Università degli Studi di Trento

SERENITY System Engineering for Security & Dependability

How to
capture, model, and verify
the knowledge of legal, security, and privacy experts:
a pattern-based approach

L. Compagna, P. El Khoury	*F. Massacci*, N. Zannone	R. Thomas
Security Research SAP	Dept. Informatics and TLC Univ of Trento	Dept. of Law Univ. of Leuven

www.massacci.org

www.tropos-project.org

www.serenity-project.org

Outline

- **What is the Problem?**
  - Address Regulatory Compliance Demands
  - Organizational Patterns
- **Which is the Solution?**
  - Graphical requirements Engineer Methodology
- **Smart Items For Health Care**
  - An Example of a Pattern
- **Conclusion & Future Work**

What's the Problem?

- **Emerging trends in Security Enginering**
  - Security solutions can longer be best effort
  - Must show verifiable evidence with ….
- **Regulatory Compliance**
  - SOX/Basel II/EU Privacy Directive
- **Industry Compliance**
  - ISO 17799, ITIL Security Management..
- **Usage of SOA Mandatory**
  - WS-Security, WS-Trust, WS-Federations
- **Audit/Certification**
  - CC formal models, verification of the model

What's the Solution?

- **Security & Privacy Patterns for Organisation**
  - Security patterns are security best practices presented in template format
  - Validated by Experts
  - Patterns can provide implementations
    - From rule of procedures to running code
- **Concept widely used in Software Patterns**
  - Large repositories are available
  - Model-Based Transformatioon available for different languages

So what is the problem?

Ask a toad what beauty is, the to kalon? He will answer you that it is his toad wife with two great round eyes issuing from her little head, a wide, flat mouth, a yellow belly, a brown back. . . . Interrogate the devil; he will tell you that beauty is a pair of horns, four claws and a tail.

Voltaire, Philosophical Dictionary (1764)

To Design a Security Pattern

- **Ask a lawyer**

  17(4)1 For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 17(1) shall be in writing or in another equivalent form.

- **Ask a computer engineer**

```
<SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <Transforms>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>
                FLuQTa/LqDIZ5F2JSaMRHSRuaiQ=
        </DigestValue>
</SignedInfo>
```

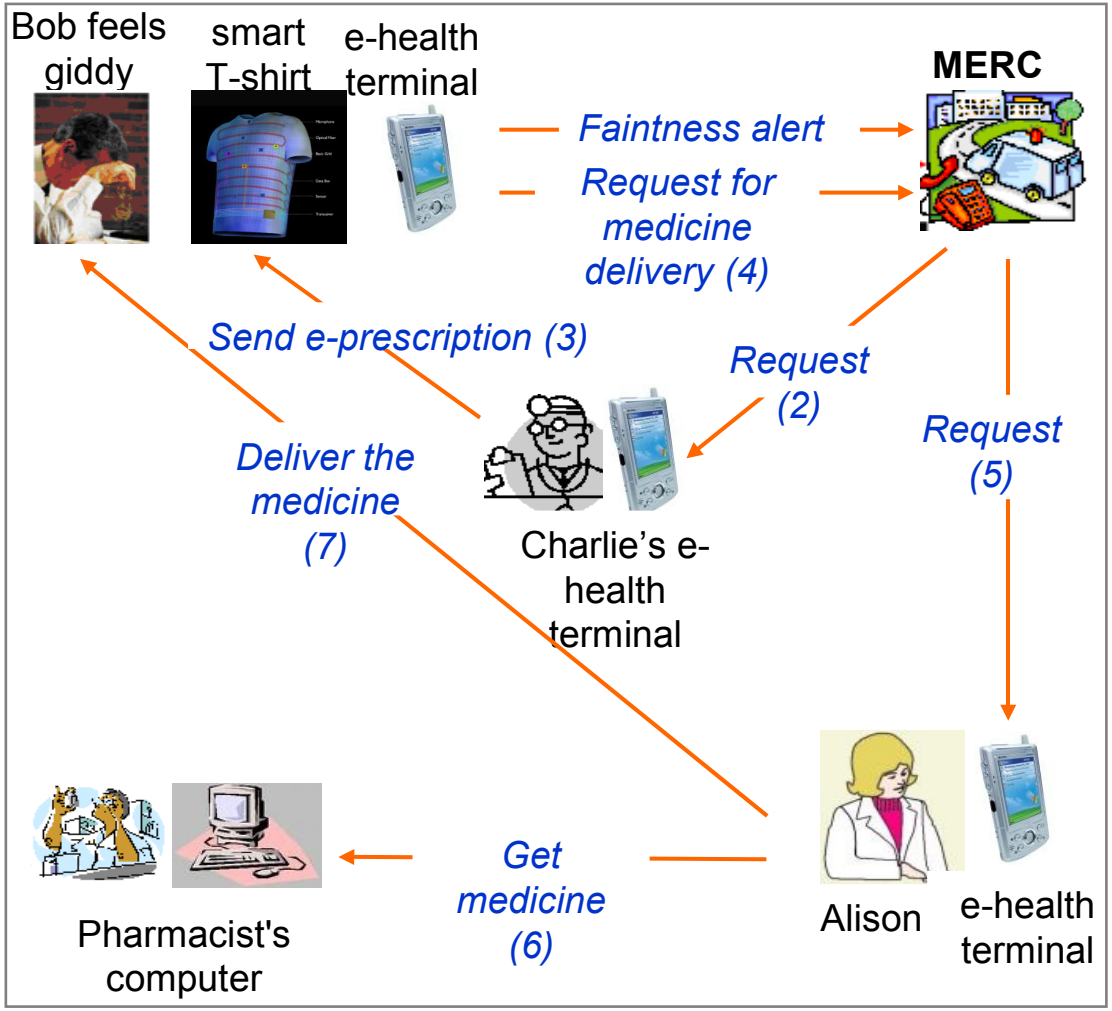
- **Ask a formal methods expert**

```
Fail_NonRepudiation(A,B,S) :- del_exec(A,B,S),  not entrust_exec(A,B,S)
entrust_exec (A,B,S) :- trust(A,B,S).
entrust_exec (A,B,S) :- prove_fulfillment(A, B, S, TP)
prove_fulfillment(A, B,S, TP) :- provides(B, PoF), proof_of_fulfillment(PoF, S),
        entrust_exec(TP, B, PoF), entrust_exec(A, TP, PoF)
```

