Detecting Conflicts of Interest

Paolo Giorgini, Fabio Massacci, John Mylopoulos, Nicola Zannone

Department of Information and Communication Technology
University of Trento

Conflicts of Interest

- Analyzing organizational requirements is fundamental to build secure systems
- Security is often compromised by exploiting vulnerabilities in the socio-technical system
- Conflicts of interest are critical in the development of secure systems since "trusted" actors often abuse their position to gain personal advantages
  - e.g., an employee working in Front Office and in Back Office
  - e.g., in the early nineties John Rusnak gained nearly $500.000 in bonuses for fake bank profits by exploiting his trader position at Allied Irish Bank

Some Proposals

- Proposed a number of classifications and solutions to mitigate conflicts
  - ✓ divergences between goals [van Lamsweerde et al.]
  - ✓ overlap of the subjects of authorization policies [Moffett et al.]
  - ✓ privilege-privilege conflicts and role-role conflicts in role-based access control [Nyanchama et al.]
- Unfortunately, current solutions are unsatisfactory
  - ✓ No analysis of the organizational setting
  - ✓ Proposed taxonomies of conflicts are based on mechanisms for preventing them, instead of understanding why and when they occur
  - ✓ Solutions hardly make any reference to the legal theory on which they are based

A Law Definition

A conflict of interest is “a situation in which a person has a duty to more than one person or organization, but cannot do justice to the actual or potentially adverse interests of both parties. This includes when an individual's personal interests or concerns are inconsistent with the best for a customer, or when a public official's personal interests are contrary to his/her loyalty to public business.”

http://dictionary.law.com

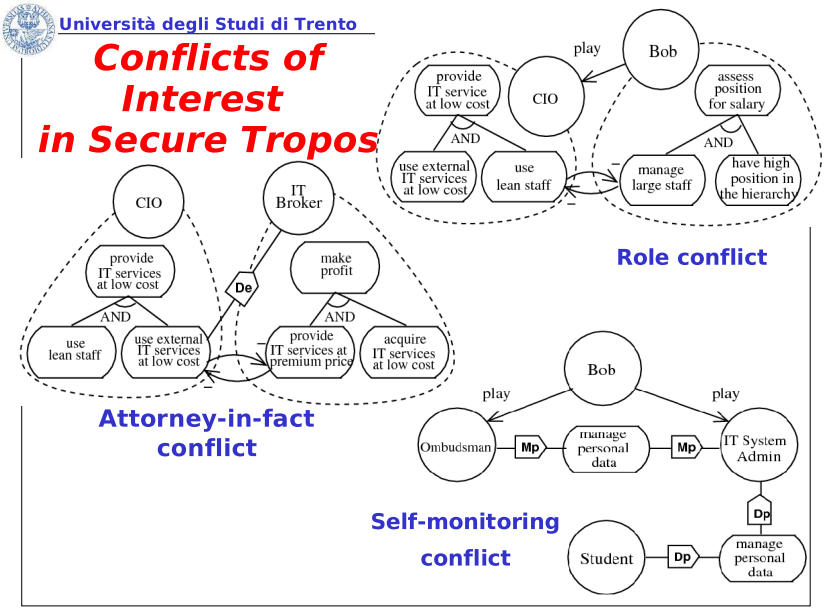
Conflict (of Interest) Classification

- Attorney-in-fact conflict
  - the interests of the delegatee interfere with the interests of the delegator
- Role conflict
  - an agent is assigned a role whose interests collide with those of the agent
- Self-monitoring conflict
  - an actor is responsible for monitoring his own behaviour

Secure Tropos

- Requirements Engineering methodology tailored to model both the organizational environment of a system and the system itself
- Support modeling and analysis of functional and security requirements
- Founded on the notions of ownership, provisioning, trust, and delegation
  - define entitlements, capabilities and responsibilities of stakeholders and system's actors and their transfer.
- Automated Reasoning Support for Security Requirements Analysis

Conflicts of Interest in Secure Tropos



Verification Process

- **Design the requirements model**
  - ✓ identify stakeholders along with their objectives, entitlements and capabilities
  - ✓ identify social relations among stakeholders
  - ✓ identify conflicting interests
- **Computer Aided Requirements Engineering**
  - ✓ Diagrams (automatically) mapped into a Formal Model
  - ✓ Check the properties on the Formal Model
    - ✓ ⟵ *delegateChain(exec,A,B,S1) ∧ neg_contribution(S1,S2) ∧ aims(B,S2)*

Conclusion

- Identify conflicts of interest during the early phases of the software system development process.
  - ✓ Investigate the sources of conflicts of interest at requirements (as opposed to policy) level grounding our notions on legal theory
  - ✓ Define a clear-cut formalization that allows for automatic detection of conflicts
- Future Work
  - ✓ Define solutions for mitigating conflicts of interest
    - ✓ Reconstructing the organizational structure
    - ✓ Automatically extracting separation of duty constraints from the requirements model
- This work is partially supported by MOSTRO, SERENITY, STAMPS and SENSORIA projects