



Modelling Security: the Secure Tropos project

Dr. Haris Mouratidis

13/09/2012

Presentation Agenda

- Security Modelling
 - Why Security is important?
 - Some challenges
- Secure Tropos Project
 - Modelling Language
 - Process
 - Algorithms
- The way forward.....
 - Trust, Privacy



What is Security?

- Economical Security
 - condition of having the resources to support a standard of living now and in the foreseeable future
- Physical Security
 - Physical security describes measures that prevent or deter attackers from accessing something (building, car, etc)
- Information Systems Security
 - Information security means protecting information and information systems from unauthorized access, use, disclosure, and disruption.

Security of Information Systems

- Information Systems are everywhere!
- Storage of personal and sensitive information
- Need to Keep such systems secure



Information Security Goals

- Security is concerned with the protection of assets from (intentional) harm.
 - Confidentiality
 - information is only accessible to authorised entities
 - Integrity
 - information remains unmodified from source to destination
 - Availability
 - Accessibility and usability of information and recourse to authorised entities
 - *Authentication....non repudiation....authorisation*

Modelling Security

Modelling security

- Security is a difficult concept to model
 - Extend to more than one domains
 - Depend on specific scope and context
 - Introduces multiple views
 - Introduces conflicts
- We need a method that allow us to overcome those challenges

Security Modelling Challenges I

- A socio-technical problem
- A problem of scope and context
 - (i.e. one solution does not fit all)



Security Modelling Challenges II

- A problem of multiple views
 - Usability
 - Effectiveness
- A problem of conflicts
 - security vs functional requirements



