

Analyzing Security Decisions with Discrete Event Simulation

Presentation of master thesis, Gjøvik University College
Magnus Felde

Agenda

- ▶ Problem description and motivation
- ▶ Approach for answering the research questions
- ▶ The results
- ▶ Example of contribution

Problem description and motivation

- ▶ **Information security**
 - ▶ Necessary for a organization to succeed
 - ▶ Must be aligned with the business
 - ▶ Funding requires justification

Problem description and motivation

- ▶ Determine the cause-and-effects of a security decision
 - ▶ Does security decisions affect organizational goals?
- ▶ A measure which incorporates organizational performance, e.g. Key Performance Indicators (KPIs)
 - ▶ Are KPIs suitable for measuring the effects of a security decision?
- ▶ A method to represent the organization and provide insight, without disrupting the business processes
- ▶ Is simulation suitable for determining the effects of a security decision?

Is the use of simulation and KPIs a suitable approach in order to determine the effects of a security decision?

Answering the research questions

- ▶ Created a health care specific scenario



- ▶ Conducted a case study to determine the effects of implementing smart cards as apposed to using passwords
 - ▶ Created a model based on the scenario
 - ▶ Conducted two separate simulation runs
 - ▶ Determined which authentication mechanism is “best”, i.e. which authentication mechanism affects the KPIs in a desirable way
- ▶ Compared the simulation approach with a non-simulation approach

