Mathematical Models for Risk Assessment in Utility Networks

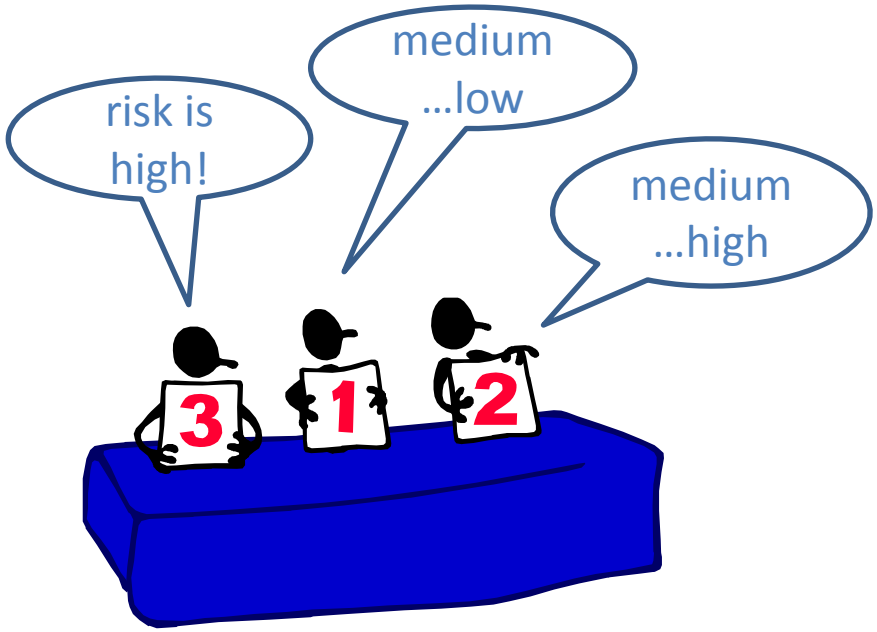
Hybrid Risk Metrics

Sandra König (AIT), Stefan Rass (AAU)

End User Workshop
Vienna 02.11.2015

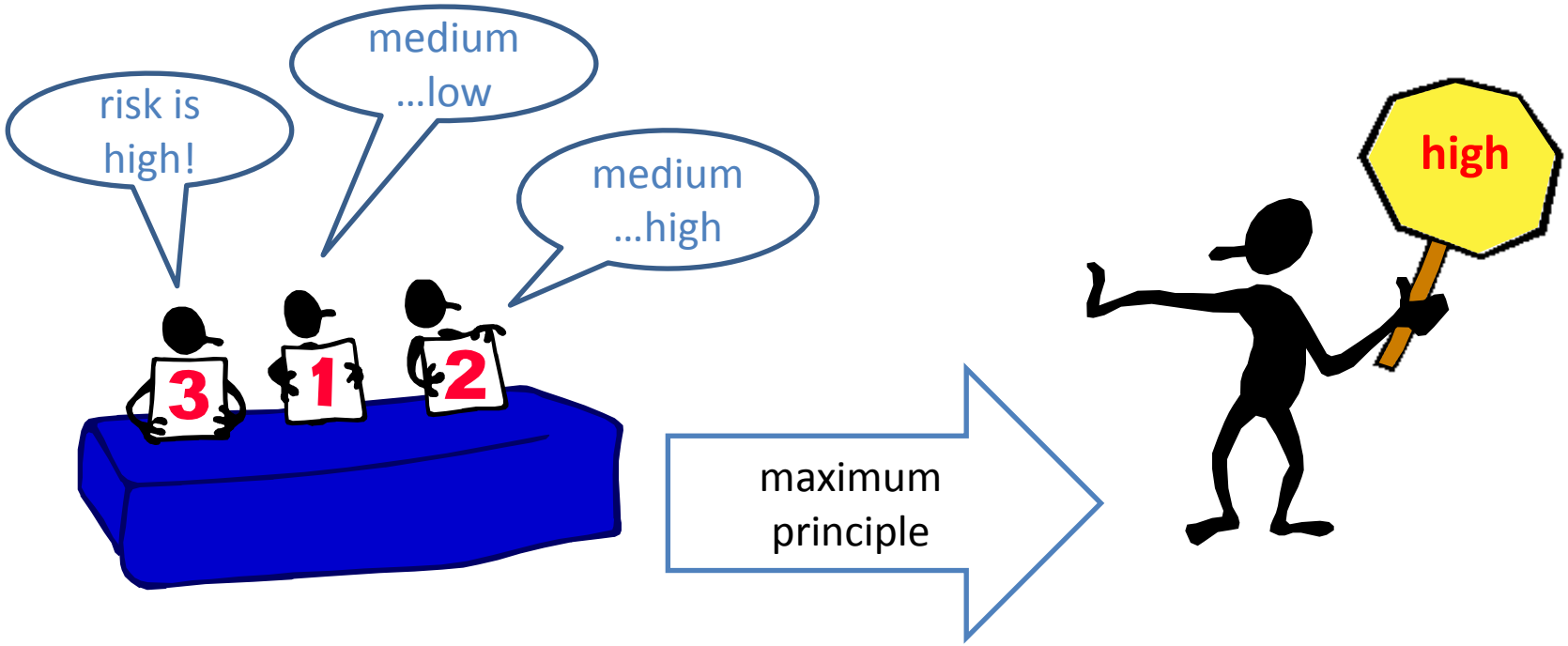
Standard Problem

- Risk elicitation and consequence estimation → based on human expertise
- A standard problem: you ask three people, you get four opinions



