Managing Security Alignment of Socio Technical Systems

Advisor:
Prof. Paolo Giorgini

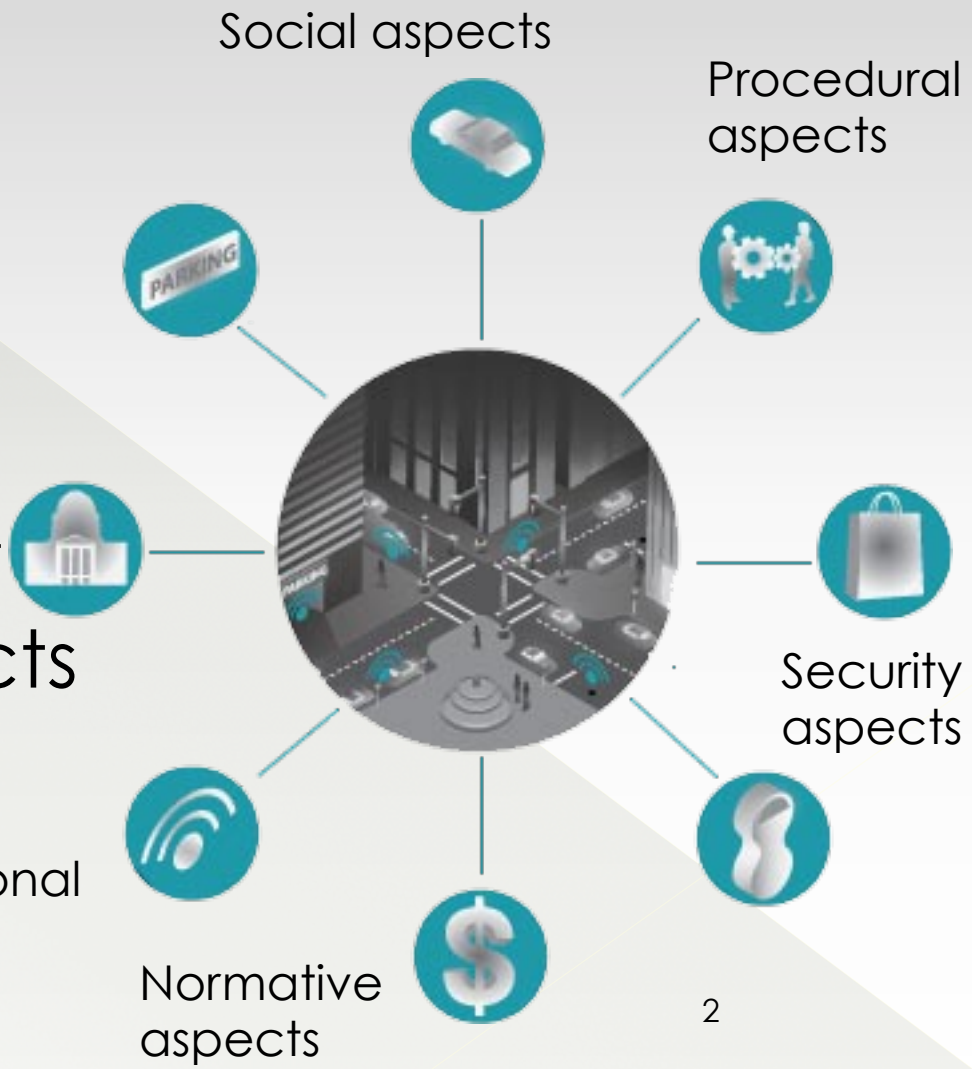
PhD candidate:
Mattia Salnitri

UNIVERSITY
OF TRENTO - Italy

Information Engineering
and Computer Science Department

Socio-Technical Systems (STSs)

- Systems composed of
  - Social Actors
  - Technical components
- Examples
  - Smart cities
  - Health care systems
  - Smart houses
  - Air Traffic management
- Heterogeneous aspects



