Fix: Use frequencies
  - "Of 10 patients 3-5 will get sexual problems"



http://www.fun-damentals.com/tag/communication/, 19/3-2014

Challenge 7: Documenting risk

Bad communication: Relative risk (G. Gigerenzer:2002)

- "People with a high level of colestreaol may reduce their risk of death by 22 % by taking medicine X"

- Basis for statement (Treatment in 5 years):

Treatment	# deaths pr 1000 with high colestreaol
Medicine X	32
Placebo	41

$$\frac{41 - 32}{41} = 22\%$$

Bad communication: Relative risk

- Often missunderstood as follows: "If 1000 persons with high colestreole takes medicine X, 220 will be saved."

- Fix: Formulate as absolute risk reduction:
  - Medicine X reduces the number of deaths from 41 to 32 per 1000.
  - The absolute risk reduction is 9 per 1000, i.e. 0,9 %.

Conclusions

The form of representations has an equal, if not greater, influence on cognitive effectiveness as their content

D.L. Moody:2009

There is a vast literature based on empirical research from which we may learn!

References

- M. Abi-Antoun, D. Wang, P. Torr. Checking Threat Modeling Data Flow Diagrams for Implementation Conformance and Security. ASE, 2007
- W. Caelli, D. Longley, M. Shain (eds). Information security handbook. MacMillan, 1994.
- W.D. Ellis (ed). A source book of gestalt psychology. The Gestalt journal press, 1997.
- G. Gigerenzer. Calculated risks. How to know when numbers deceive you. Simon and Schuster, 2002.
- ISO/IEC 17799. Information technology – Security techniques – Information security management systems. 2005.
- M.J. Jorden (ed). Learning in graphical models. MIT Press, 1998.
- J. Jürjens. Secure systems development with UML. Springer, 2004.
- B. Kordy et al. DAG-based attack and defence modeling: Don't miss the forest for the attack trees. arXiv:1303.7397 [cs.CR].
- J.H. Larkin, H.A. Simon. Why a diagram is (sometimes) worth ten thousands words. Cognitive Science Vol 11, 1987.
- W. Lidwell, K. Holden, J. Butler. Universal principles of design. Rockport publisher, 2010.

References

- T. Lodderstedt et al. SecureUML: A UML-based modeling language for model-driven security. UML, 2002.
- M.S. Lund, B. Solhaug, K. Stølen. Model-driven risk analysis: The CORAS approach. Springer, 2011.
- Microsoft. Threat modelling. http://msdn.microsoft.com/en-us/library/ff648644.aspx 2014-04-03.
- G.A. Miller. The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological review. Vol 63, 1956.
- D.L. Moody. The "physics" of notations: Toward a scientific basis for constructing visual notations in software engineering. IEEE Tran. on Soft. Eng. Vol 35, 2009.
- B. Schneier. Attack trees: Modeling security threats. Dr. Jobb's Journal of Software Tools, 1999.
- R. N. Shepard. Mind Sights: Original Visual Illusions, Ambiguities, and Other Anomalies, With a Commentary on the Play of Mind in Perception and Art. Freeman & Co, 1990.
- G. Sindre, A.L. Opdahl. Eliciting security requirements by misuse cases. TOOLS Pasific, 2000.
- B. Solhaug. Policy specification using sequence diagrams. University of Bergen, 2009.
- J. Wagemans et al. A century of Gestalt psychology in visual perception: I. Perceptual grouping and figure-ground organization. Psychol Bull., 2012.
- Wikipedia. Graphical model. http://en.wikipedia.org/wiki/Graphical_model 2014-04-01.