# Human modeling for IoTSec

Adam Szekeres
30.08.2017
Institute for Technology Systems

## Overview

- Importance of investigating human aspects
- Research perspective
- Scenarios
- Feedback

# Importance of focusing on human aspects

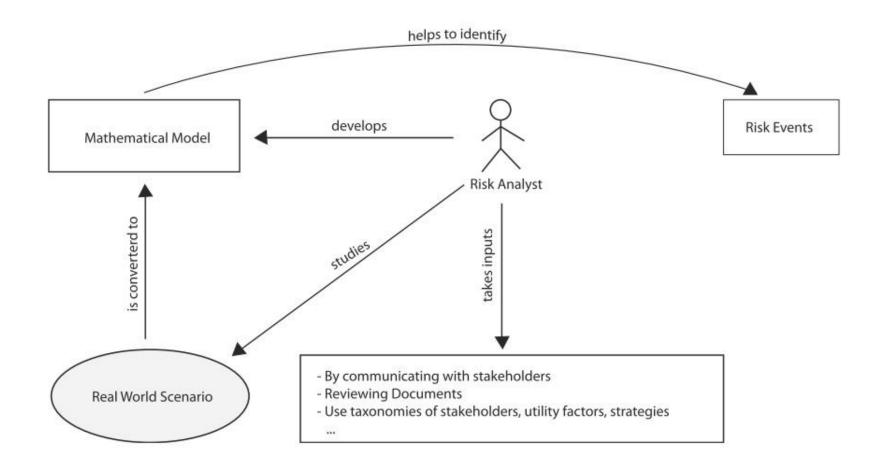
STOCKHOLM (Reuters) - Swedish Prime Minister Stefan Lofven replaced two ministers on Thursday in a scandal over the leaking of sensitive data, trying to contain the damage and stave off an early election.

The scandal involves the handling of data under a 2015 outsourcing deal between the Swedish Transport Agency and IBM Sweden. Lofven admitted on Monday that his country and its citizens had been exposed to risks by potential leaks of sensitive information.

Among some of the details that could have been accessible outside Sweden were the registration numbers of most vehicles on land, air and sea.

#### Reuters

### The Risk Analysis process



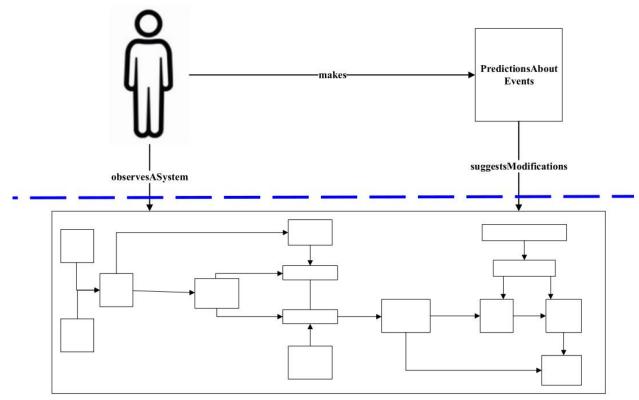
### The big picture – research perspective

I. Enhancement of the method(stakeholder behavior – CIRA)

Artifacts: CIRA + SGAM extension

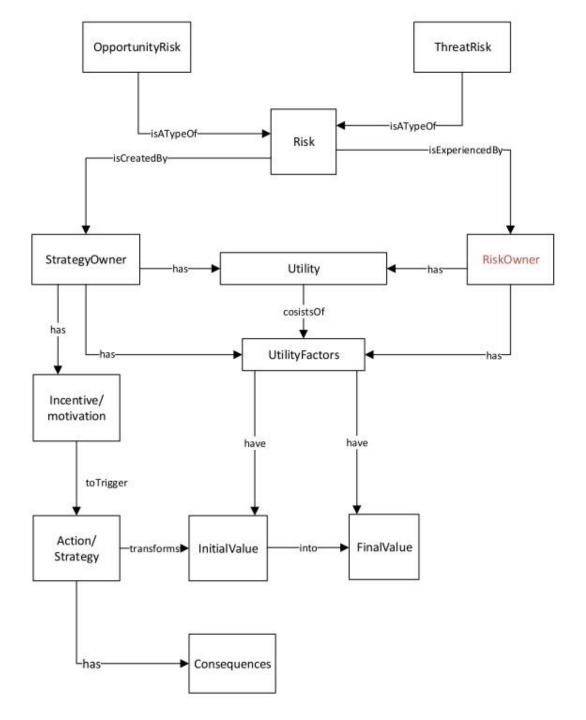
II. Evaluation of the Artifacts(predictive capabilities of the analyst when using CIRA)