Security in STS

Example:
protect municipality sensitive data

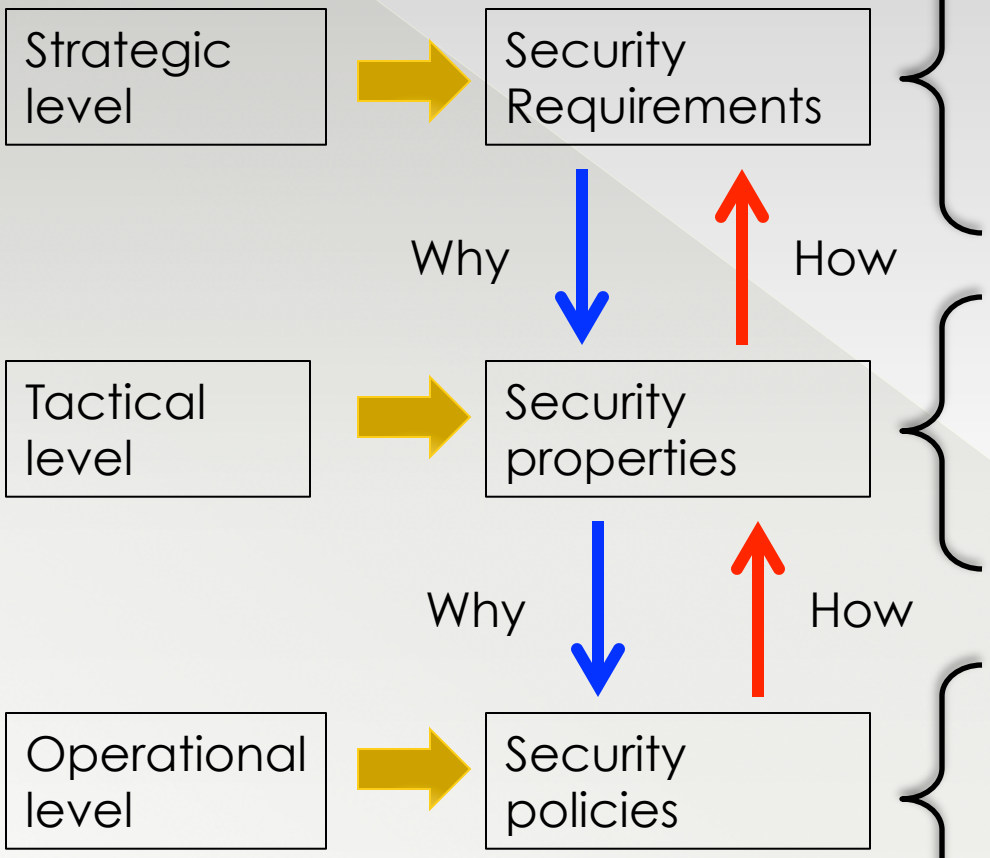
- **communication**
  - PGP cryptographic algorithm
  - The mayor may print the sensitive data and forget them in a public space
- **procedure**
  - Municipality send data –> Mayor use data –> mayor delete data
  - Relatives of the mayor can access and manage data
- **social organization**
  - The wife can receive data but not the son

Security is not only a technical problem

Modeling STSs

Strategic Level	**Social aspects**: social interactions, legal impact, organizational structure.	UML Use case [20] Tropos [19] *i**[18] KAOS[21]
Tactical level	**Procedural aspects**: Business processes, flow of actions, flow of messages, protocols.	BPMN[15] YAWL [12] EPC[25]
Operational level	**Technological aspects**: methods calls, quality of service, cryptographic algorithm parameters.	UML Class diagram [20] UML Component diag. [20] WSAg [16] WSLA[17]

Modeling security in STSs



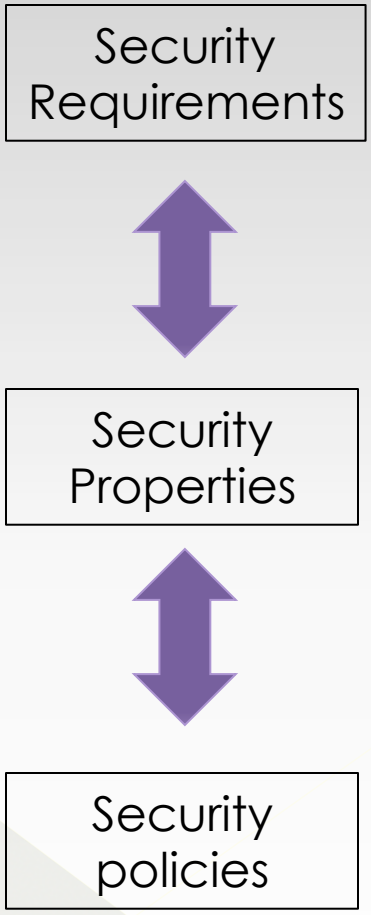
- Stakeholder needs about security
- E.g. the need of avoiding unauthorized disclosure of sensitive data

- Restrictions on modalities of procedures execution
- E.g. use a cryptography protocol for sensitive data communications

- Patterns on system specification
- E.g. how to pre-process parameters of a cryptography algorithm

STSs dynamism

- STSs adapt to external changes
  - Eg: a new law imposes that all communication cannot be encrypted
- Misalignment of security aspects
  - Eg: **security properties** of the traffic management system are adapted, but there still is a **security requirements** that sensitive data have to be protected



Misaligned security aspects may lead to severe consequences

PhD Objective

Define a run time and design time semi-automated framework which:

Objective 1:

checks alignment of STS security aspects

- Check if security aspects are coherent

Objective 2:

reestablishes alignment STS security aspects

- If security aspects are misaligned, it proposes STS adaptation so to reestablish alignment.