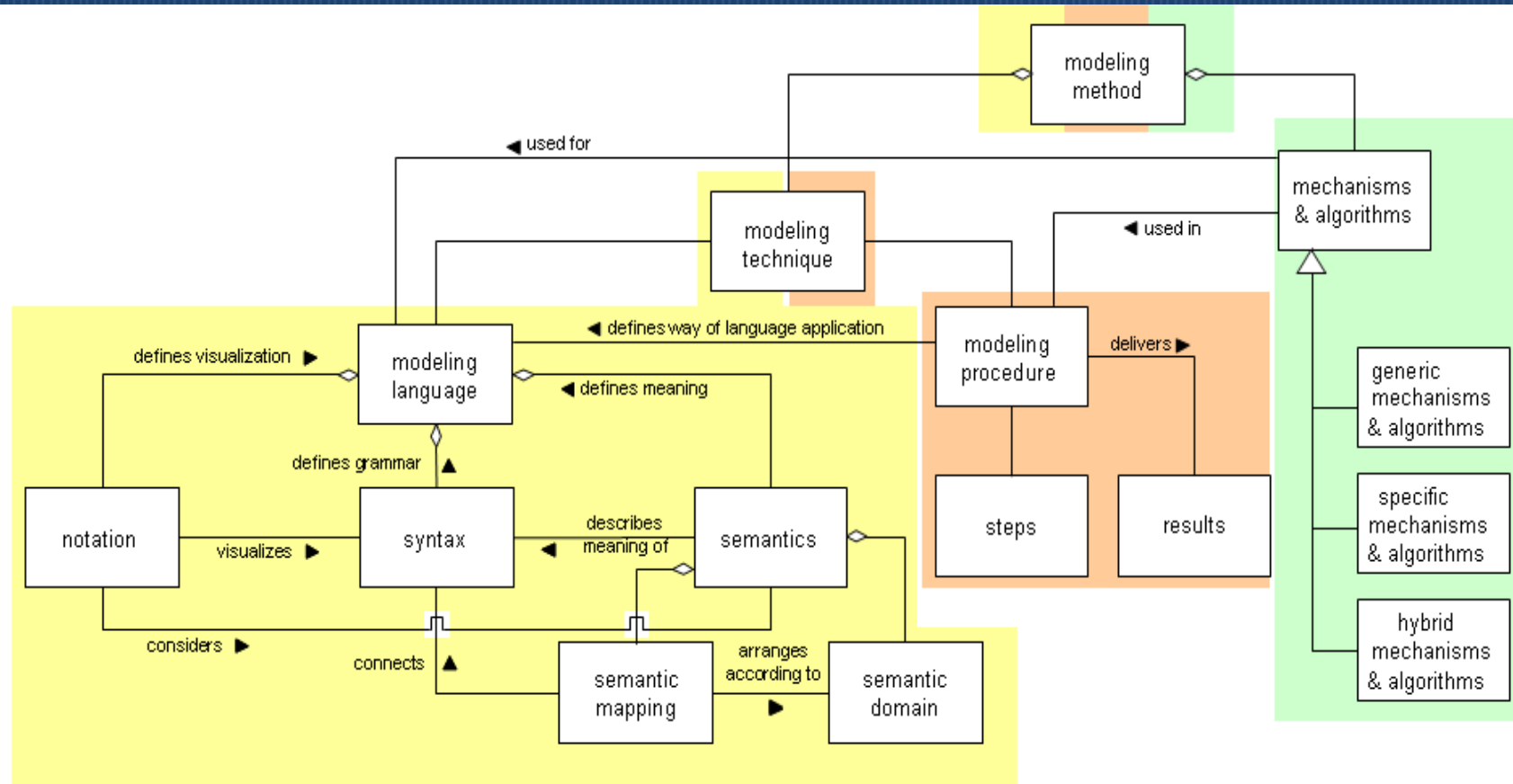
Secure Tropos Method

- Supports security modelling not just at system level but also at the system environment level
 - Security is affected by the system environment
 - Technical and social requirements
- Supports the identification of security requirements focused on the developed system
 - The process does not start from “we need to add authorisation mechanisms etc”

Secure Tropos method II

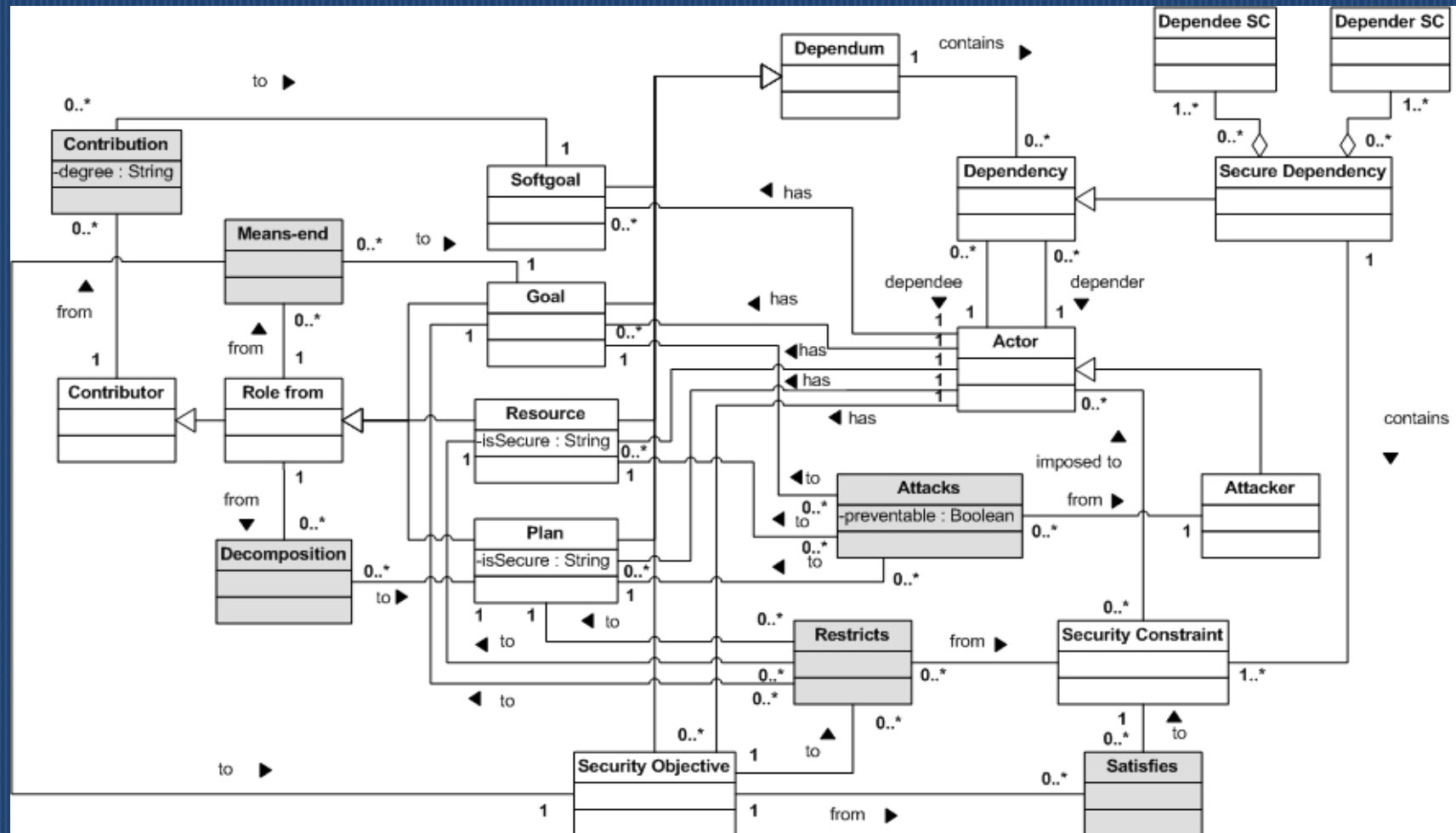
- Supports multiple views of security
 - Organisational
 - System
 - requirements
 - attacks
- Supports simultaneous modelling and analysis of security and functional requirements (at system level)
 - Assist in limiting conflicts