Lingua Franca…

- **Software Patterns work because they essentially are by toads only**
  - The difference between C++, Java, C#, Eiffel, Perl, Python etc is negligible compared to the ones just made
- **Security Patterns needs integration of different "languages"**
- **Idea: a picture is worth a thousand words**
  - Provided you are able to get the picture from the words and the words back from the picture

Smart Items For Health Care



Steps:

2. Bob feels giddy and sends via his e-health terminal a request for assistance to MERC.
3. MERC receives the request and, since Bob's doctor is in vacation, redirects it to Charlie.
4. Charlie analyses Bob's medical data and history and sends to Bob an e-prescription.
5. Bob requests MERC for a medicine delivery.
6. MERC selects Alison to execute this task, sends a message to her to which she promptly acknowledge receiving then back the data for accomplishing this activity.
7. Alison goes to the pharmacy and after a successful credentials exchange, she gets the medicine from the pharmacist.
8. Alison delivers the medicine to Bob.

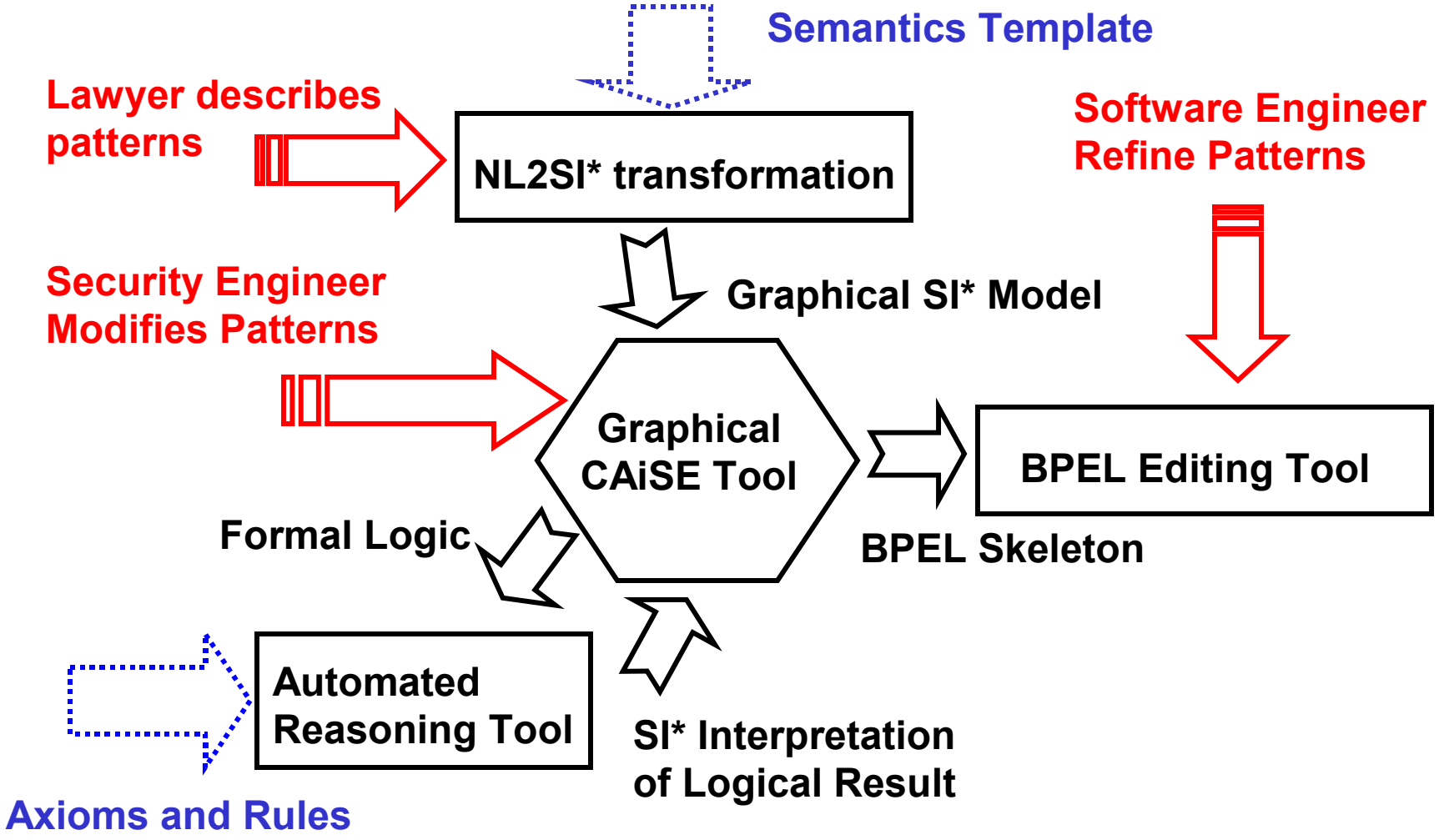