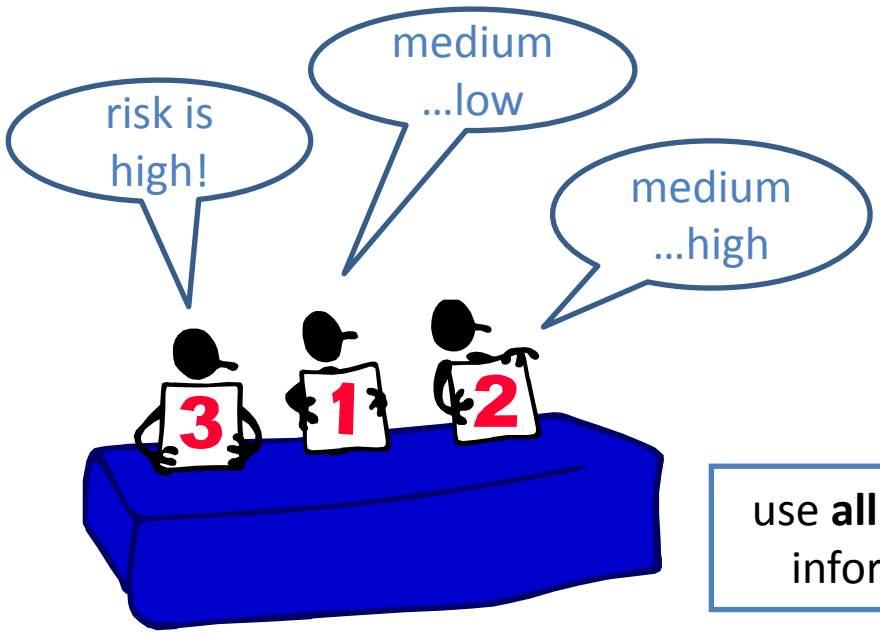
Standard Solution

- Risk elicitation and consequence estimation → based on human expertise
- A standard problem: you ask three people, you get four opinions
- A standard solution: **risk aggregation**

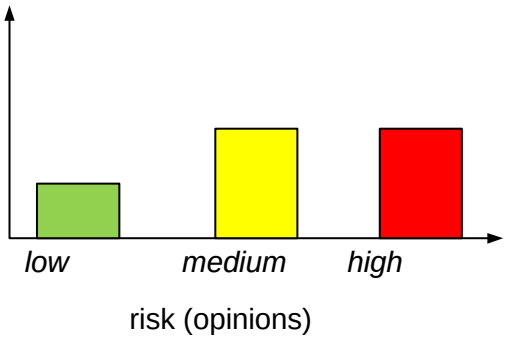


HyRiM Approach

- Risk elicitation and consequence estimation → based on human expertise
- A standard problem: you ask three people, you get four opinions
- **HyRiM approach**: simply don‘t aggregate



use **all** available information



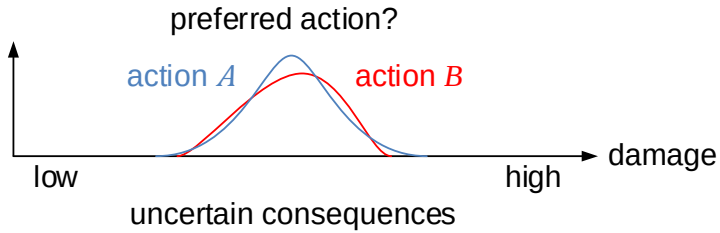
HyRiM Approach

- Multi-criteria risk management using uncertain (ambiguous, vague…) information

- Multiple goals can be optimized using game theory *
- Uncertain information is described in probabilistic terms

→ decisions with uncertain consequences

→ introduce preference relation $\preccurlyeq$



- Game theory helps to compute optimal security strategies automatically

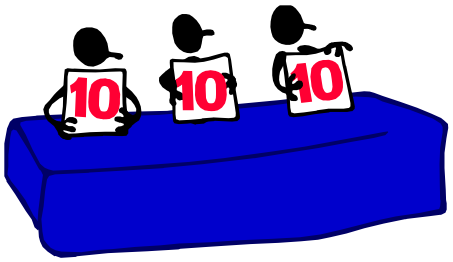
* game with uncertain payoffs

In practice

Intuitive application of reference relation $\preccurlyeq$

→ Basic idea: prefer scenario with smaller likelihood of extreme events

- For opinions: the $\preccurlyeq$-best action is the one with the smallest number of sceptics



- If scenarios can be simulated: the $\preccurlyeq$-best action is the one with the smallest number of simulated extreme outcomes

Infection of a Network

How sensitive is a network to viral infection of one component (e.g. due to BYOD at node 19)?

