ADAPTIVE SECURITY

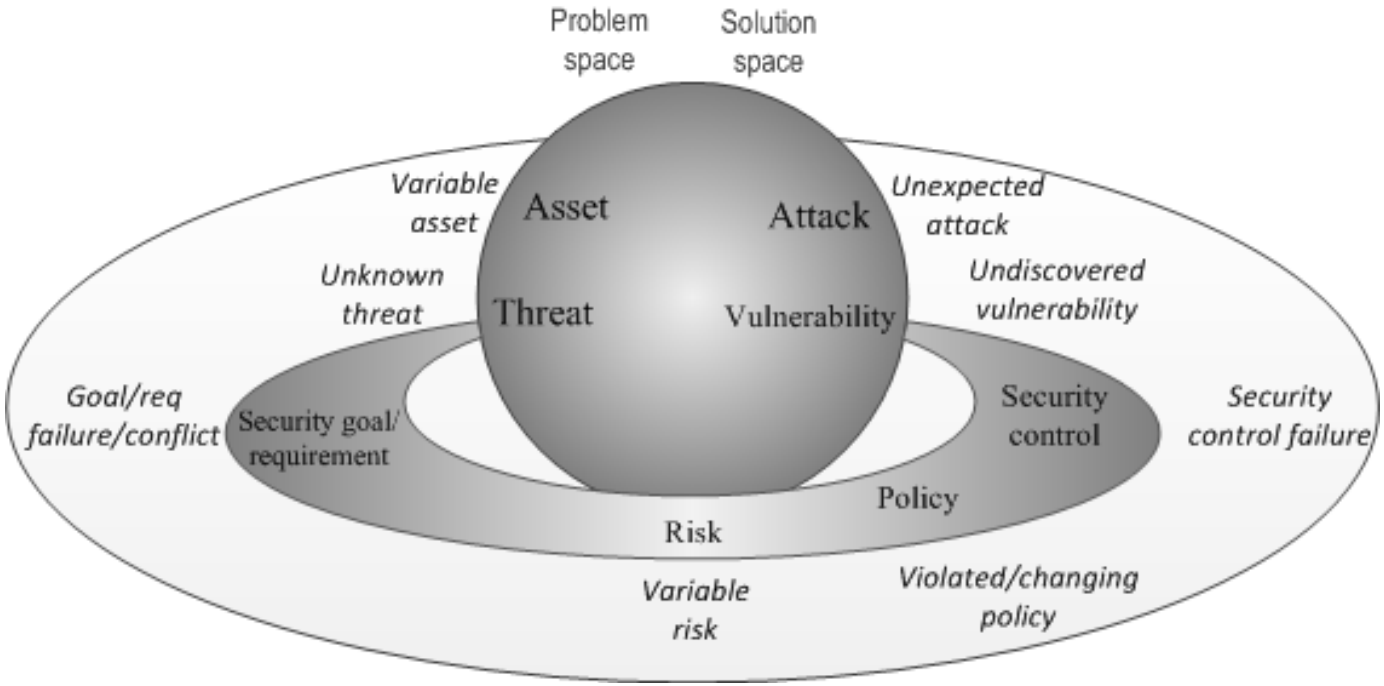
A Requirements-Driven Approach

Mazeiar Salehie
EASSY, Japan
September 2013

SHONAN MEETING
NII

lero THE IRISH SOFTWARE ENGINEERING RESEARCH CENTRE

Adaptive Security

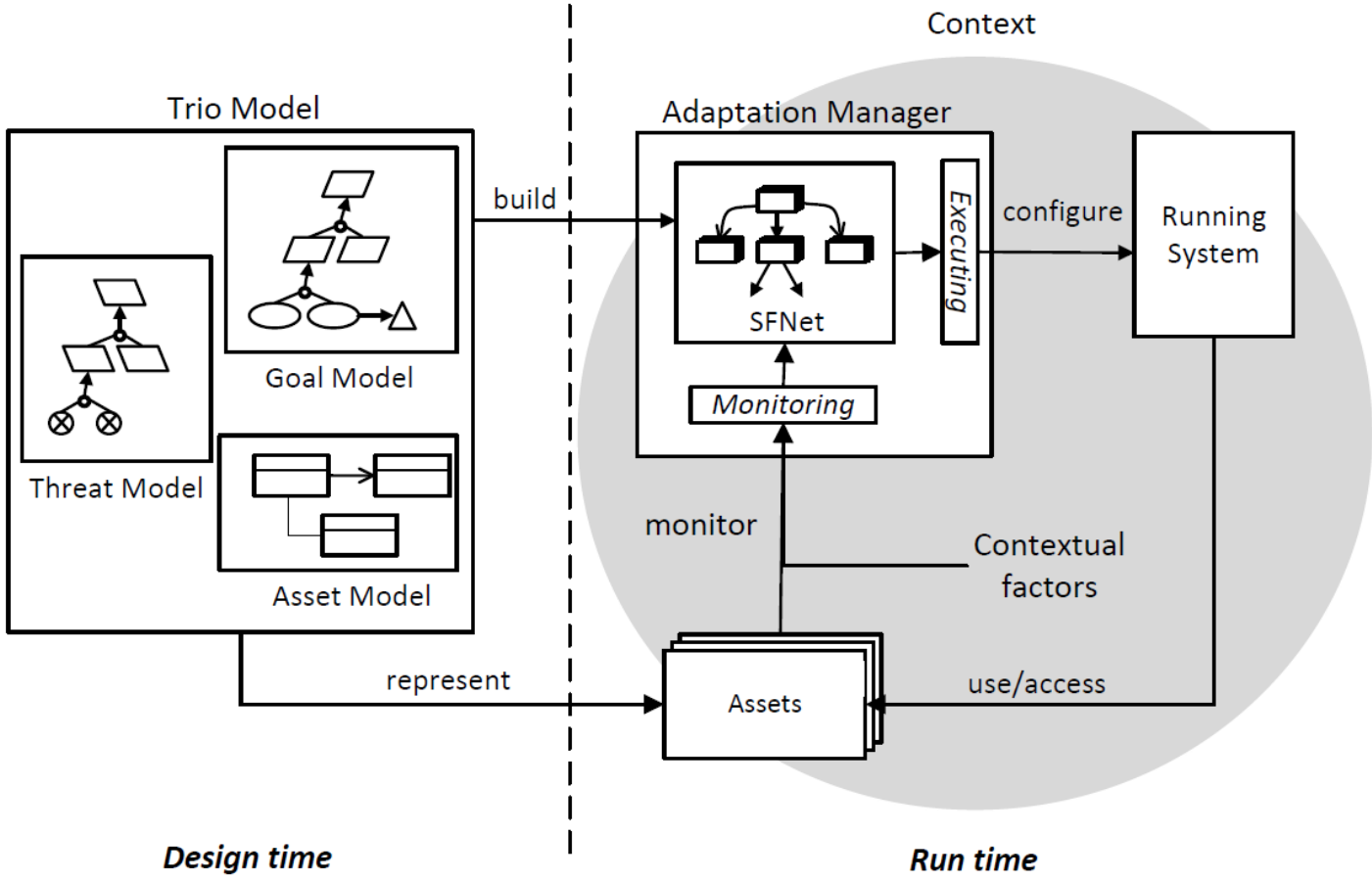


Saturn model

Adaptive security: Our Focus

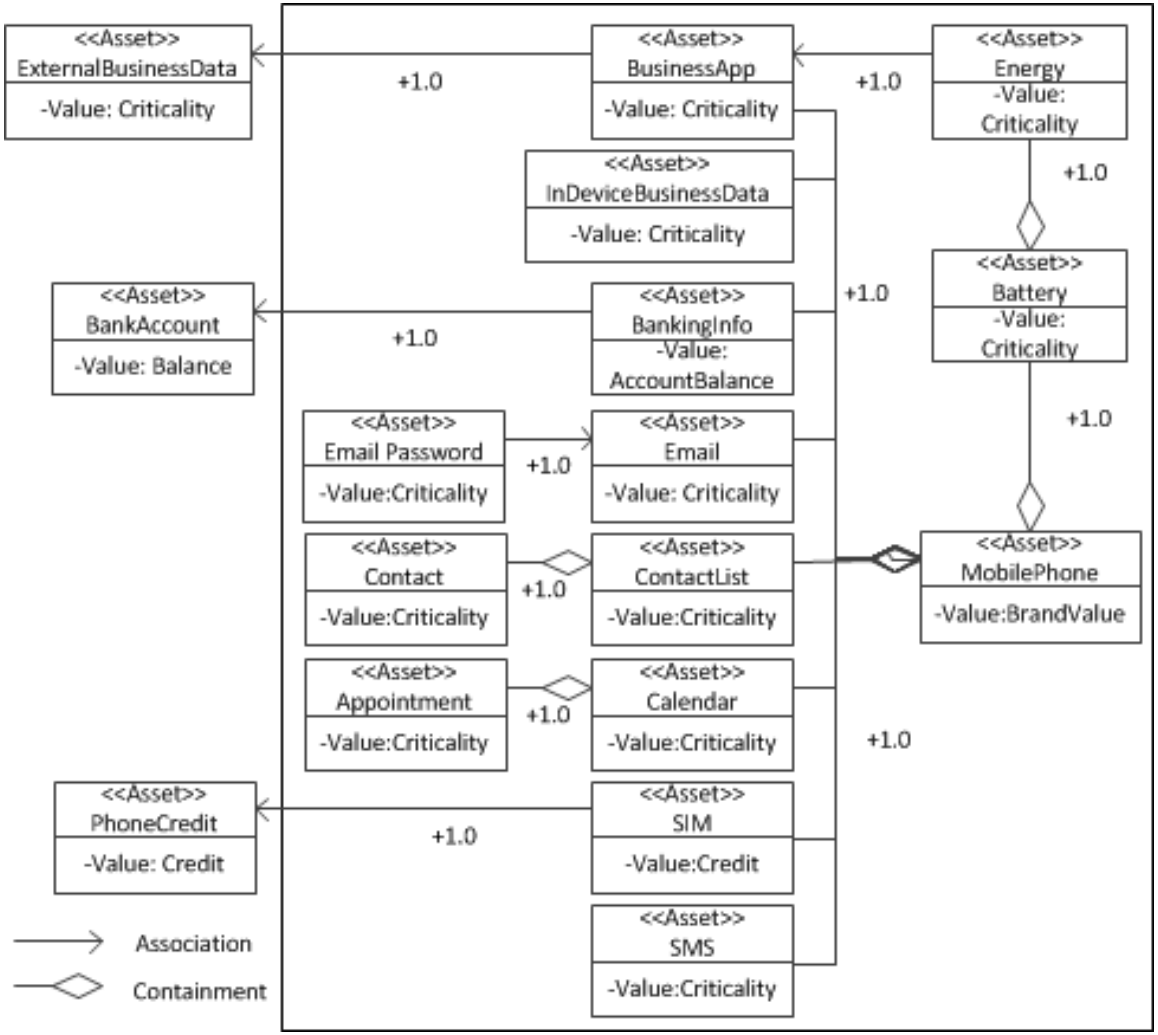
- Protecting valuable assets as the main goal of security
  - Changes in assets should be monitored
  - Security goals should be adequately satisfied all the time with considering other goals
- Proactive adaptive security
  - Asset variability, threat variation, risk fluctuation, changing context without harms to assets

