Decision-Making in Security Requirements Engineering with Constrained Goal Models

N. Argyropoulos, K. Angelopoulos, H. Mouratidis, A. Fish

School of Computing, Engineering and Mathematics
University of Brighton, Brighton, United Kingdom

University of Brighton

Introduction

- The continuous growth of modern information systems renders their configuration a challenging process.
  - the number of interconnected goals they expected to satisfy;
  - the complexity of their architectures;
  - cyber-threats they must be able to protect against;
  - continuous changes in their operational environment.

Challenges

- The selection of appropriate **security configurations** taking into account:
  - the continuously evolving *threat landscape*
  - the *effects* of threats towards system goals
  - trade-offs between security and other *functional* and *non-functional* system goals

*"Thus, striking a balance between **effective risk management** and **functional system design** can be a challenging endeavour."*

University of Brighton

Research Approach

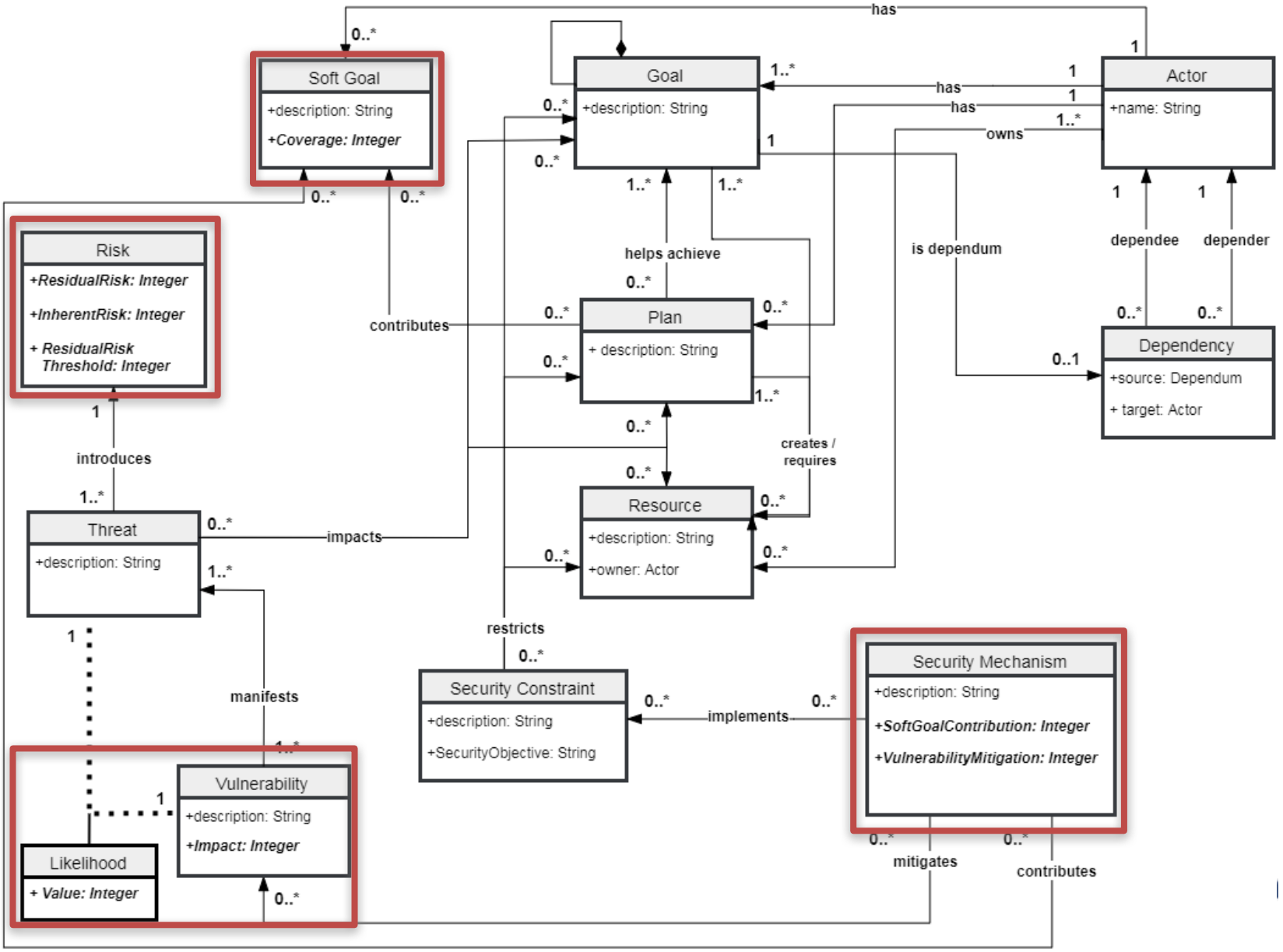
To overcome such challenges this work proposes:

- The extension of **Secure Tropos** in order to support *risk-aware decision-making* for the design of secure system configurations.
- A structured, **quantitative** approach towards the calculation of *risk related aspects* (impact, likelihood, mitigation)
- A framework that selects **optimal security configurations** with respect to the severity of threats and the priorities of other goals using *constraint goal models*.