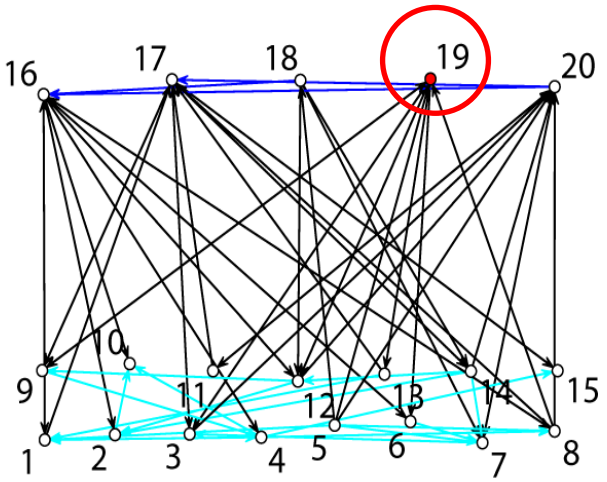
Consider different nature of edges

How many nodes are affected after a certain period of time?

Same approach can be applied to

- Spread of epidemics
- Social risk response
- ... and others

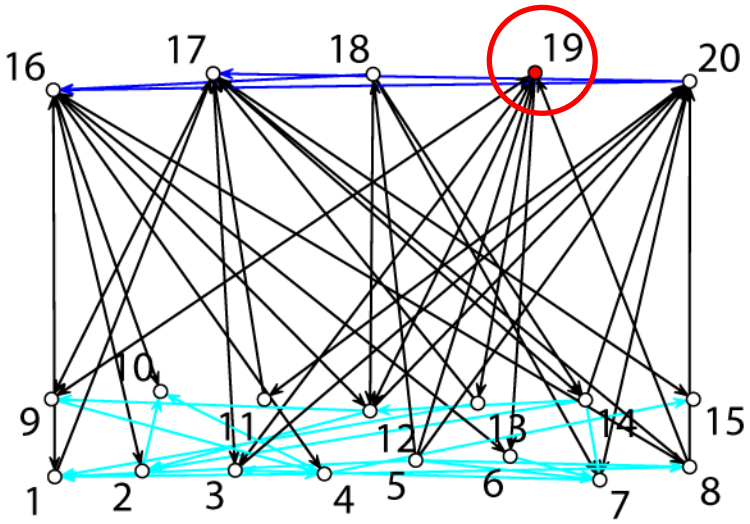
SCADA network monitoring a real network (e.g. water supply)



BYOD Infection – Time t_0

- How sensitive is a network to infection of one component?

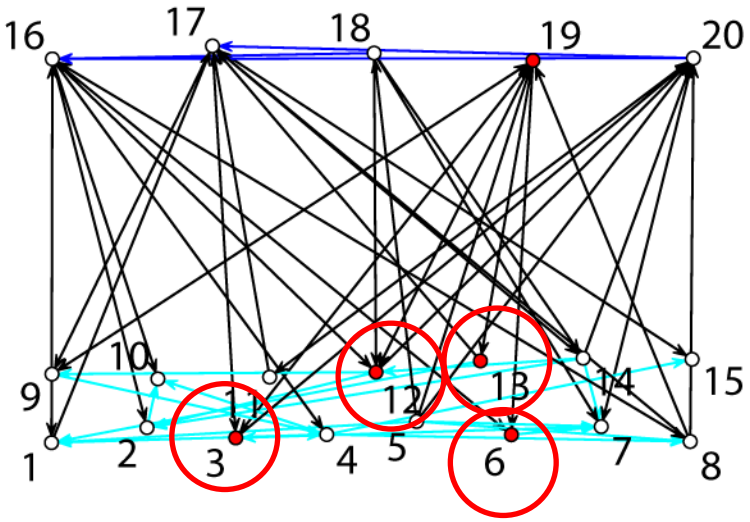
infected
nodes: 1 (initial outbreak)



BYOD Infection – Time t_1

- How sensitive is a network to infection of one component?

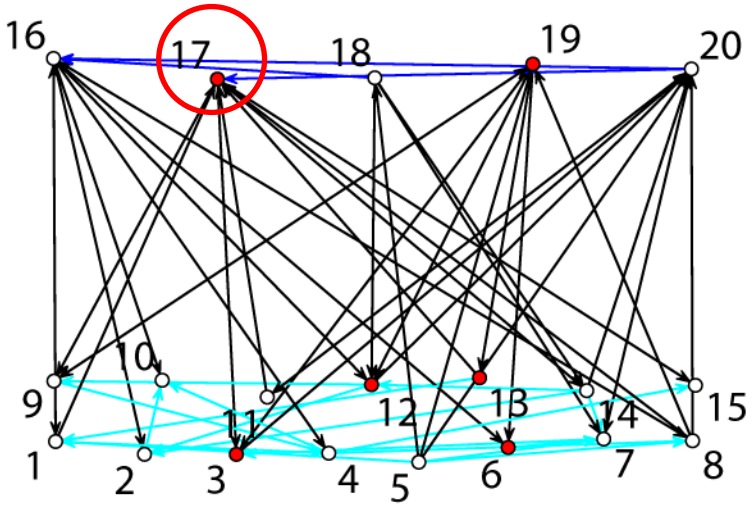
infected
nodes: 5 (+4)



BYOD Infection – Time t_2

- How sensitive is a network to infection of one component?