Objective 3:

It is **supported by a software**

Objective 4:

It is **validated** with industrial case studies

State Of The Art

Requirement Engineering
+check alignment (Bauer et al. [1], Ghanavati et al. [6])
+link different modeling languages(Massacci et al. [23])
-security alignment not covered in all abstraction levels
OBJ1 OBJ2

Co-evolution
+check alignment (D'Hondt et al. [2], Etien and Salinesi [3])
+reestablish alignment (Potter and De Jong [24])
-security alignment not cover all abstraction levels
OBJ1 OBJ2

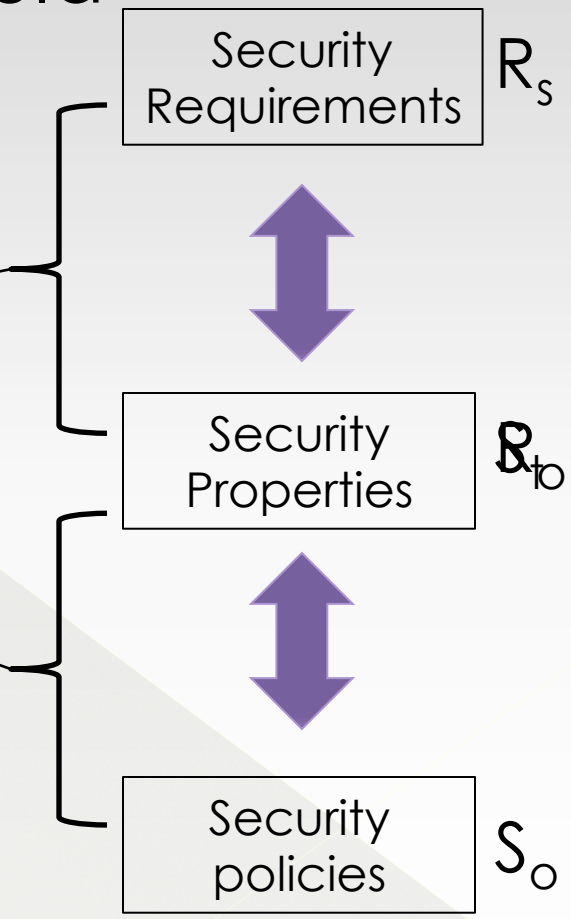
Model Transformation
+link concepts of different modeling languages (Evans and Kent [4])
+transform models to models in different abstraction levels (Anastasakis et al.[27], Rodriguez et al. [28])
+generated models are aligned with security aspects of original models (Fox and Jurjens [5])
OBJ1 OBJ2

Formal approaches
+check alignment(Liu et al. [8], Rushby [9])
-not usable at runtime
-considerable amount of effort by specialists
OBJ1 OBJ2

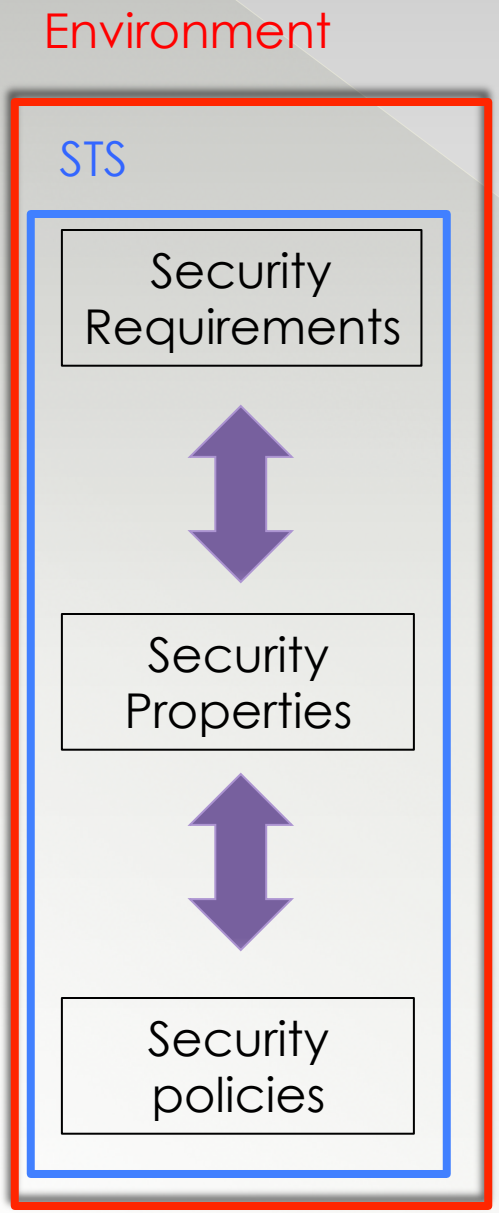
We need an approach that
-covers all abstraction levels
-usable ad design-time and run-time