Adaptive Security Framework

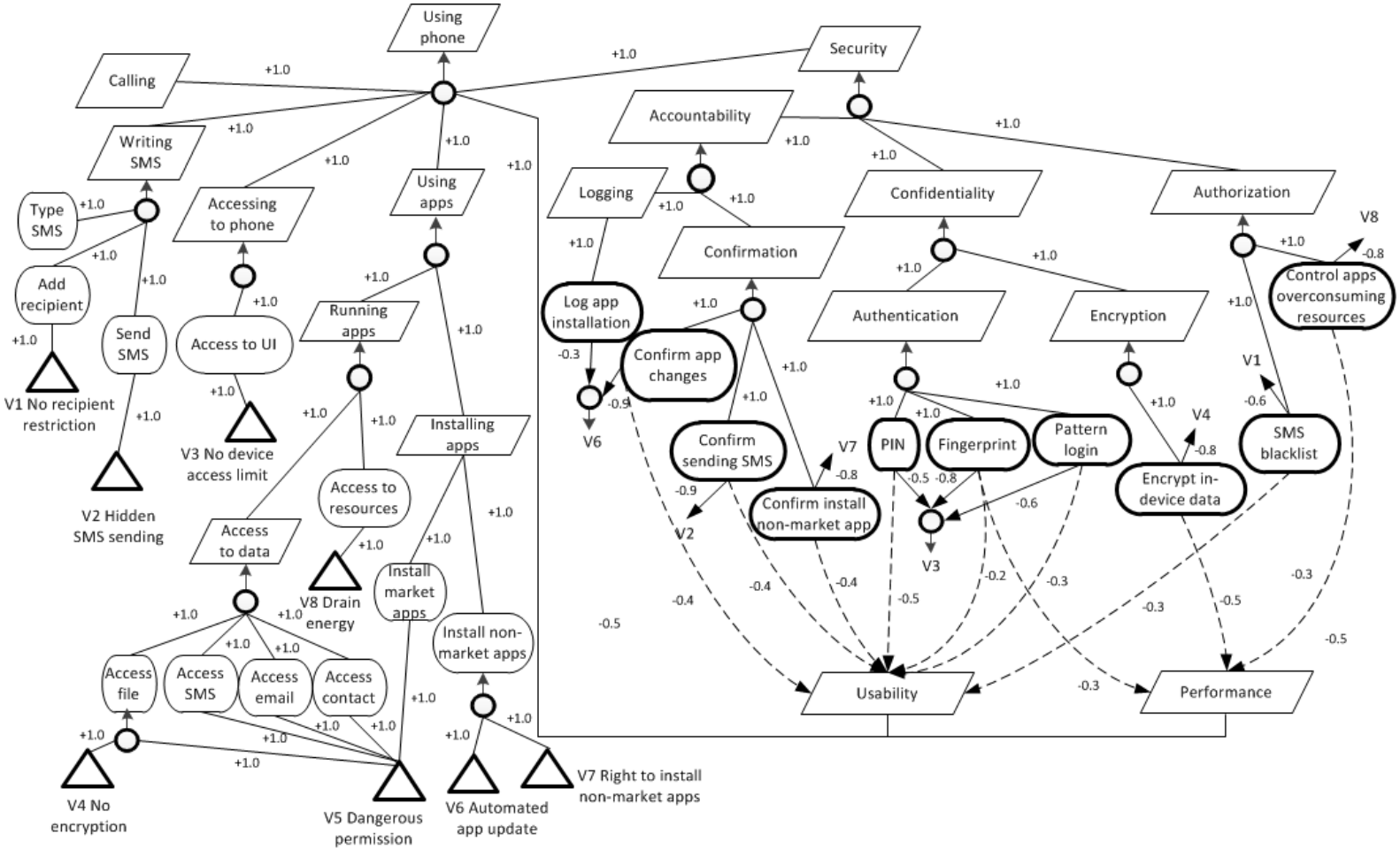


- Requirements at runtime
- Causal reasoning for
  - Analyzing
  - Planning (Decision making)