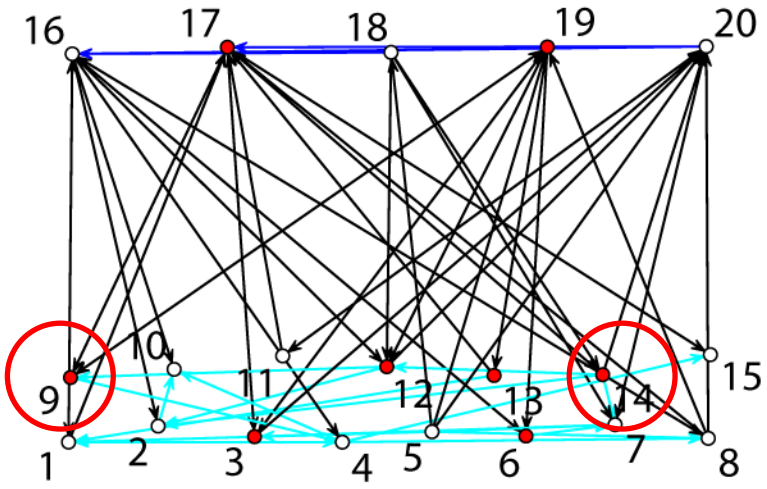
infected
nodes: 6 (+1)



BYOD Infection – Time t_3

- How sensitive is a network to infection of one component?

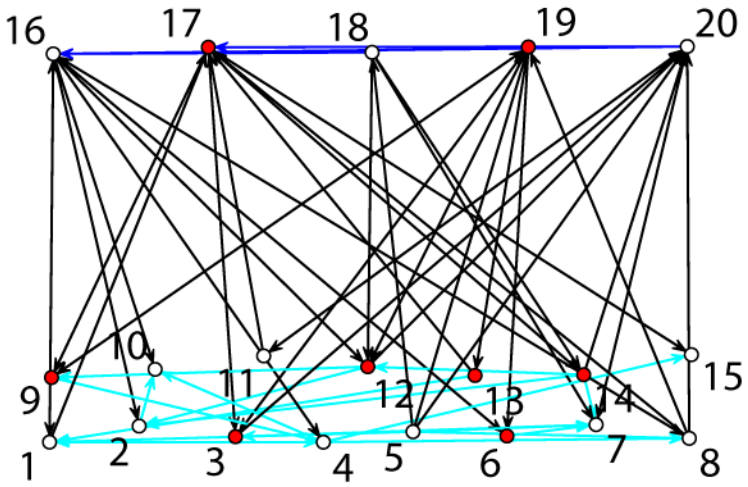
infected nodes: 8 (+2)



BYOD Infection – Time t_4

- How sensitive is a network to infection of one component?

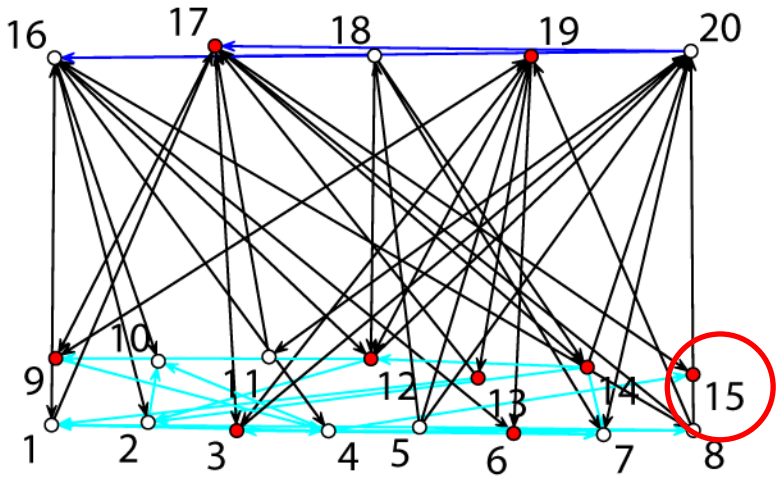
infected
nodes: 8
(no new infections)



BYOD Infection – Time t_5

- How sensitive is a network to infection of one component?