Problem formalization

- Zave and Jackson [10] formula
  - $S, K \vdash R$
- Extension
  - Changed definition of **S**
  - $S_t, R_o \cup K' \vdash R_s$ }
  - $S_o, K'' \vdash R_o$ }



Problem formalization



$S_t, R_o \cup K' \vdash R_s$

$S_o, K'' \vdash R_o$

R_s: Customer needs to avoid disclosure of data about his financial investments

S_t: Secure Cash-in-Transit (CiT) transfer from A to B;
No communications of financial data to unauthorized users;

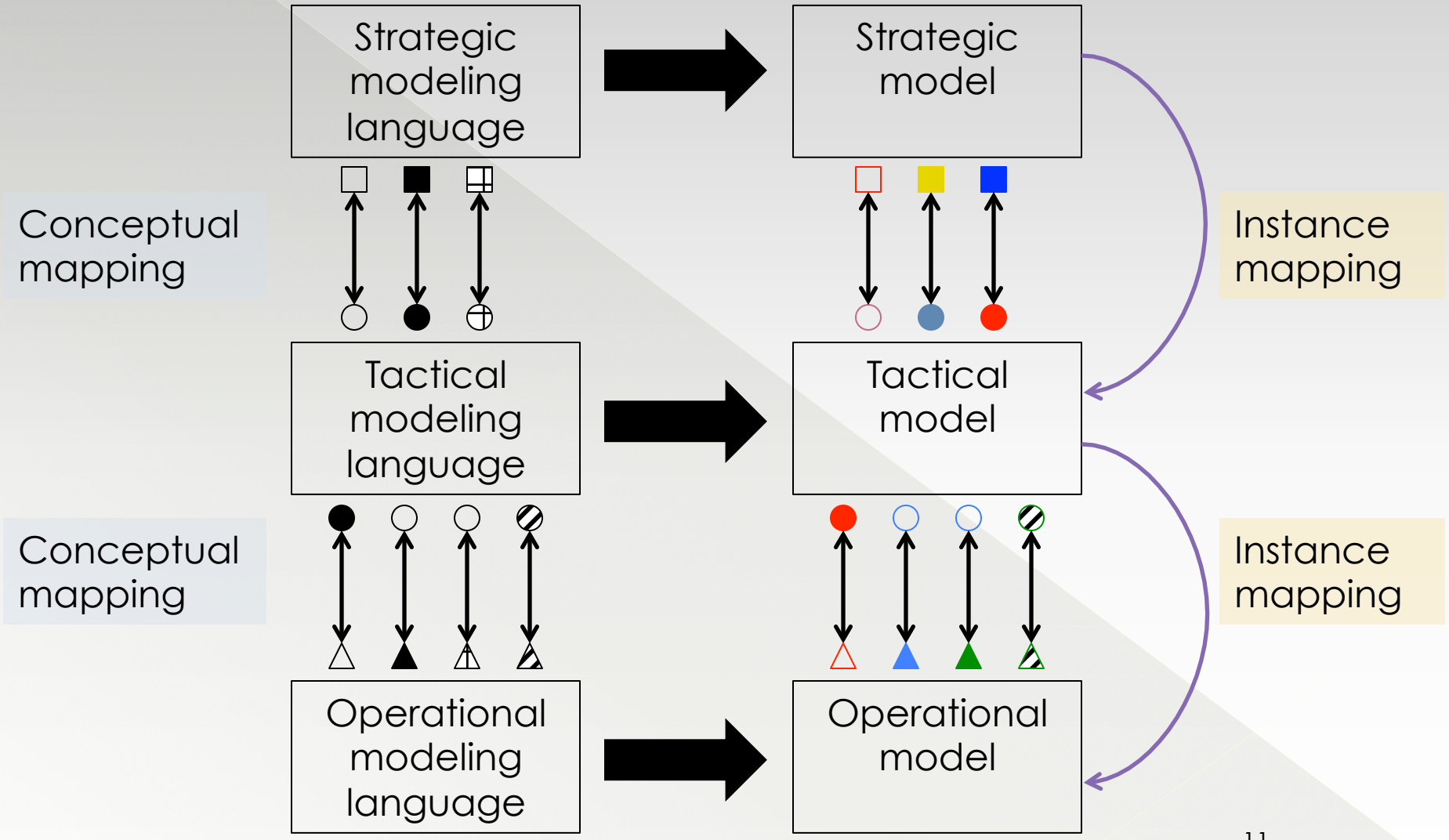
K': Exists CiT; Exists Bank A,B; B is reachable from A

R_o: Secure CiT transfer;