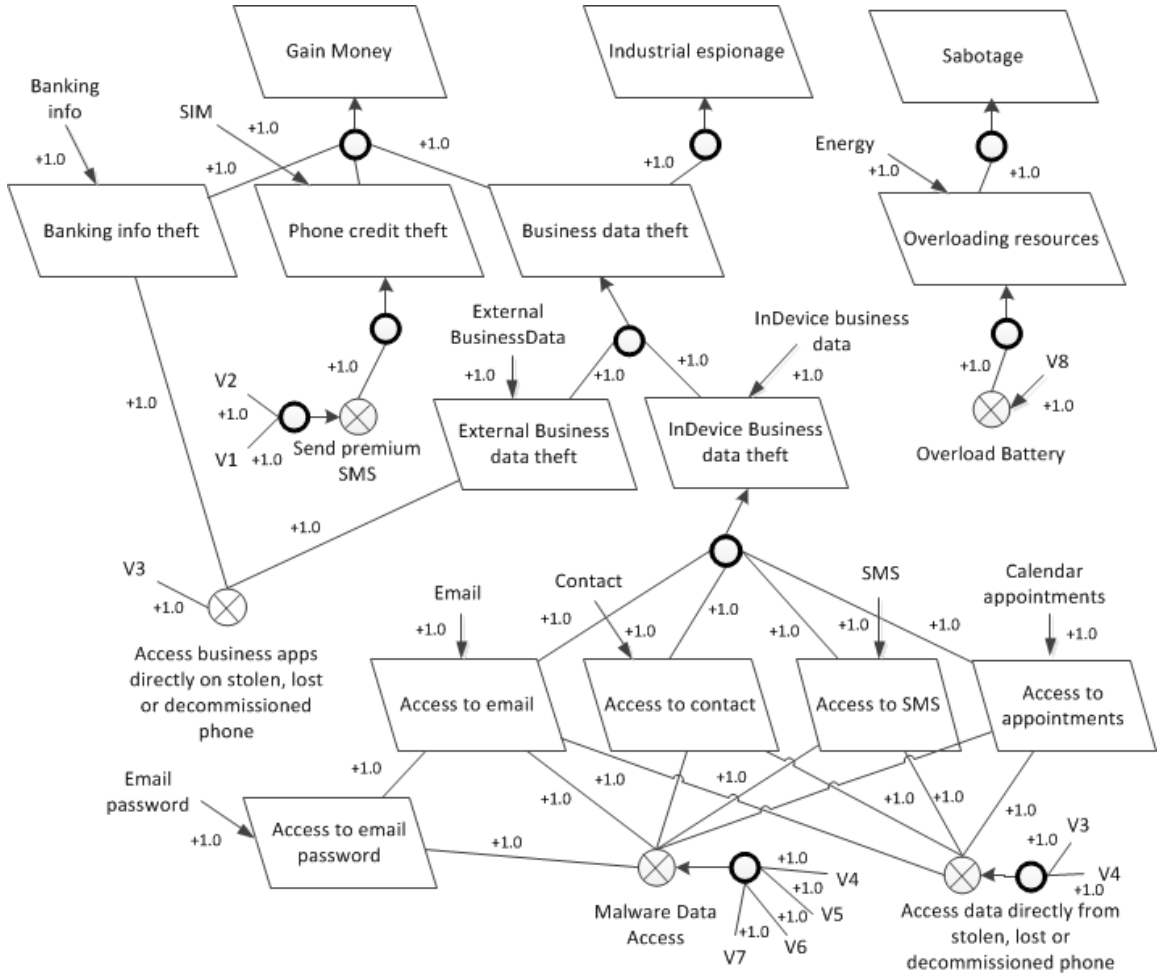
Trio: Asset Model



Trio: Goal Model

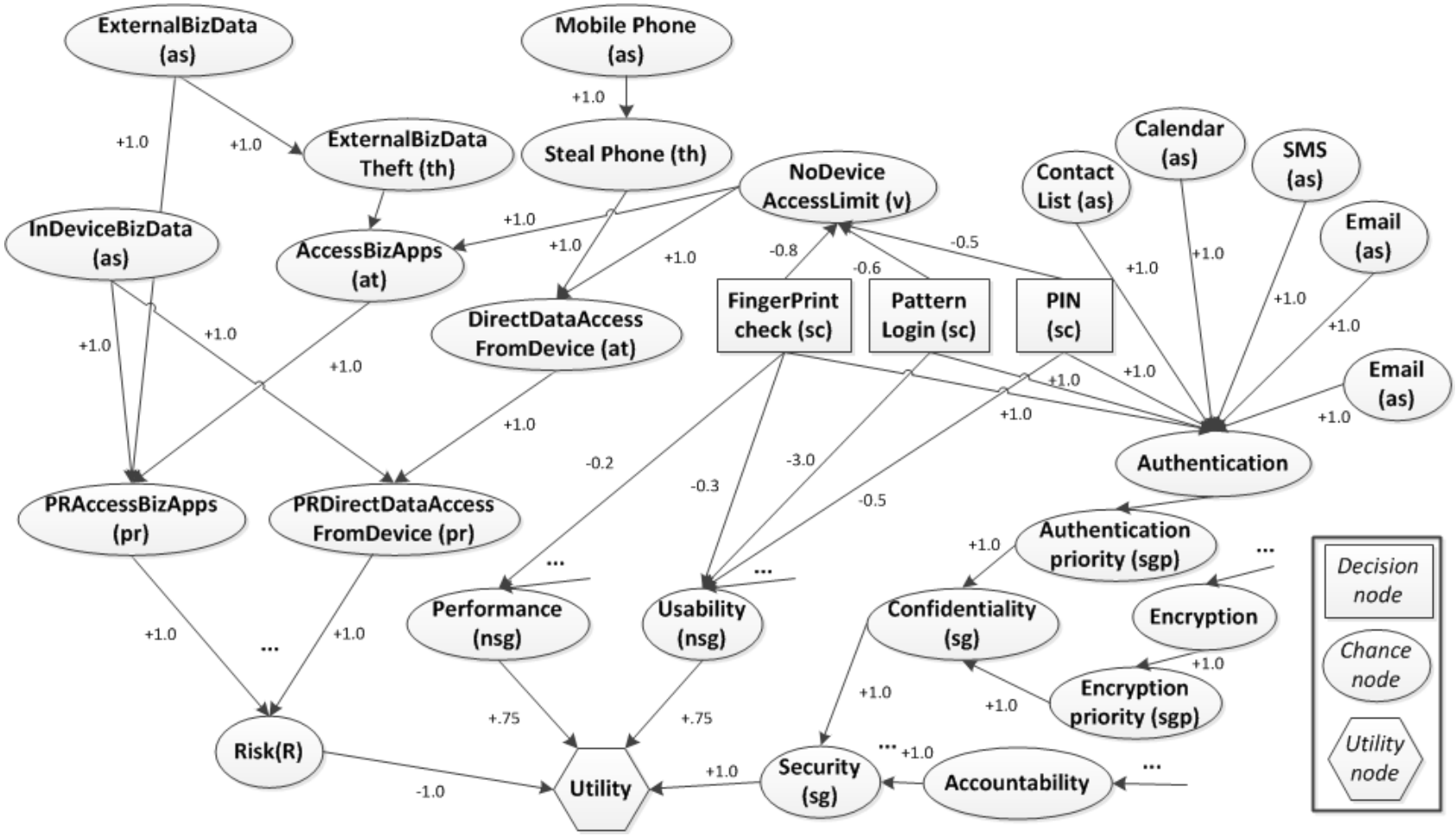


Trio: Threat Model

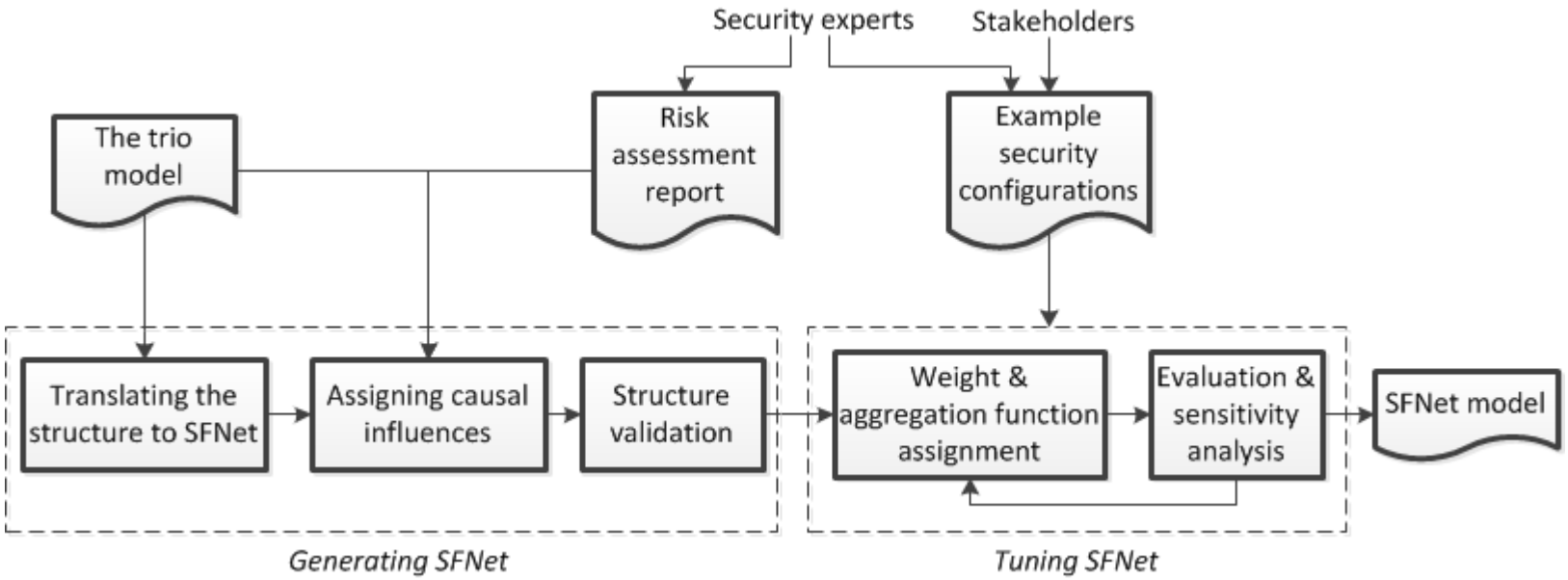


Security Fuzzy Causal Network (SFNet)

SFNet for Mobile Security (partial model)



Building SFNet



- Transforming Trio to SFNet
  - e.g., Asset containment and association to positive causality
- SFNet structure validation
  - e.g., Holding properties for primary assets, security controls and partial risks

Aggregation Functions

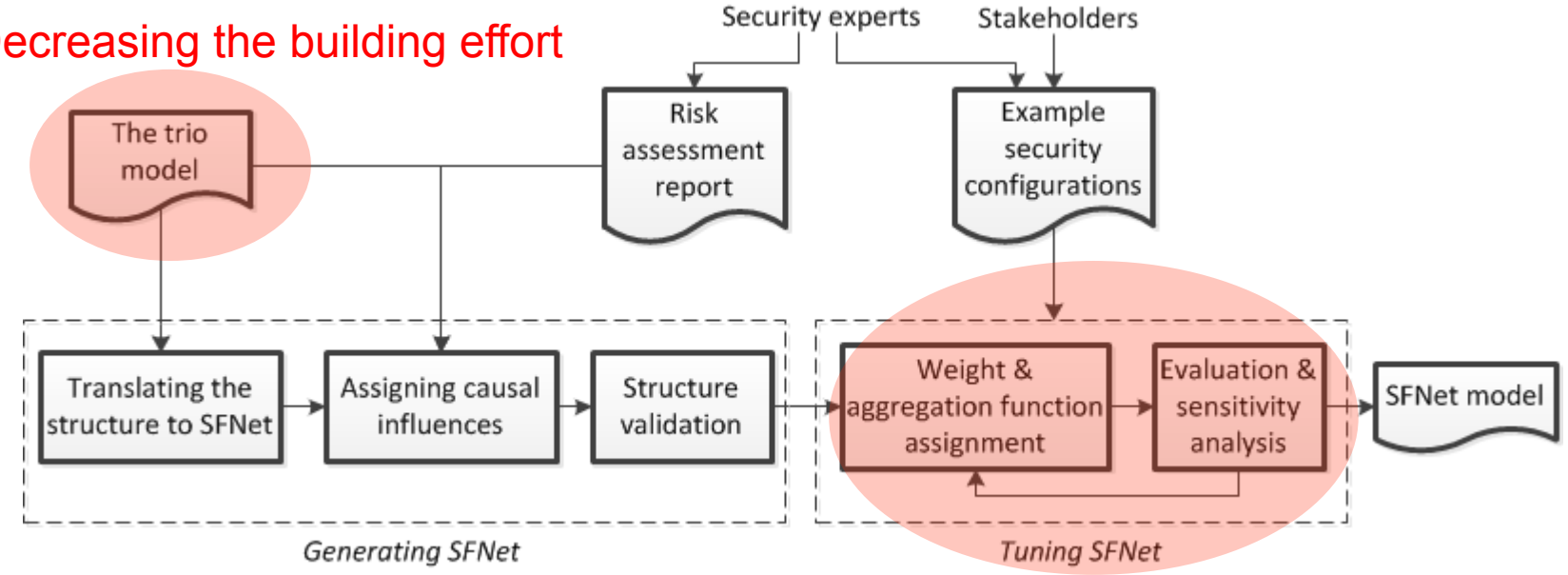
Causal Link	Aggregation
$\{as\} \rightarrow as$	TCoNorm
$\{as\} \rightarrow th$	TCoNorm
$\{th\} \rightarrow at$	TCoNorm
$\{v\} \rightarrow at$	TCoNorm
$\{th\}, \{v\} \rightarrow at$	TNorm
$\{as\} \rightarrow sgp$	TCoNorm
$\{sg\} \rightarrow sgp$	No aggregation (only one goal)
$\{as\}\{sg\} \rightarrow sgp$	TNorm
$\{sc\} \rightarrow sg$	TCoNorm
$\{sg\} \rightarrow sg$	TConorm
$\{sc\} \rightarrow v$	TNorm
$\{sc\} \rightarrow nsg$	Average
$\{as\} \rightarrow pr$	TCoNorm
$at \rightarrow pr$	No aggregation (only one attack)
$\{as\}, at \rightarrow pr$	TNorm
$\{pr\} \rightarrow R$	TCoNorm
$R, \{sg\}, \{nsg\} \rightarrow U$	Average

Aggregation	Function	
TNorm	Minimum	$\top(a,b) = min(a,b)$
	Product	$\top(a,b) = a.b$
	Lukasiewicz	$\top(a,b) = max(0, a+b-1)$
TCoNorm	Maximum	$\bot(a,b) = max(a,b)$
	BoundedSum	$\bot(a,b) = min(a+b,1)$
	ProbabilisticSum	$\bot(a,b) = a+b-a.b$
Average	Average	$Average(a,b) = a+b/2$