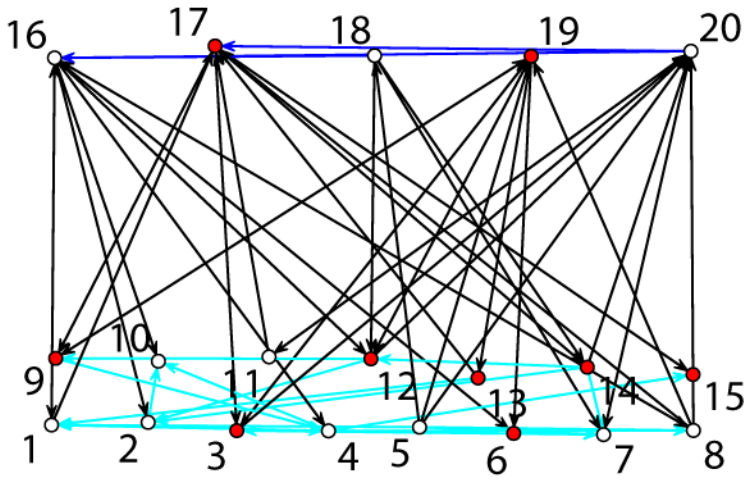
infected
nodes: 9 (+1)



BYOD Infection – Time t_6

- How sensitive is a network to infection of one component?

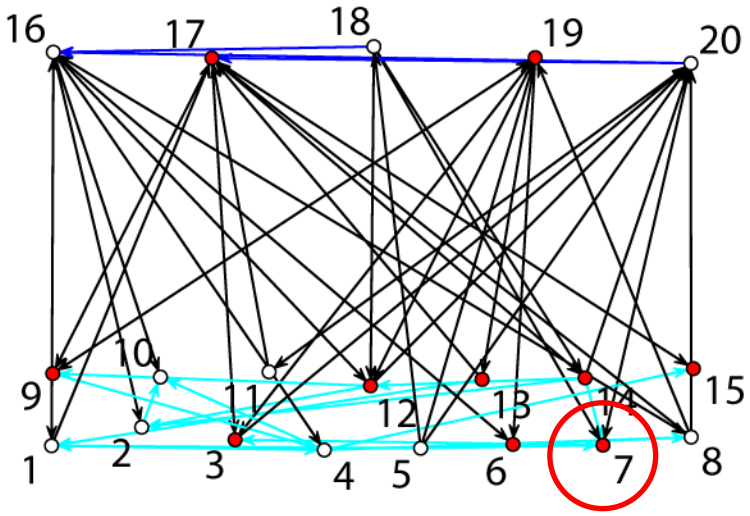
infected
nodes: 9
(no new infections)



BYOD Infection – Time t_7

- How sensitive is a network to infection of one component?

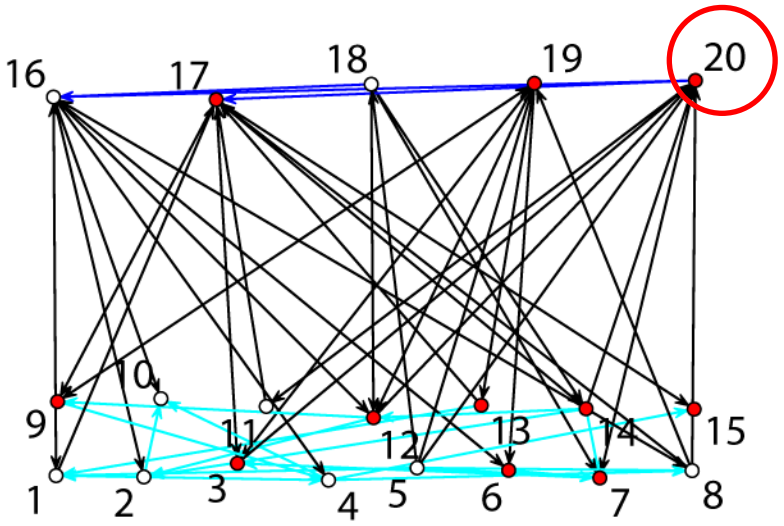
infected
nodes: 10 (+1)



BYOD Infection – Time t_8

- How sensitive is a network to infection of one component?

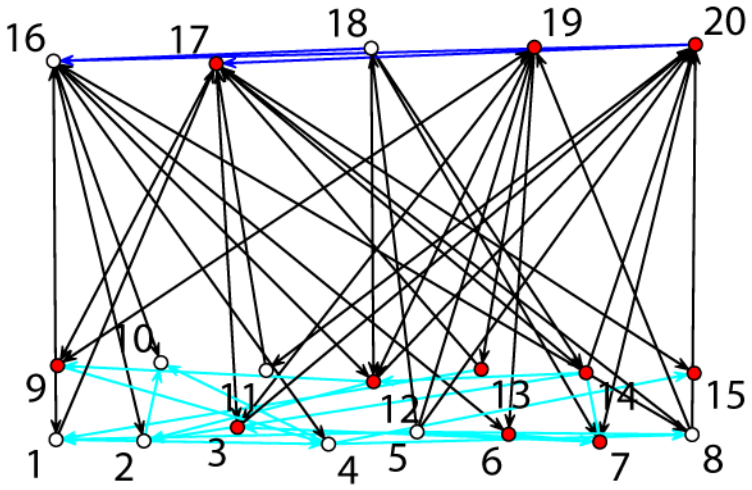
infected
nodes: 11 (+1)