#### 2. Activities and performance of the analyst

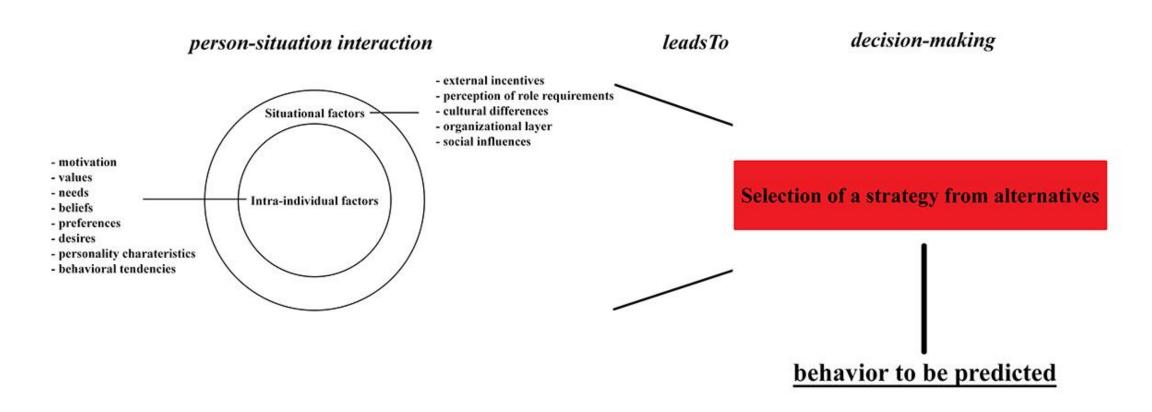


1. The model of a system with human actors

### CIRA – risk framing



# Factors to be included in a model



#### OpportunityRisk ThreatRisk Risk of service disruption due -isATypeOf isATvpeOfto cyber attack -isCreatedBy-DSO Manager Home Owner isExperiencedBv-(StrategyOwner) (RiskOwner) has Utility Utility has cosistsOf cosistsOf -stable supply of el. -profit -comfort -reputation -privacy -compliance -accurate bills Save money (UtilityFactors) (UtilityFactors) (Incentive/motivation) toTrigger Each UtilityFactor has Buy cheap Smart InitialValue FinalValue Devices with weak transforms --security (Action/Strategy) Consequences

### Scenario 1. - choice of equipment

Scenario where the strategy owner (Head of purchasing department at a DSO) is responsible for the procurement of Smart Devices that will be utilized in the grid. When making his choice he has to consider several vendors, that vary in their offers in terms of the security, price and capabilities of the devices.

Is he tempted to choose the cheaper ones that come with weaker security measures, therefore leaving customers more vulnerable to cyber-attacks?

#### OpportunityRisk ThreatRisk Risk of senstive └isATypeOf isATypeOfinformation leakage isCreatedBy DSO Home Owner -isExperiencedBv-(StrategyOwner) (RiskOwner) has Utility Utility has cosistsOf cosistsOf has -stable supply of el. -profit -comfort -reputation -privacy -compliance -accurate bills Save money (UtilityFactors) (UtilityFactors) (Incentive/motivation) toTrigger Each UtilityFactor has Dispose e-waste -transforms Initial Value → FinalValue without making intodata inaccessible (Action/Strategy) Privacy violation / punishment (Consequences)

# Scenario 2. - Privacy violation through improper handling of electronic waste

Storage of sensitive information about customers and the handling of electronic waste (i.e. discarded devices with sensitive information).

What are the existing practices for handling e-waste?

Risk owner: DSO/Customers

Strategy owner: Data Protection Authority/DSO

### Strategies:

- Establish plans that protect privacy after equipment is discarded
- Discard devices without necessary care

# Collaboration

• Establishing collaboration with a PhD student at Eötvös Loránd University (ELTE), Hungary – focus on modeling social psychological aspects

# Your input is needed

Development of a common ontology that includes humans

Results from workshop on DSO needs -> can be converted to utility factors within CIRA for further analysis

Suggestion of other relevant scenarios where DSOs are risk owners?