Modelling Method



Vortrag Karagiannis (2006) [vgl. auch Kühn (2004)]

Modelling Language



Security Requirements

- Various definitions
 - Security community
 - Requirements community
- A useful definition
 - *Constraints on system functions that support the achievement of security goals*
 - *The system **shall not** provide Patient Information **except to** members of the patient's medical team*

Secure Tropos Procedure

- Iterative
 - ▣ The identification of security requirements of the system;
 - ▣ The development of a design that satisfies the security requirements of the system;
 - ▣ The testing of the system under development.

- The process has recognizable steps

- The procedure has recognizable artefacts (results)
 - ▣ Models/diagrams

Process Steps / Results

- Organizational Analysis.
 - The organisations are modelled as actors and the developer identifies actors' goals, plans and resources. This stage can be skipped if the developer wants to focus just on the system.
 - Output model: Organizational Model.
- System Analysis.
 - The system is modelled as an actor. There is analysis of system's goals, plans, resources and secure entities.
 - Output model: System Model.

Process Steps/Results

- System Components Design.
 - This stage includes the development of an architecture that fulfils the security requirements. System components are identified.
 - Output model: Architectural Model, Components Model.
- Security Attacks Analysis.
 - This stage includes the introduction of potential security attacks to the system and an analysis of how existing system countermeasures can support system defences.
 - Output model: Security Attacks Model.

Algorithms

- Architecture
- Attacks
- Security Balance
 - Provide an analysis that identifies the impact each component has on the security of the system.
 - define how critical each security constraint is for the overall security of the system.
 - **Security Criticality** *is the measure of how the security of the system will be affected if the security constraint is not achieved.*

Security Balance Analysis

- To be able to evaluate how much effort is required by each of the components to achieve their security constraints.
- **Security Complexity** *is the measure of the effort required by the responsible component for achieving a security constraint.*

Security Balance Analysis

- the Rebalance algorithm
 - given a representation of a system and its constraints,
 - produce a new configuration (if it exists), in which the constraints are satisfied.
- For sake of simplicity the algorithm considers only the complexity and not the criticality, but it is easy to extend it to consider both complexity and criticality.

Trust, Privacy

How we model trust?

- Trust is the positive expectation of one actor, the trustor, about the behaviour of another actor, the trustee, by whom he might be positively or negatively affected.
 - Trust is a characteristic of the trustor, while trustworthiness is a characteristic on the trustee.
 - Trust is based on the perception of the trustor about the trustworthiness of the trustee (how many trustworthy characteristics he has according to the trustor).

Modelling Privacy

- Usually as separate or a subset of security;
- Need to be modelled in its own right but in a unified framework with security
 - Multi-facet concept
 - Social, legal issue (human right)
 - Solutions to guarantee privacy is very different than security
 - Separate to support informed decisions

Is security an Issue just for IS?

- Information Systems is just an application area for security modelling
 - Business Process Modelling
 - Production Lines
 - Supply Chain
 - Critical Infrastructures
 - Building and Civil Engineering

Danke! Any Questions?



For more information



Haris@uel.ac.uk



<http://www.openmodels.at/web/secure-tropos/home>