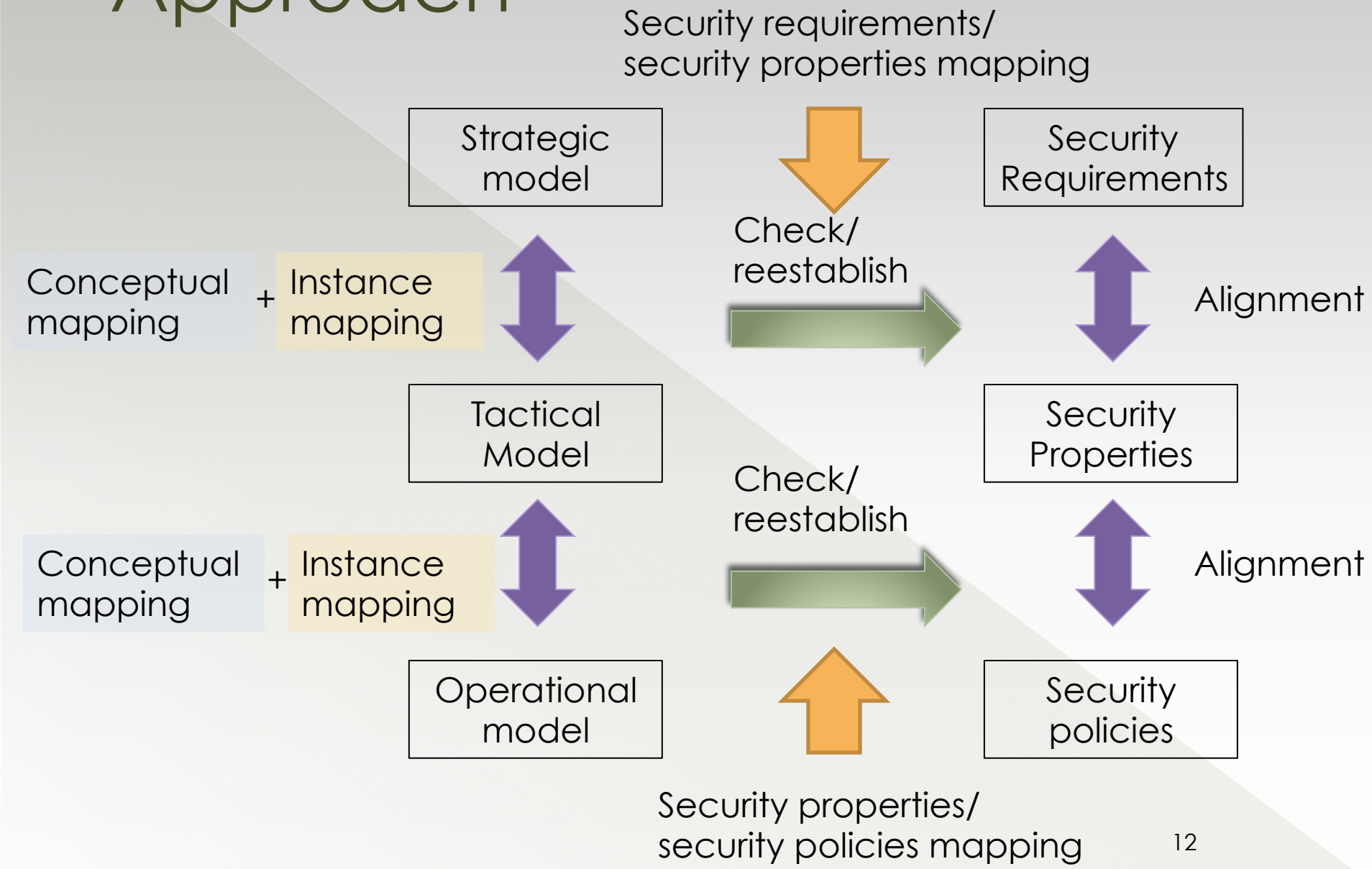
S_o: CiT max value 1mln E;
CiT max speed 50 Km/h

K'': CiT service is available

Approach


Strategic modeling language
Strategic model
Conceptual mapping
Instance mapping
Tactical modeling language
Tactical model
Conceptual mapping
Instance mapping
Operational modeling language
Operational model