BYOD Infection – Time t_9

- How sensitive is a network to infection of one component?

infected
nodes: 11
(no new infections)

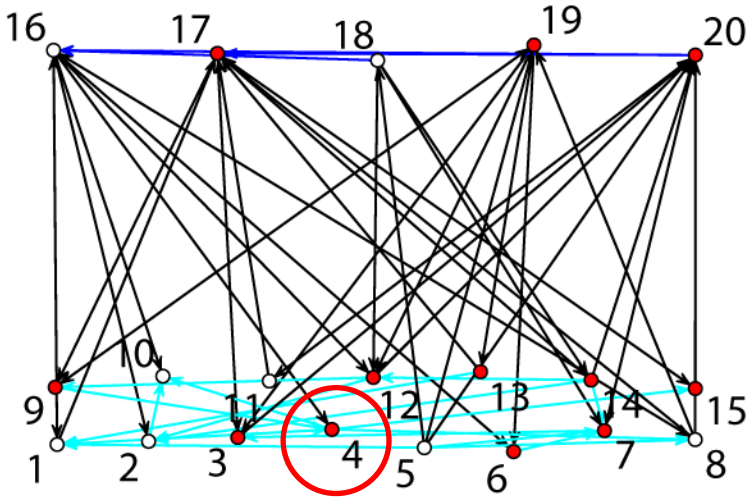


BYOD Infection – Time t_{10}

- How sensitive is a network to infection of one component?

infected
nodes: 12 (+1)

Total infection: 60%



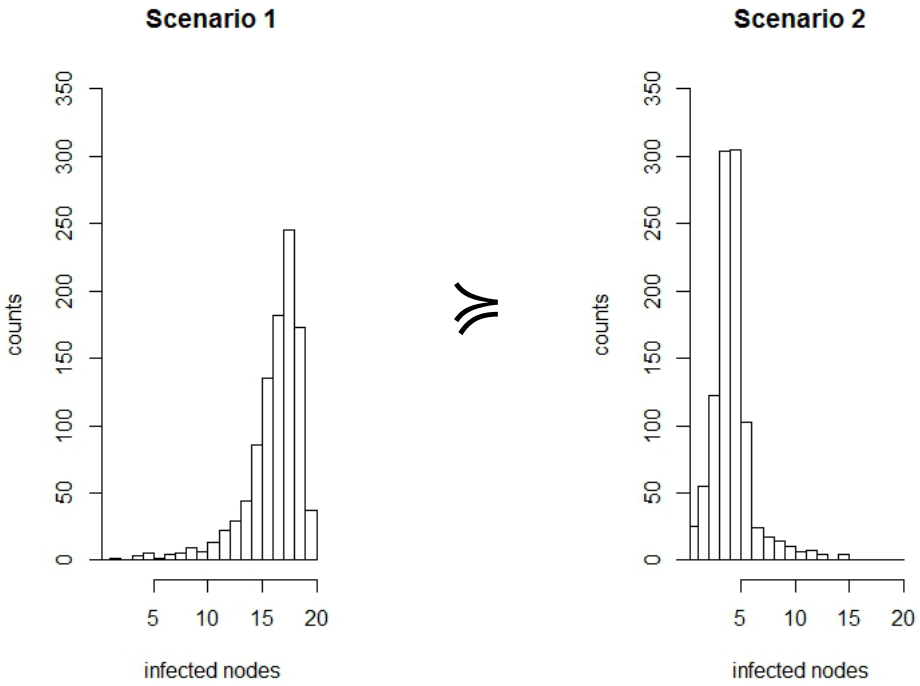
Risk Management Problem

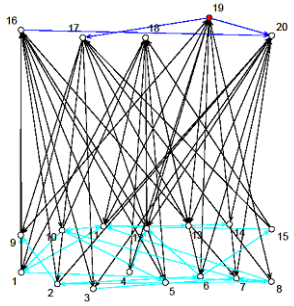
- The risk managers problem: “Which is the best action to minimize risk?”
  - Option 1: change communication patterns (organisational control)
  - Option 2: enhance link protection (technical control)
- Solution: use the $\preccurlyeq$- preference relation devised in HyRiM to compare uncertain consequences corresponding to different scenarios

Example

Simulation of error propagation on example network

- Scenario 1: frequent status updates (black links, current setting)
- Scenario 2: occasional status updates