Building SFNet

Validity of the trio model

Decreasing the building effort



Selecting aggregation functions

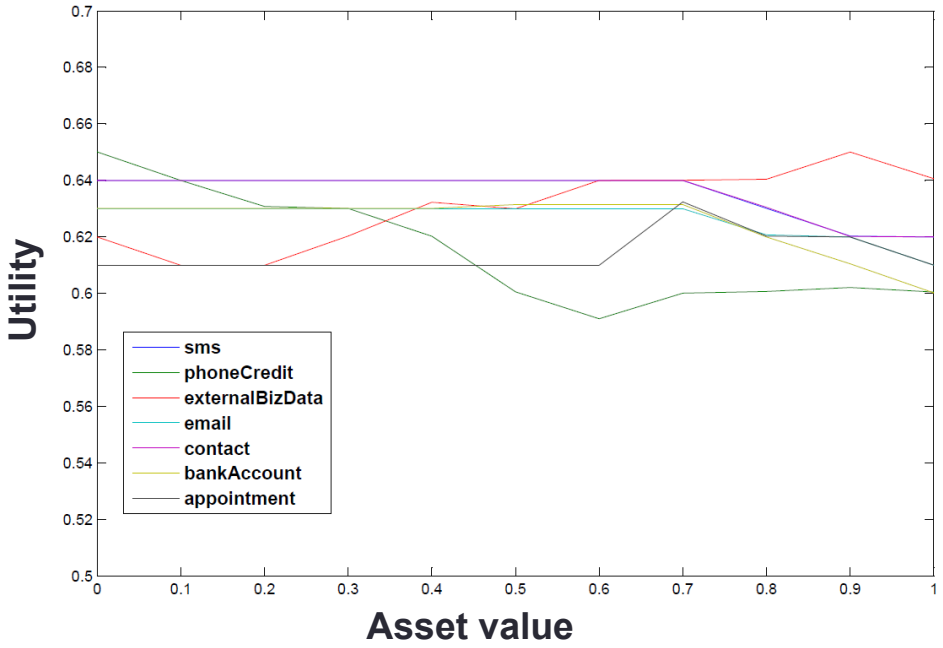
Tuning weights

Fuzzy Causal Reasoning

- Propagate changes in source nodes (e.g., assets) through causal links and aggregation functions

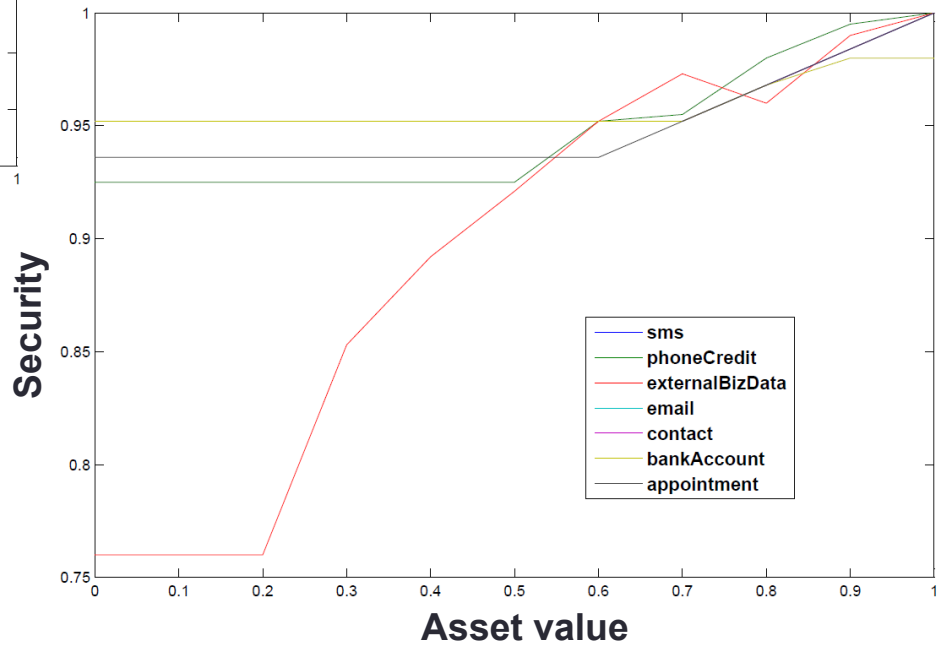
- Search for a security configuration
  - For each specific utility solve a satisfaction problem (Using Z3 SMT solver)
  - Perform a binary search between utility [0,1] with a precision