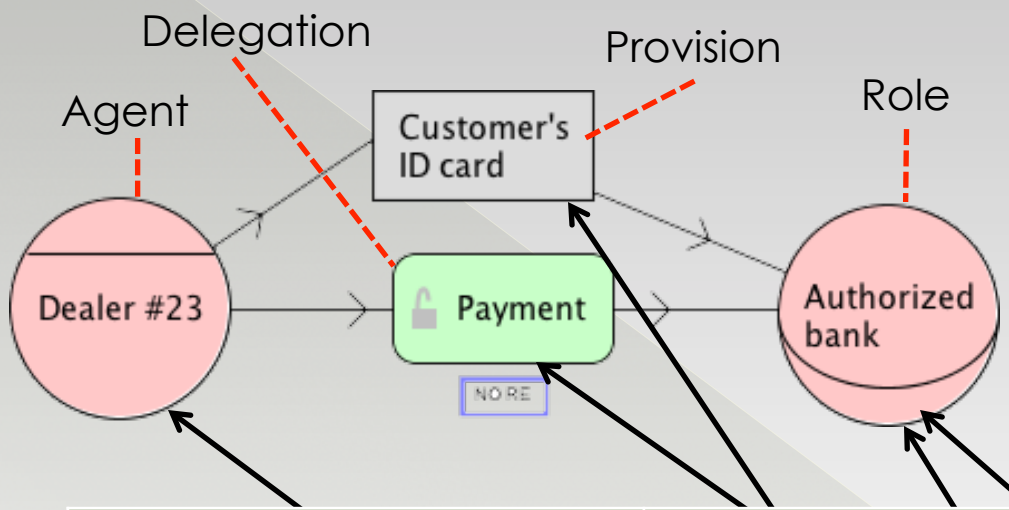
Approach


Security requirements/
security properties mapping
Strategic model
Security Requirements
Check/
reestablish
Conceptual mapping
+
Instance mapping
Alignment
Tactical Model
Security Properties
Check/
reestablish
Conceptual mapping
+
Instance mapping
Alignment
Operational model
Security policies
Security properties/
security policies mapping

Preliminary results

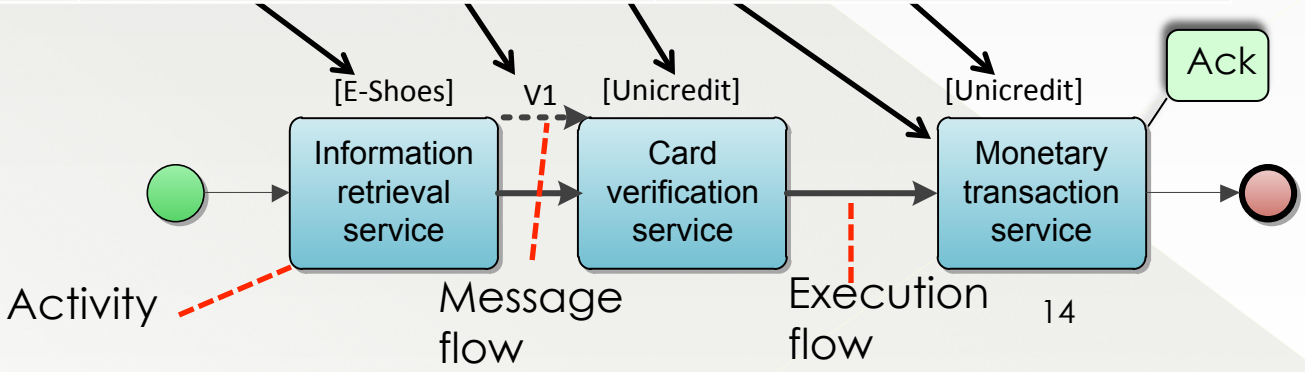
- We developed algorithms to check alignment between **strategic** and **tactical** security aspects **[Obj 1]**
- We chose
  - STS-ml[29] as strategical modeling language
    - Created for modeling STS
    - Focused on security
  - SecureBPMN[13] as tactical modeling language
    - Extends BPMN standards
    - Focused on security
- We implemented a software that uses the algorithms we created **[Obj 3]**

Conceptual mapping example



SecureBPMN concept	Relation	STS-ml concept
Participant	Is-a	Actor
Participant	Plays	Role
Data Object	Represent	Document
Activity	Relates-to	Goal