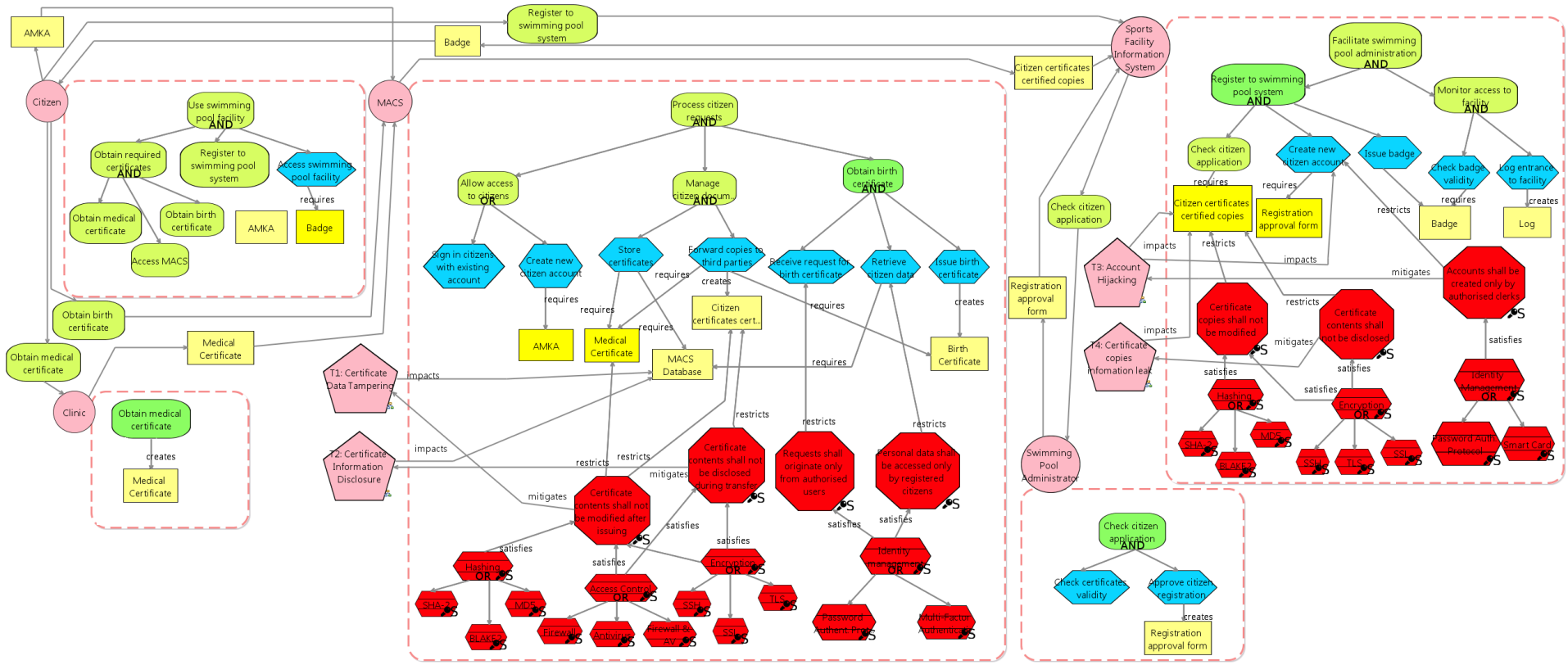
Secure Tropos – Baseline

- A security-oriented extension of Tropos methodology for the elicitation of *security requirements*.
- Standard goal-oriented requirements engineering concepts (e.g., *actors, goals, dependencies*)
- Security related concepts (e.g., *security constraints, threats, security mechanisms*).
- Supports a number of interrelated modelling views
  - *Security Requirements view* captures the goal decomposition of each system actor and the dependencies between them.
  - *Security Attacks view* decomposes each threat to identify its attack methods, the system vulnerabilities they exploit and the coverage provided by the security mechanisms.