Mobile Phone Security: Asset variability

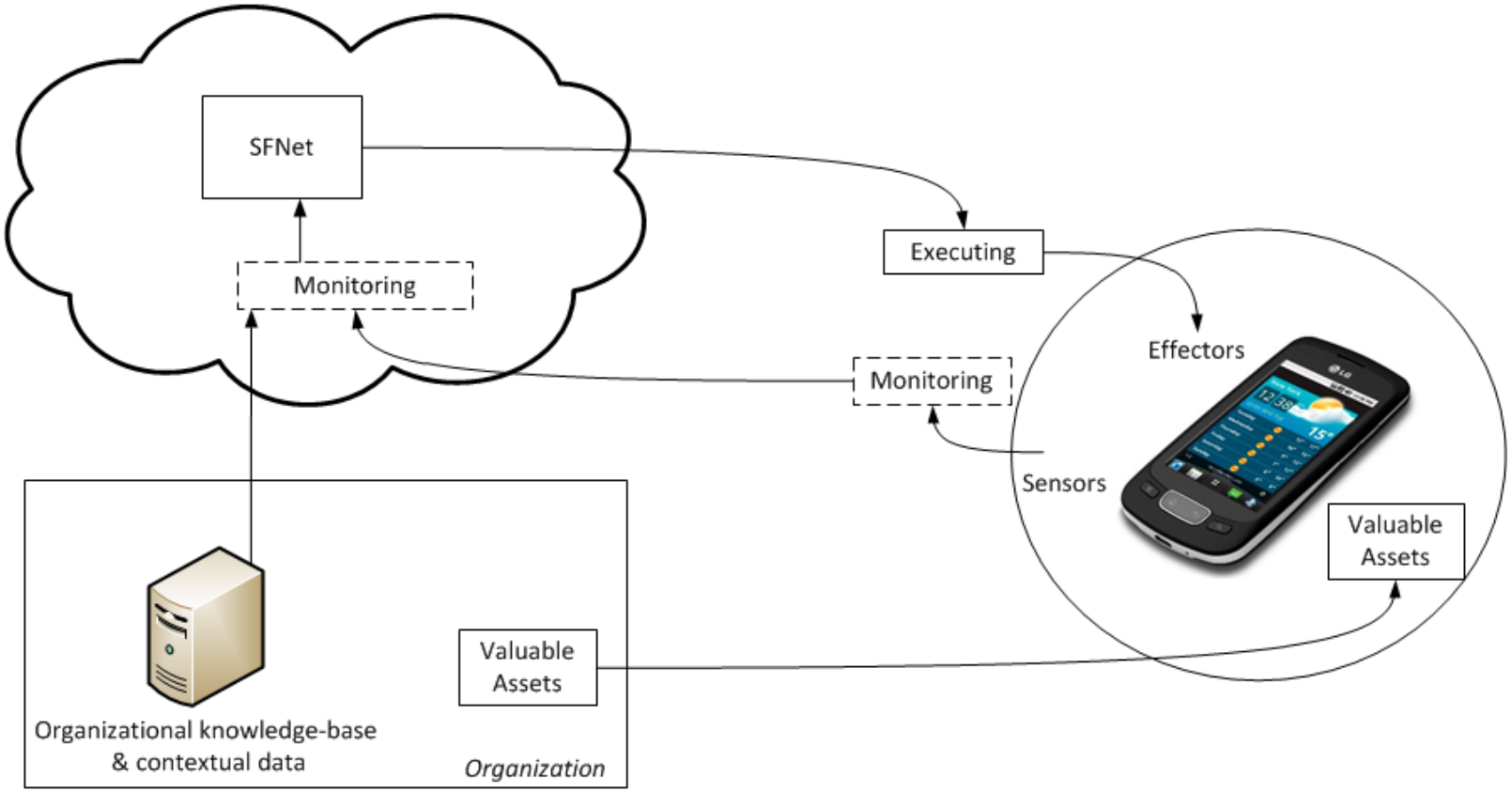


- Utility variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75

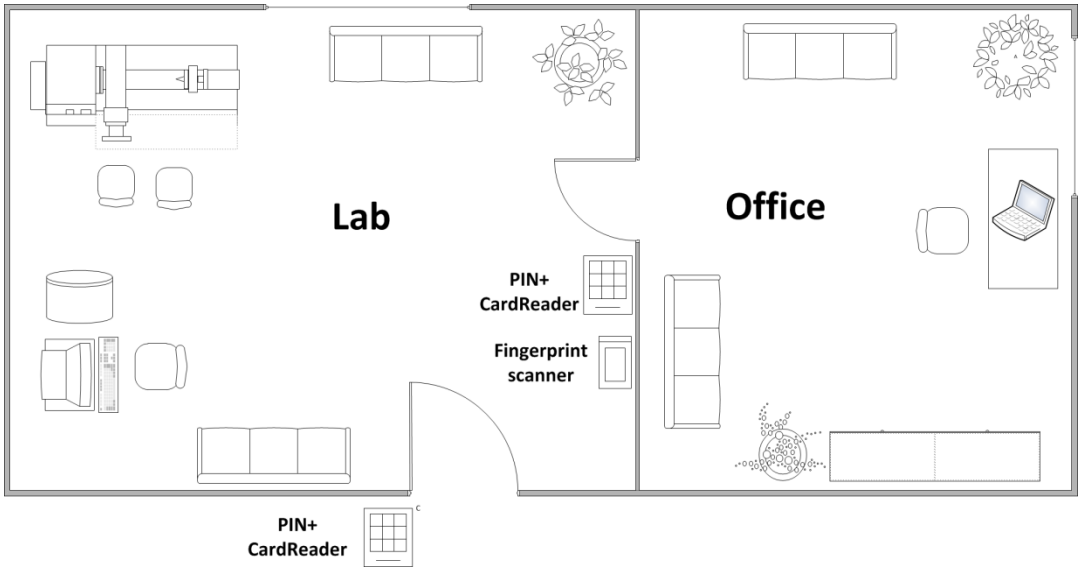
- Security variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75