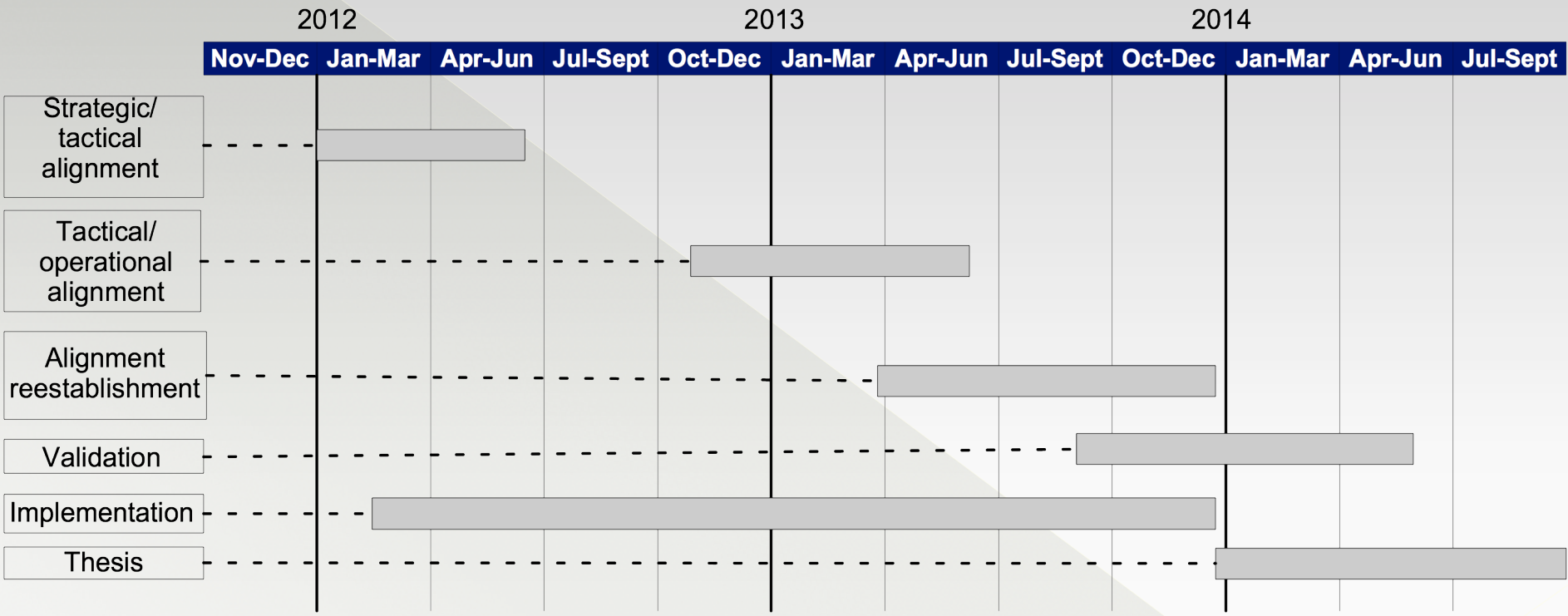
SecureBPMN Element	Relation	STS-ml Element
Unicredit	Is-a	Authorized bank
E-shoes	Is-a	Dealer#23
Money transaction	Relates-to	Payment
V1	Represents	CustomerID



Ongoing and future work

Objective	First results	Future work
OBJ1: Alignment check	-strategic and tactical alignment	-tactical and operational alignment
OBJ2: Alignment reestablishment		-use model transformation techniques
OBJ3: Tool support	-support STS-ml and SecureBPMN file formats -support alignment checking strategic and tactical level security aspects	-support alignment checking of tactical and operational level security aspects -support re-alignment
OBJ4: Validation	-first analysis on case studies	-validation with case studies -FP7 Aniketos

PhD plan


2012
2013
2014
Nov-Dec
Jan-Mar
Apr-Jun
Jul-Sept
Oct-Dec
Jan-Mar
Apr-Jun
Jul-Sept
Oct-Dec
Jan-Mar
Apr-Jun
Jul-Sept
Strategic/ tactical alignment
Tactical/ operational alignment
Alignment reestablishment
Validation
Implementation
Thesis

Conclusions

- Expected outcome
  - Semi-automated framework which helps analysts in managing alignment of security aspects
- Limitations
  - Modeling languages chosen
  - Focused on security
  - Heavily depends on human skills
- Novelty of our proposal
  - Check and reestablish alignment of security aspects in different abstraction levels
  - Usable both at design time and run time

Thank you!

Mattia Salnitri
mattia.salnitri@unitn.it
DISI
University of Trento, Italy

February 8th 2013

References

1. Andreas Bauer, Jan Jurjens, and Yijun Yu. **Run-time security traceability for evolving systems**. Comput. J., 54(1):58–87, January 2011.
2. T. D'Hondt, K. De Volder, K. Mens, and R. Wuyts. **Co-evolution of object-oriented software design and implementation**. In Mehmet Aksit, editor, Software Architectures and Component Technology, pages 207–224. Kluwer Academic Publisher, January 2001. Proceedings of SACT 2000.
3. Anne Etien and Camille Salinesi. **Managing requirements in a co-evolution context.** In Proceedings of the 13th IEEE International Conference on Requirements Engineering, RE '05, pages 125–134, Washington, DC, USA, 2005. IEEE Computer Society.
4. Andy Evans and Stuart Kent. **Core meta-modelling semantics of uml: The puml approach.** In Robert B. France and Bernhard Rumpe, editors, UML, volume 1723 of Lecture Notes in Computer Science, pages 140–155. Springer, 1999.
5. Jorge Fox and Jan Jurjens. **Introducing security aspects with model transformations.** In Proceedings of the 12th IEEE International Conference and Workshops on Engineering of Computer-Based Systems, ECBS '05, pages 543–549, Washington, DC,
6. Sepideh Ghanavati, Daniel Amyot, and Liam Peyton. **Compliance analysis based on a goal-oriented requirement language evaluation methodology.** In Proc. of RE'09, pages 133–142, 2009.
7. Aditya Ghose and George Koliadis. **Auditing business process compliance.** In Proceedings of the 5th international conference on Service-Oriented Computing, ICSOC '07, pages 169–180, Berlin, Heidelberg, 2007. Springer-Verlag.
8. Y. Liu, S. Muller, and K. Xu. **A static compliance-checking framework for business process models.** IBM Syst. J., 46(2):335–361, April 2007.
9. John Rushby. **Using model checking to help discover mode confusions and other automation surprises.** Reliability Engineering and System Safety, 75(2):167–177, February 2002.
10. Pamela Zave and Michael Jackson. **Four dark corners of requirements engineering.** ACM Trans. Softw. Eng. Methodol., 6(1):1–30, January 1997.
11. Mattia Salnitri, Fabiano Dalpiaz, and Paolo Giorgini. **Aligning Service-Oriented Architectures with Security Requirements.** In Proc. of the 20th International Conference on Cooperative Information Systems (CoopIS 2012), 2012. To appear.

