

ST-Tool

**A CASE tool for security-aware software
requirements analysis**

Paolo Giorgini · Fabio Massacci · John Mylopoulos · Nicola Zannone

Tropos

Methodology for software development

- **Agent-oriented methodology**
 - Based on the notions of actor, goal, task, resource and social dependency
- **Software development phases:**
 - Early requirements
 - Late requirement
 - Architectural design
 - Detailed design

SecureTropos

Security-oriented extension to Tropos:

- capture *trust* and *security* requirements;
- distinguish between the actors that manipulate resources and actors that own the resources or the goals;
- two different *levels of analysis*:
 - social
 - individual

ST-Tool goals

Provide a *visual framework* to draw models

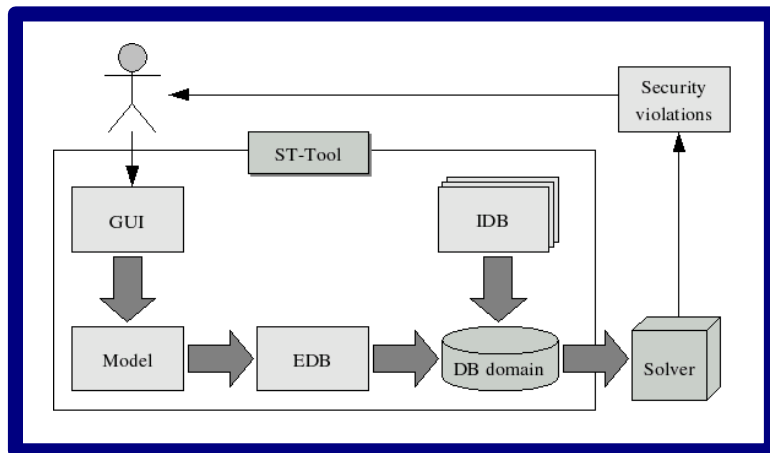
Maintain a consistent representation of the *data* underlying to graphical diagrams

Translate models into *formal specifications*

Analyze models through external *ASP solvers*

Use of ASP

Idea: considering the model as a database



- An Extensional Database (EDB) contains a set of all the rows (e.g. actors, services and relations)
- An Intensional Database (IDB) contains the axioms of the domain
- A second IDB is the properties database

Case study

Compliance to Italian data protection legislation

Definition and analysis of a ISO-17799-like security management scheme

Benchmark for the solvers:

- **starting from the structure of the university (base case) by adding a growing number of agents playing the roles occurring in the model**