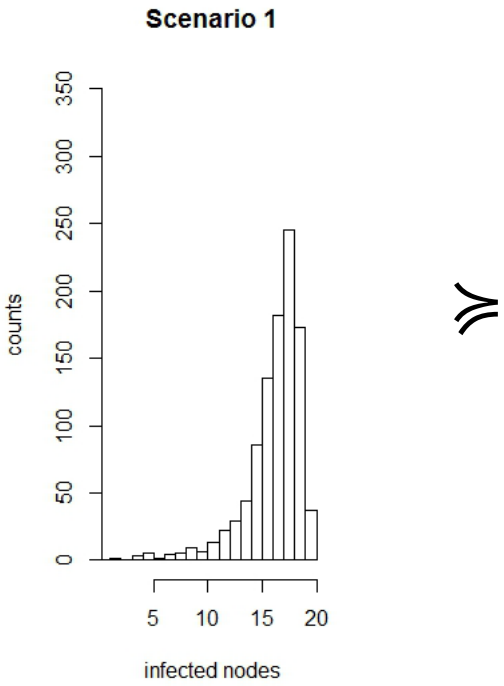


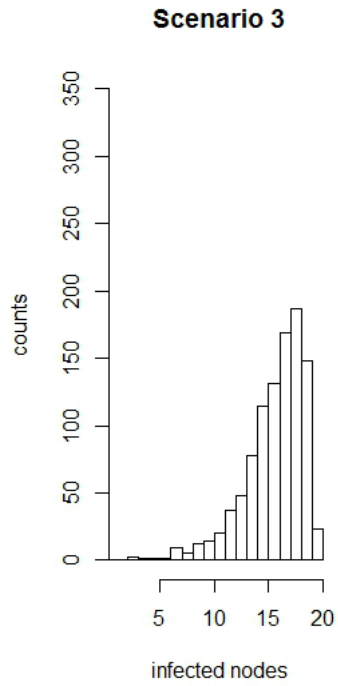


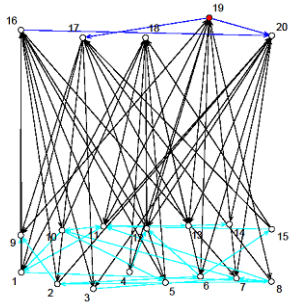
Example

Simulation of error propagation on example network

- Scenario 1: existing SCADA link protection (existing IDS)
- Scenario 3: enhanced protection (random spot checks for malware)