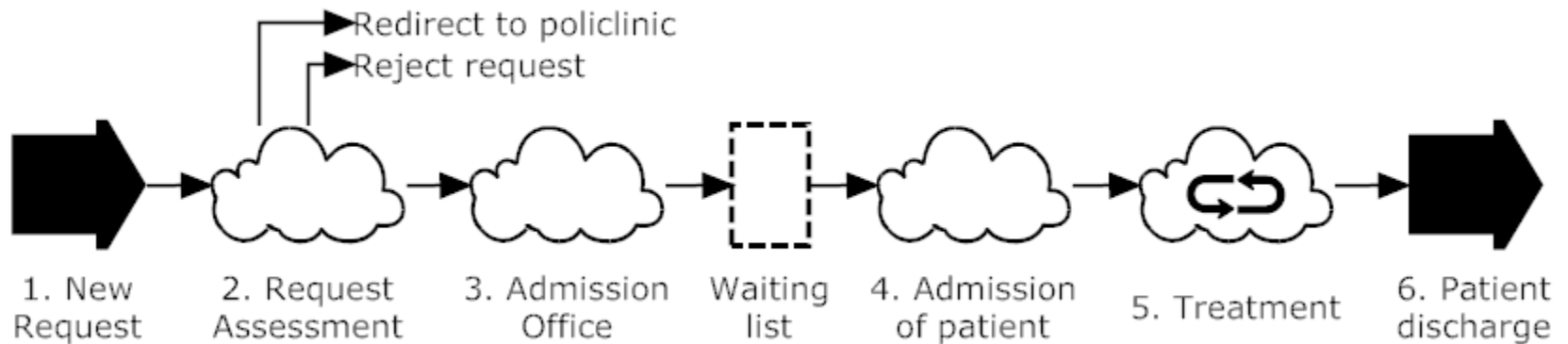
The results

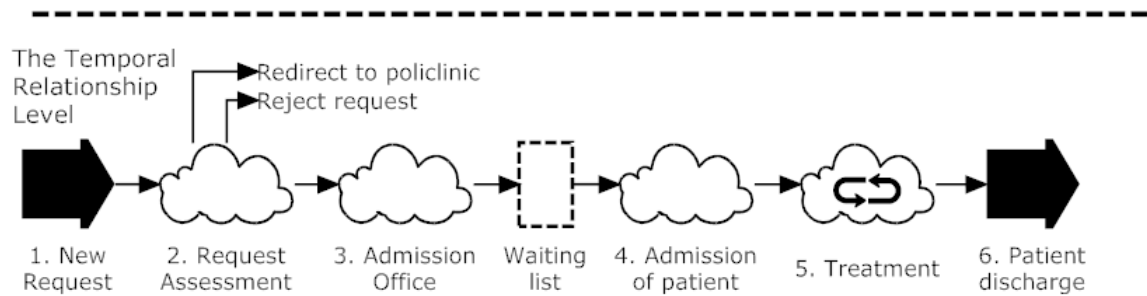
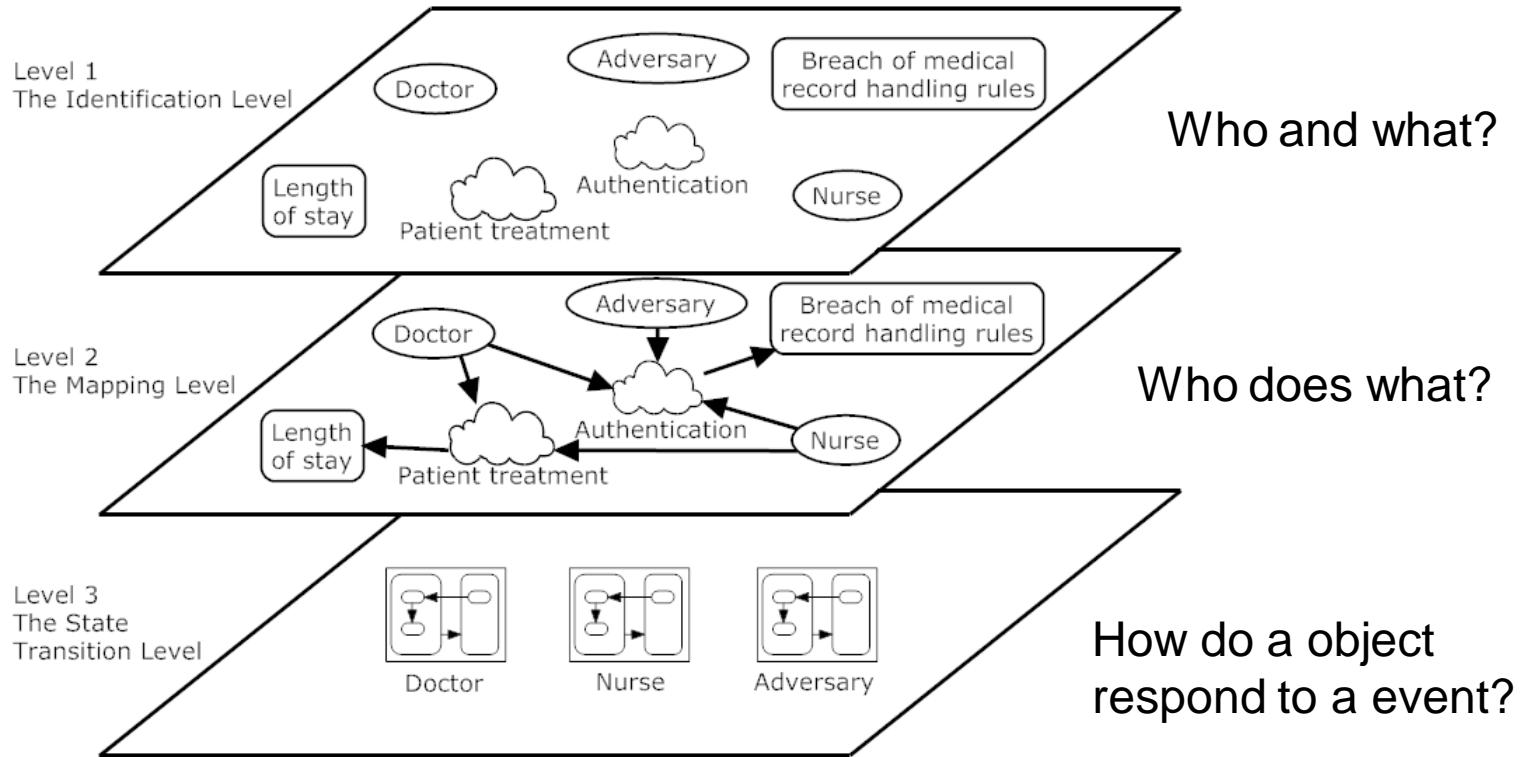
- ▶ Security decisions affect the goals
- ▶ Findings suggest that this effect is possible to measure with the use of KPIs
 - ▶ Different scenarios and KPIs are needed to confirm this results
- ▶ Compared to the non-simulation approach, the simulation approach
 - ▶ Less cost-effective
 - ▶ Weak relationship between input data and results
 - ▶ Suitable for conducting “what if” analyses
- ▶ Data collection is a very important, but a difficult and time consuming task - regardless of approach.
 - ▶ Especially true in the area of information security