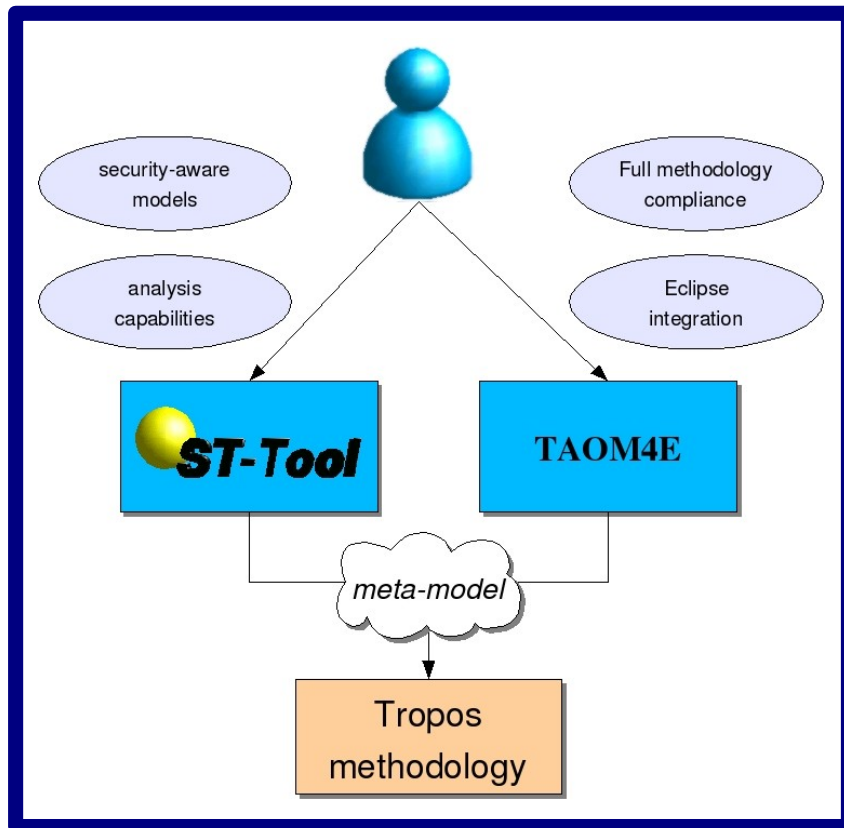
Results

<i>Solver</i>		<i>ASSAT</i>			<i>Cmodels-1</i>			<i>Cmodels-2</i>			<i>DLV</i>			<i>Smodels</i>		
<i>Problem / Instance</i>		<i>R</i>	<i>Wall</i>	<i>CPU</i>	<i>R</i>	<i>Wall</i>	<i>CPU</i>	<i>R</i>	<i>Wall</i>	<i>CPU</i>	<i>R</i>	<i>Wall</i>	<i>CPU</i>	<i>R</i>	<i>Wall</i>	<i>CPU</i>
UNITN	0	0	15.360"	0.200"	0	15.340"	0.210"	0	15.350"	0.190"	0	0.090"	0.000"	0	15.710"	0.240"
UNITN-1	24	0	1'6.010"	0.870"	0	1'5.230"	1.020"	0	1'5.460"	0.830"	0	0.310"	0.020"	0	1'5.670"	0.820"
UNITN-2	45	0	2'2.480"	3'30.030"	0	2'2.880"	3'27.070"	0	2'0.090"	3'26.740"	0	0.690"	0.020"	0	2'4.440"	3'28.610"
UNITN-3	62	1	43.800"	14.49'0"	1	42.580"	15.350"	1	42.720"	15.350"	0	0.940"	0.030"	1	43.680"	14.710"
UNITN-4	113	1	1'10.450"	56.910"	1	1'11.940"	55.160"	1	1'12.340"	56.800"	0	2.410"	0.010"	1	1'11.560"	55.060"
UNITN-5	166	1	33.440"	3.720"	1	33.080"	4.530"	1	33.590"	3.930"	0	4.970"	0.080"	1	33.640"	3.770"

**bi-processor XEON, 3.2 GHz, 1 MB of Cache, 4GB of RAM,
running Linux**

R: 0 - success; 1 - failure (e.g.: memory limits exceeded)

Methodology integration



TAOM4E modeler

- **Tool for Agent-Oriented modeling for Eclipse**
- **Supports full standard modeling methodology**
- **Oriented to interoperability (Eclipse)**

ST-Tool Demos

Case Study on Privacy Protection in the Enterprise

Demos

- **Create actor's model of goals**
- **Shows various format (XML, Formal Tropos, ASP)**
- **Show basic reasoning mechanism**

A bit of a show

- **Basic Demo (4 min)**
- **Short Demo (6 min)**
- **Long Demo (7past min)**

Conclusions

SecureTropos = Tropos + security extension

ST-Tool:

- **Diagram design**
- **Data model management**
- **Front-end to ASP**

ASP analysis:

- **Model consistency**
- **Detection of security lacks**

References

Web site: <http://www.troposproject.org>

- P. Giorgini, F. Massacci, J. Mylopoulos and N. Zannone.* Filling the gap between Requirements Engineering and Public Key/Trust Management Infrastructures. **In Proceedings of the 1st European PKI Workshop: Research and Applications (1st EuroPKI), LNCS 3093, pages 98-111. Springer-Verlag Heidelberg, 2004.**
- P. Giorgini, F. Massacci, J. Mylopoulos and N. Zannone.* Requirements Engineering meets Trust Management: Model, Methodology, and Reasoning. **In Proceedings of the Second International Conference on Trust Management (iTrust 2004), LNCS 2995, pages 176-190. Springer-Verlag Heidelberg, 2004.**
- P. Giorgini, F. Massacci, and J. Mylopoulos.* Requirement Engineering meets Security: A Case Study on Modelling Secure Electronic Transactions by VISA and Mastercard. **In Proceedings of the 22nd International Conference on Conceptual Modeling, LNCS 2813, Springer, 2003.**
- P. Giorgini, F. Massacci, J. Mylopoulos and N. Zannone.* Modeling Social and Individual Trust in Requirements Engineering Methodologies. **In Proceedings of the Third International Conference on Trust Management (iTrust 2005), LNCS 3477, pages 161-176. Springer-Verlag GmbH, 2005.**
- P. Giorgini, F. Massacci, J. Mylopoulos, A. Siena and N. Zannone.* ST-Tool: A CASE Tool for Modeling and Analyzing Trust Requirements. **In Proceedings of the Third International Conference on Trust Management (iTrust 2005), LNCS 3477, pages 415-419. Springer-Verlag GmbH, 2005.**