References

12. W. M. P. van der Aalst and A. H. M. ter Hofstede. 2005. **YAWL: yet another workflow language.** Inf. Syst. 30, 4 (June 2005), 245-275.
13. Yulia Cherdantseva, Jeremy Hilton, and Omer Rana. **Towards SecureBPMN - aligning BPMN with the information assurance and security domain.** In Jan Mendling and Matthias Weidlich, editors, BPMN, volume 125 of Lecture Notes in Business Information Processing, pages 107–115. Springer, 2012.
14. Irem Aktug and Katsiaryna Naliuka. **Conspec - a formal language for policy specification.** Electronic Notes in Theoretical Computer Science, 197(1):45 – 58, 2008. Proceedings of the First International Workshop on Run Time Enforcement for Mobile and Distributed Systems (REM 2007).
15. P. Wohed, W.M.P. Aalst, M. Dumas, A.H.M. Hofstede, and N. Russell. **On the suitability of BPMN for business process modelling.** In Schahram Dustdar, JosLuiz Fiadeiro, and AmitP. Sheth, editors, Business Process Management, volume 4102 of Lecture Notes in Computer Science, pages 161–176. Springer Berlin Heidelberg, 2006.
16. http://www.ogf.org/documents/GFD.107.pdf
17. http://www.research.ibm.com/wsla/WSLASpecV1- 20030128.pdf
18. Eric S. K. Yu. **Towards modeling and reasoning support for early-phase requirements engineering.** In Proceedings of the 3rd IEEE International Symposium on Requirements Engineering, RE '97, pages 226–, Washington, DC, USA, 1997. IEEE Computer Society.
19. Paolo Bresciani, Anna Perini, Paolo Giorgini, Fausto Giunchiglia, and John My- lopoulos. **Tropos: An agent-oriented software development methodology**. Autonomous Agents and Multi-Agent Systems, 8(3):203–236, 2004.
20. http://www.uml.org/
21. R. Darimont, E. Delor, P. Massonet, and A. van Lamsweerde. **GRAIL/KAOS: An environment for goal-driven requirements engineering.** In 20th International Conference on Software Engineering ICSE'98, pages 58–62. ACM, 1998.

References

23. Fabio Massacci, John Mylopoulos, Federica Paci, Thein Than Tun, and Yijun Yu. **An extended ontology for security requirements.** In Camille Salinesi and Oscar Pastor, editors, CAiSE Workshops, volume 83 of Lecture Notes in Business Information Processing.
24. Mitchell A. Potter and Kenneth A. De Jong. 2000. **Cooperative Coevolution: An Architecture for Evolving Coadapted Subcomponents**. Evol. Comput. 8, 1 (March 2000), 1-29.
25. W.M.P. van der Aalst. **Formalization and verification of event-driven process chains**. Information and Software Technology, 41(10):639 – 650, 1999.
26. Guido L. Geerts and William E. McCarthy. **Modeling business enterprises as value-added process hierarchies with resource-event-agent object templates.** In in business object design and implementation, pages 94–113. Springer-Verlag, 1997.
27. Kyriakos Anastasakis, Behzad Bordbar, Geri Georg and Indrakshi Ray. **Uml2alloy: A challenging model transformation.** In In: ACM/IEEE 10th International Con- ference on Model Driven Engineering Languages and Systems (MoDELS, pages 436–450. Springer, 2007.
28. Alfonso Rodriguez, Eduardo Fernandez-Medina, and Mario Piattini. 2007. **Towards CIM to PIM transformation: from secure business processes defined in BPMN to use-cases**. In Proceedings of the 5th international conference on Business process management (BPM'07), Gustavo Alonso, Peter Dadam, and Michael Rosemann (Eds.). Springer-Verlag, Berlin, Heidelberg, 408-415.
29. Fabiano Dalpiaz, Elda Paja, and Paolo Giorgini. **Security Requirements Engineering via Commitments.** In Proc. of STAST'11, 2011.