Deployment Architecture

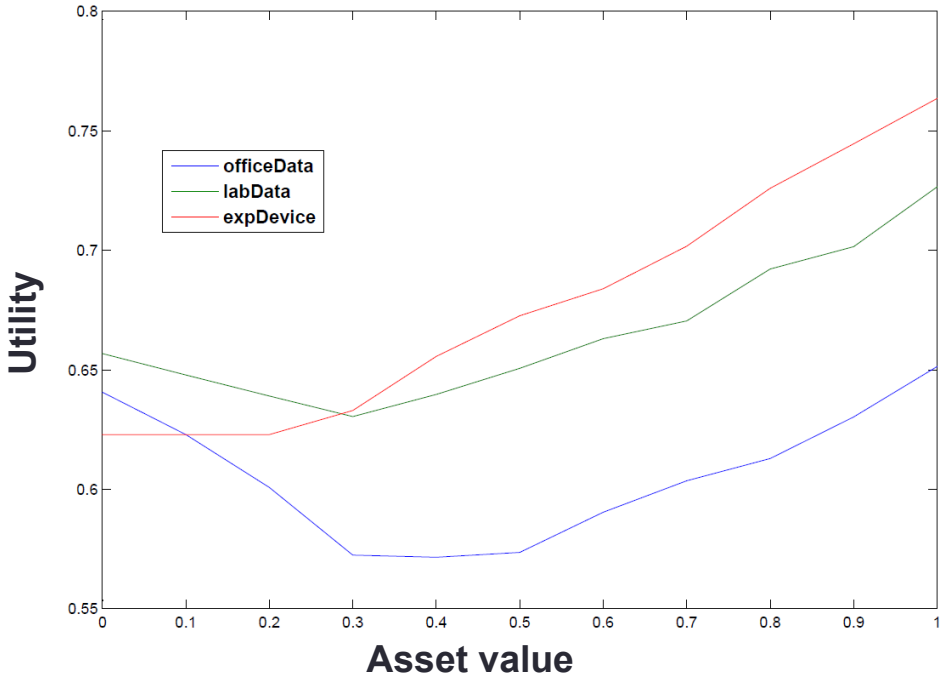


Adaptive Access Control



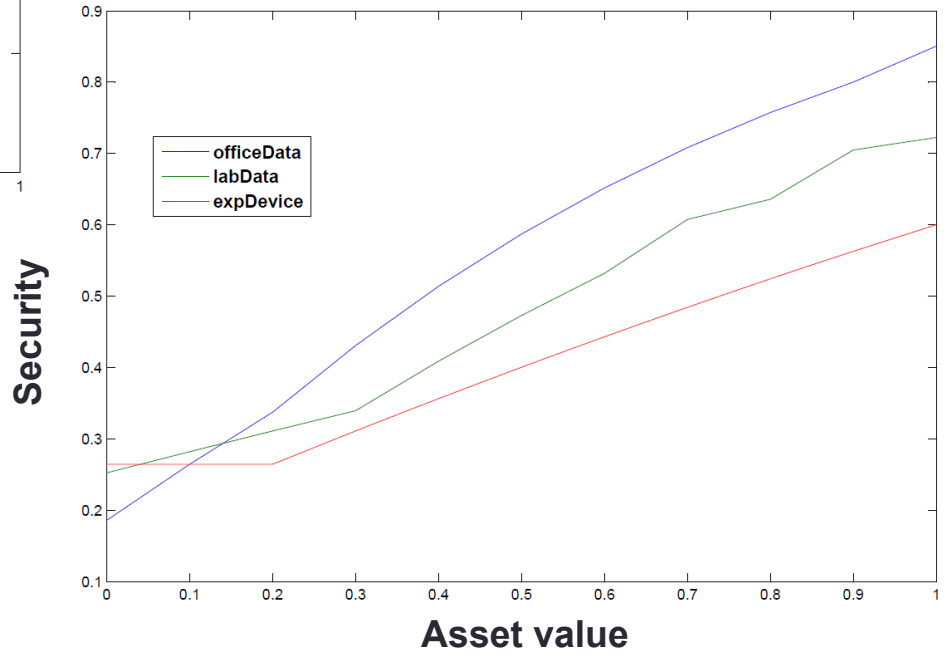
- Asset-based physical access control
- Cyber and physical assets may move in/out areas
- People may move in/out areas
- Authentication, authorization, logging and surveillance mechanisms as security controls
- Adaptive security can be realized as single or two different controllers

Exp: Asset variability in access control



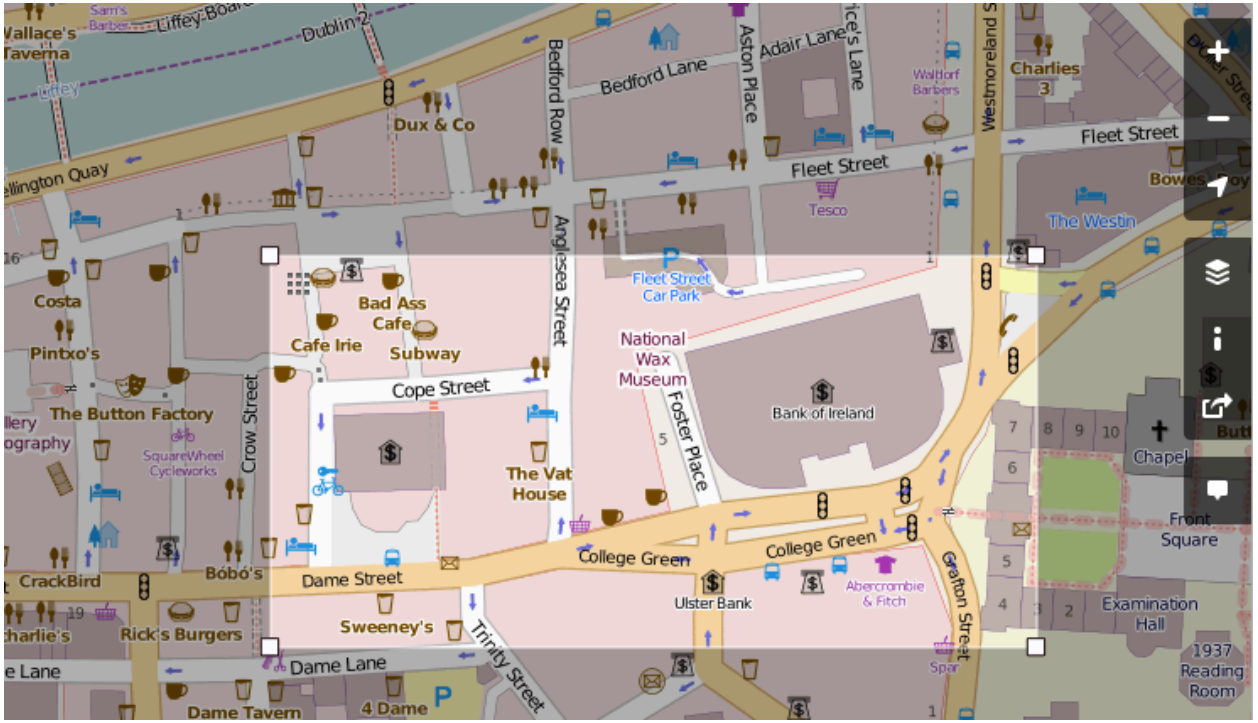
- Utility variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75

- Security variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75



Adaptive Emergency Response Service

- Protecting valuable assets in an area after occurring an incident with possible security impacts
- Dynamically generating SFNet from a template model



Summary & Next Steps

- Focusing on assets to achieve the ultimate goal of security: “Protecting valuable assets”
- Linking assets, goals and threats in the trio model
  - Can be useful for other security analyses as well
- Turning the configuration search to solving several satisfaction problems

- Validating the trio model
- Automated weight & aggregation function tuning
- Generating SFNet from a template
- Alternative search algorithms