Extending Secure Tropos

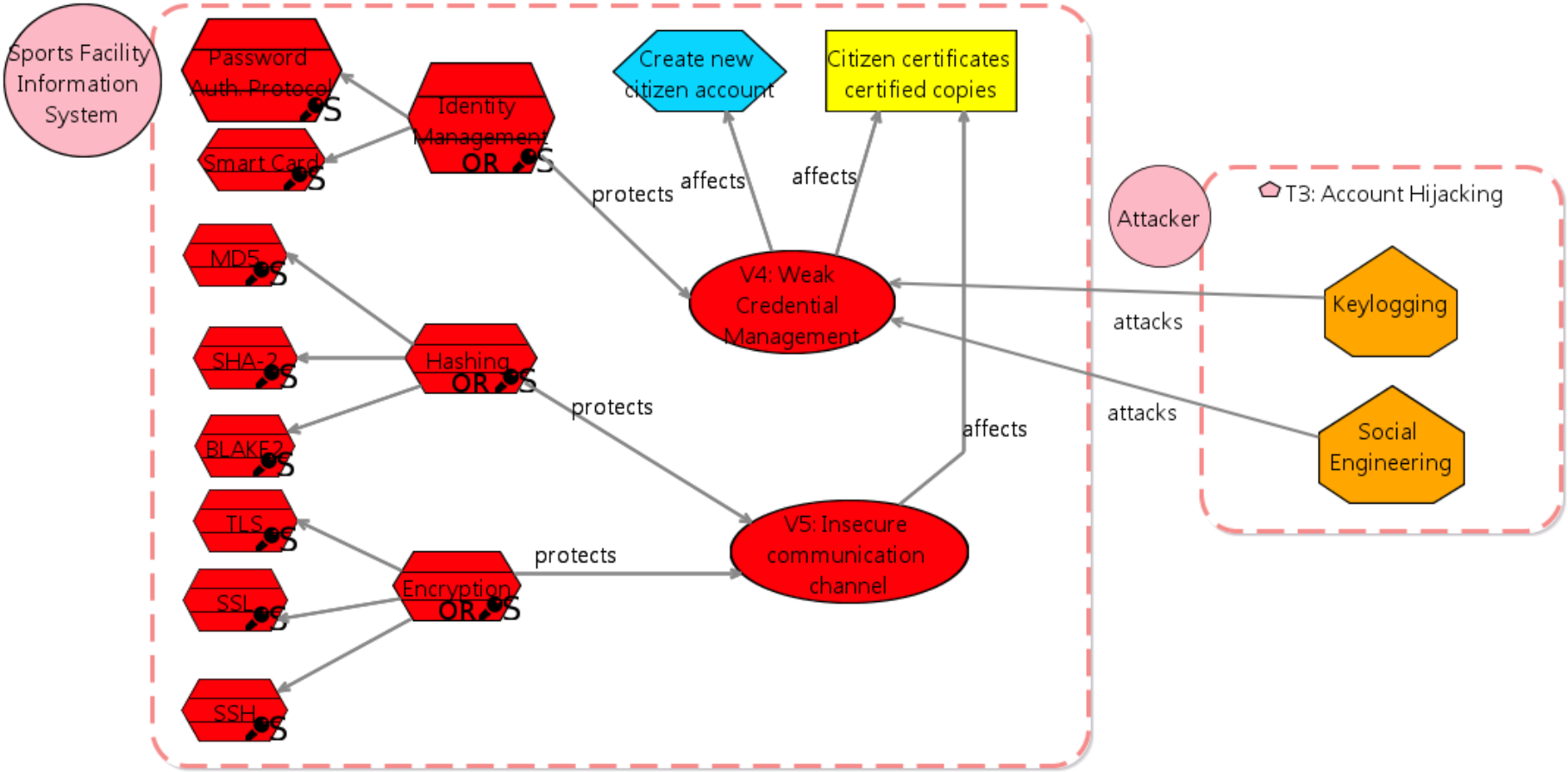


Security Analysis using Secure Tropos



University of Brighton

Security Analysis using Secure Tropos



University of Brighton

Risk Assessment 1/2

- **Step 2: Likelihood Estimation**
  - Assign a *Likelihood* value (L) for each threat that affects each vulnerability, using AHP (0≤ L ≤1).
- **Step 3: Impact Estimation**
  - For each vulnerability, estimate an *Impact* value (I) using AHP (0≤ I ≤1).