Example of contribution:

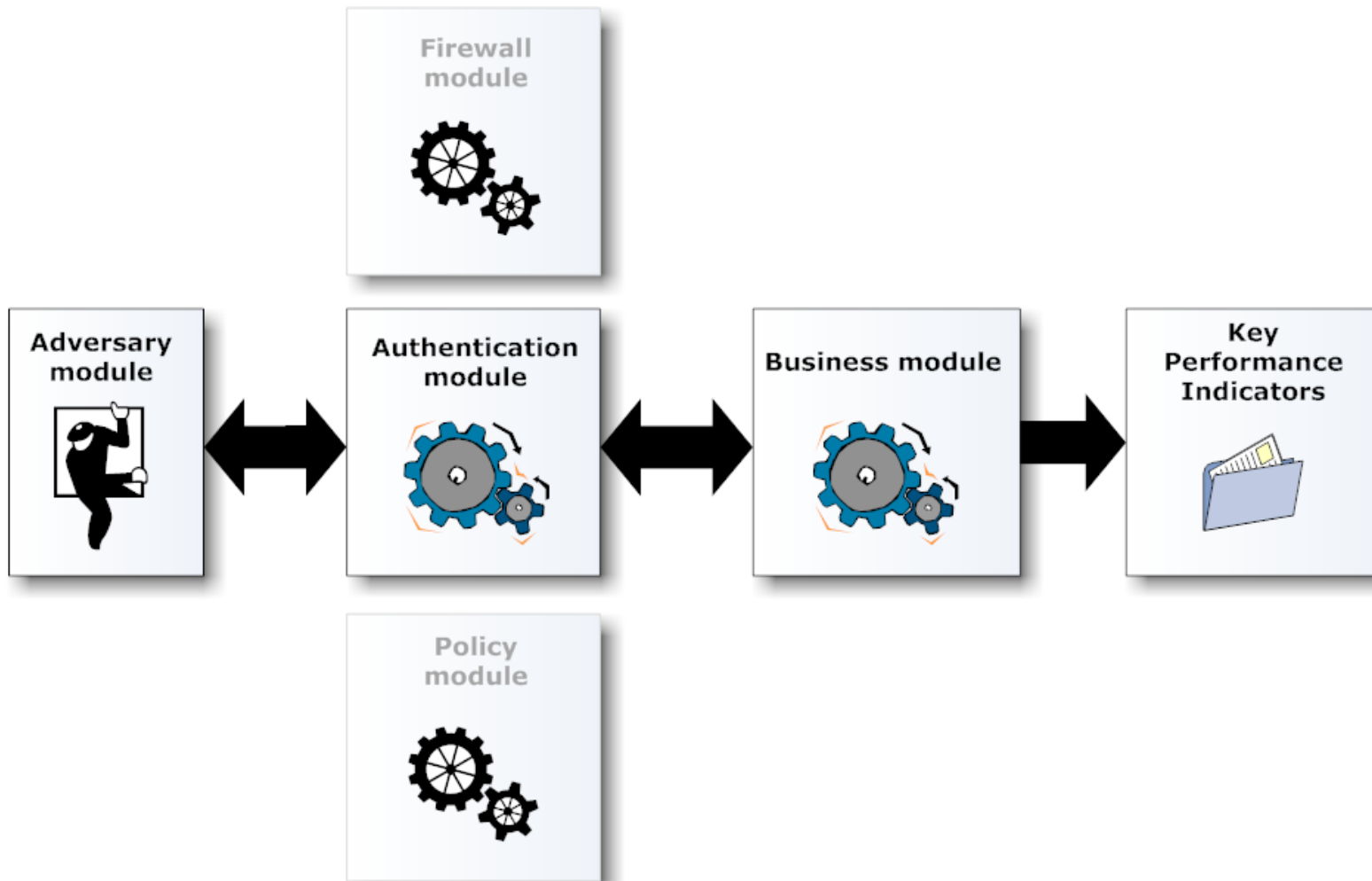
- ▶ **Minimalistic Model Design (MIMD) methodology**
 - ▶ Helps to identify relevant KPIs, objects and events
 - ▶ Reduces the complexity of the system of interest
 - ▶ Creates a model based on modularization

Patient treatment process





Model based on modules



Thank you for your attention!

Questions?