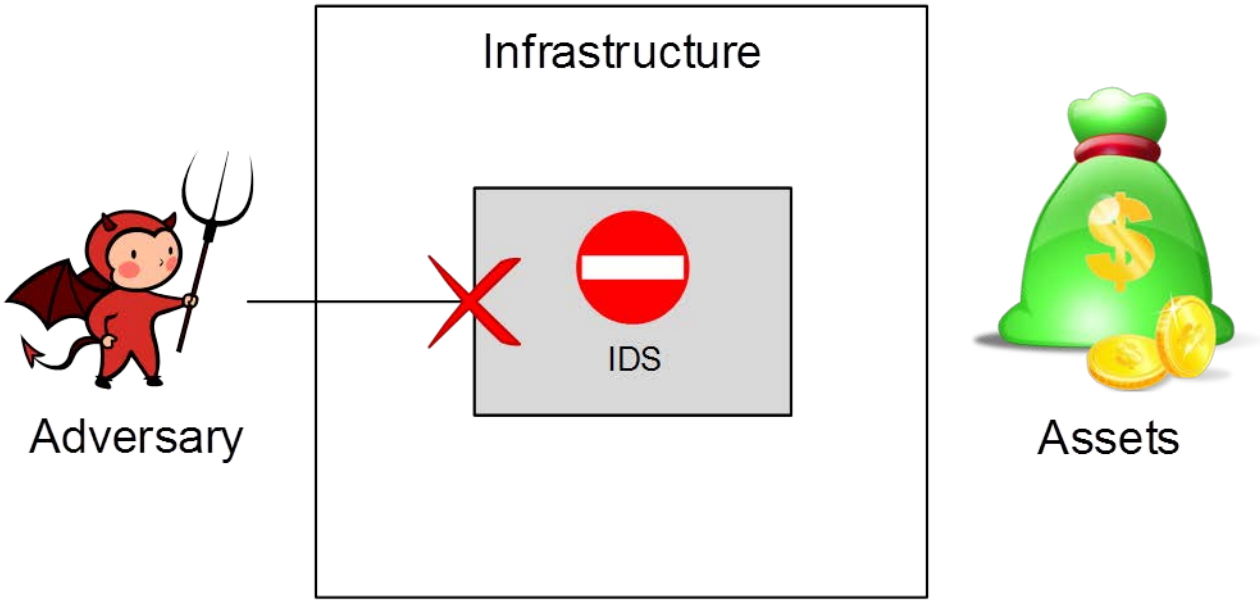






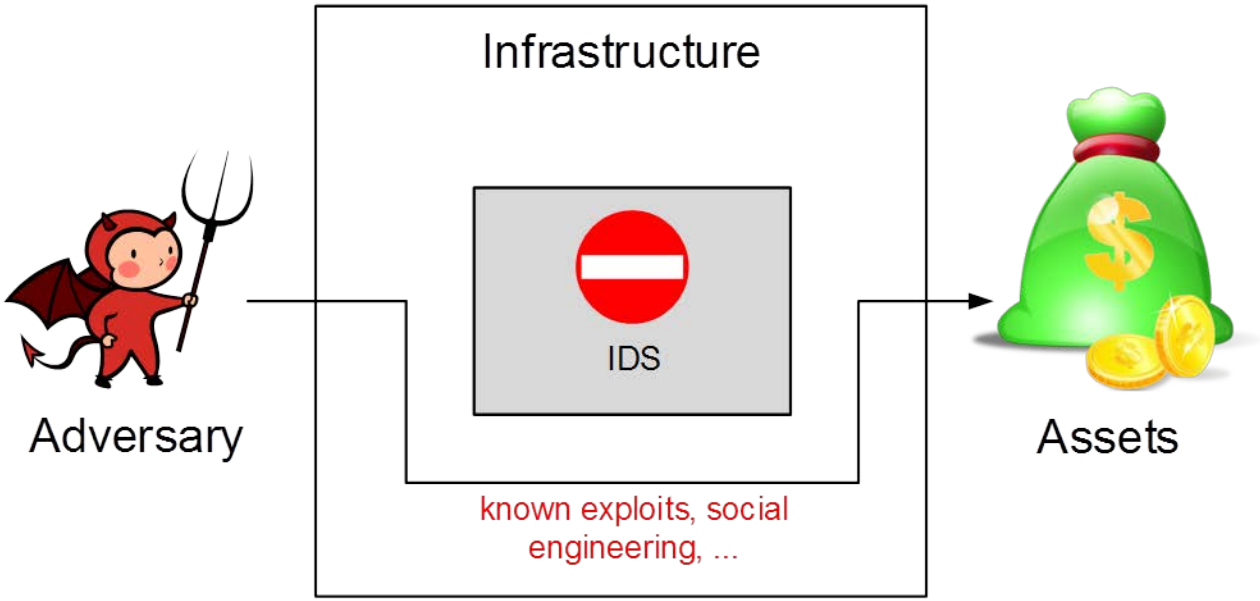
Choosing Actions

- What a fixed security policy (alone) can do:
  It blocks the direct (known) ways into the system…



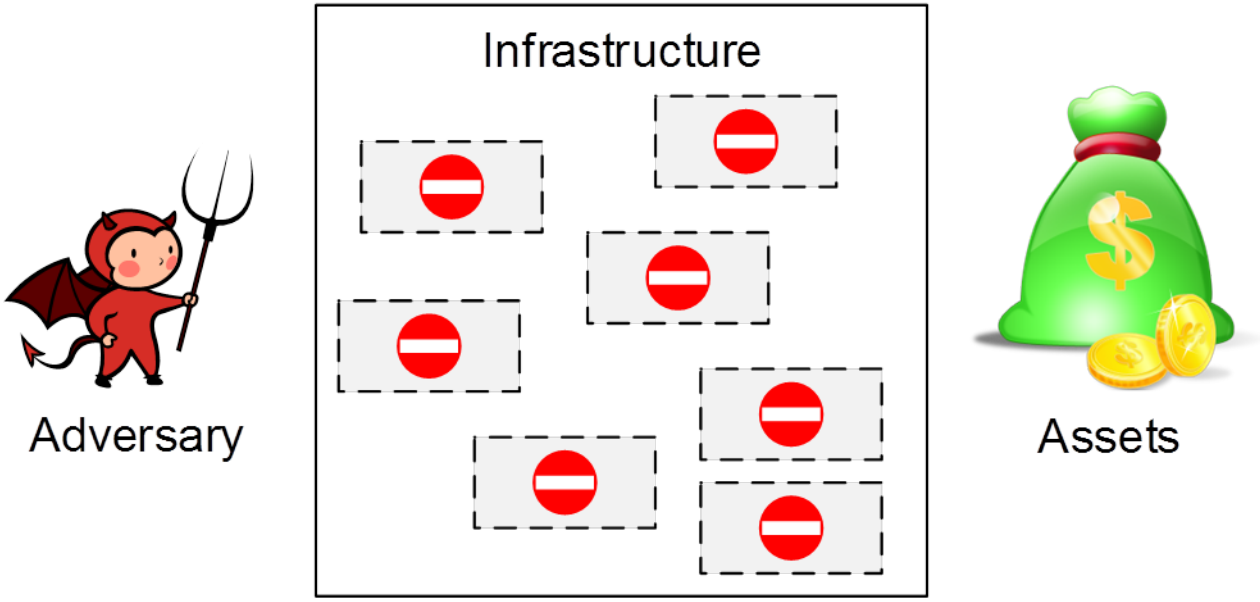
Choosing Actions

- What a fixed security policy (alone) can do:
  It blocks the direct (known) ways into the system…
  …but may fail to protect against indirect access



Choosing Actions

- What HyRiM adds to standard risk management (ISO27000, …):
  Risk diversion by “optimized” usage of the infrastructure, e.g., where to do the spot-checks and how often should we do them?



Summary

- HyRiM supports multi-criterial risk management decisions with uncertain effects
  - New method to compare vague consequences
  - Find optimal decisions using game theory

- HyRiM aids risk management as prescribed by
  - ISO 27005
  - ISO 31000
  - BSI Grundschutz
  - … and others