Therefore, the Inherent (initial) Risk of each Threat

Definit … od of a
vulnera … act, V,
where V … = 1) or
not (V … entified
vulnera … nt Risk
introdu …

Threat	Vulnerability	Impact	Likelihood	Inherent Risk
T1	V1	0.15	0.4	0.15
	V2	0.15	0.6	
T2	V2	0.15	0.25	0.2625
	V3	0.3	0.75	
T3	V4	0.25	1	0.25
T4	V5	0.15	1	0.15

(1)

University of Brighton

Risk Assessment 2/2

Mechanism Group	Security Mechanism	M_{V1}	M_{V2}	M_{V3}	M_{V4}	M_{V5}	Cost	Perf.
Encryption	SSH	0	0.6	0	0	0.6	30	30
	SSL	0	0.3	0	0	0.3	20	20
	TLS	0	0.8	0	0	0.8	40	20
Access Control	Firewall	0.3	0.6	0.4	0	0	50	60
	AntiVirus	0.5	0.3	0.3	0	0	40	70
	Firewall & Antivirus	0.7	0.8	0.7	0	0	90	80
Hashing	MD5	0.3	0	0	0	0.3	10	20
	SHA2	0.6	0	0	0	0.6	30	20
	BLAKE2	0.8	0	0	0	0.8	40	20
Ident. Management EMACS	Password	0.3	0	0	0	0	50	50
	Multi-Factor	0.7	0	0	0	0	60	80
Ident. Management SP IS	Password	0	0	0	0.3	0	50	50
	Smart Card	0	0	0.6	0	0	60	30

University of Brighton

Risk Minimisation

- **Step 5: Risk Minimisation**
  - *Using Constraint Goal Models and Satisfiability solvers identify the optimal Security Mechanism combinations that minimise the Residual Risk of each Threat and contribute towards the system's soft goals.*

Where, Residual Risk for each Threat is calculated as follows:

Definition 3. *Let R_R be the Residual Risk of a threat, then:*

$$R_R = R_I - R_M \overset{(1),(2)}{=} \sum_{i=1}^{n}[(L_i \times I_i \times V_i) \times (1 - \sum_{j=1}^{m} \frac{M_{ji}}{m})] \quad (3)$$

University of Brighton

Optimisation Scenarios

- Using the OptiMathSAT solver we can create optimisation scenarios where:
  - Each variable has a soft cap (min/max) or a specific hard cap limit (e.g., Residual Risk T1 < 25%)
  - Priorities can be assigned for the optimisation of variables (e.g., Residual Risk T1 > Cost > Residual Risk T2)

Variable \ Scenario	1	2	3	4	5	6
T1 Res. Risk ($R_{R_{(T1)}}$)	min	$min^{[1]}$	$min^{[3]}$	$min^{[2]}$	$< 25\%$	$< 50\%$
T2 Res. Risk ($R_{R_{(T2)}}$)	min	$min^{[2]}$	$min^{[4]}$	$min^{[3]}$	$< 25\%$	$< 50\%$
T3 Res. Risk ($R_{R_{(T3)}}$)	min	$min^{[3]}$	$min^{[5]}$	$min^{[4]}$	min	$< 75\%$
T4 Res. Risk ($R_{R_{(T4)}}$)	min	$min^{[4]}$	$min^{[6]}$	$min^{[5]}$	min	$< 50\%$
Added Cost Coverage	min	$min^{[5]}$	$min^{[1]}$	$min^{[6]}$	$min^{[1]}$	$min^{[1]}$
Performance Overhead Coverage	min	$min^{[6]}$	$min^{[2]}$	$min^{[1]}$	$min^{[2]}$	$min^{[2]}$

Optimisation Results

- Each scenario results in different set of selected Security Mechanisms, that satisfies its initial parameters

Scenario / Mechanism	1	2	3	4	5	6
Encryption	SSL	TLS	SSL	TLS	TLS	TLS
Access Control	Firewall	Firewall & AntiVirus	AntiVirus	Firewall	Firewall & AntiVirus	Firewall
Hashing	MD5	BLAKE2	MD5	BLAKE2	BLAKE2	MD5
Ident. Mgmt EMACS	Password	Multi-Factor Authent.	Password	Password	Multi-Factor Authent.	Password
Ident. Mgmt SP IS	Password	SmartCard	Password	SmartCard	Password	SmartCard

University of Brighton

Conclusions – Future Work

- Contributions of proposed framework
  - Extending Secure Tropos with Risk related concepts,
  - Support for quantitative risk assessment and trade-off analysis between security and other requirements.
  - Identification of optimal security configurations for a number of different scenarios
- Future Work
  - Exploring more advanced reasoners to support more complex optimisation scenarios
  - Support a more structured approach for Likelihood and Impact value estimation

University of Brighton

Thank you!

Contact the authors:
n.argyropoulos@brighton.ac.uk
k.angelopoulos@brighton.ac.uk

Visit us:
www.sense-brighton.eu

Secure and Dependable SenSe Research Cluster Software Systems

University of Brighton