Notes: this last step involves an exchange of electronic credential between Bob and Alison. Their e-health terminals are used at this purpose.

Bob.

Goal-Based Req. Engineering

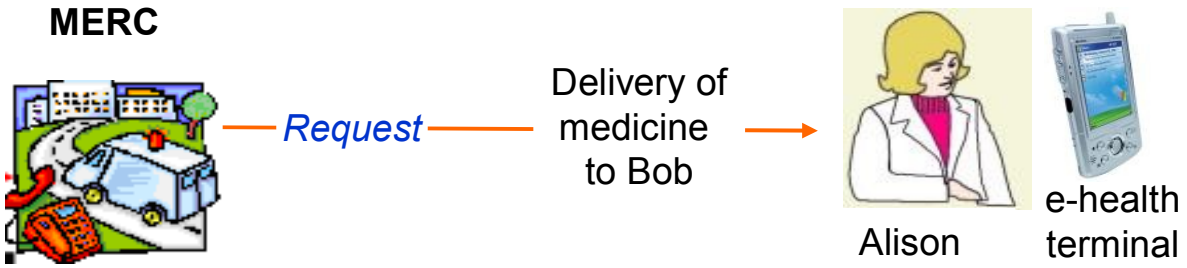
- **Graphical Requirement Language SI***
  - Agents, Roles, Relations among them
  - Execution, Delegation of Permissions
- **Legal text**
  - (semi) automatic extraction of graphical model from Natural Language description
- **Logical Formulae**
  - Experts provide general axioms and property descriptions
  - Instances added automatically from graphical model
- **Executable Business Process**
  - (Semi) automatic BPEL generation from graphical model

Pattern Design and Validation



Non repudiation requirement presented in SI*

The Employer (MERC) shall have evidence that the Executor (Alison) cannot repudiate her commitment.



What is an organizative security pattern?

Security Requirements

NOT fulfilled

Fulfilled

Initial organizational structure

- Agents
- Resources
- Tasks
- Relations: delegation, trust…

Security Pattern

Revised organizational structure

- *Add/Remove* Agents
- *Add/Remove* Resources
- *Add/Remove* Tasks
- *Add/Remove* Relations

Context

Solution

SI* MODELS

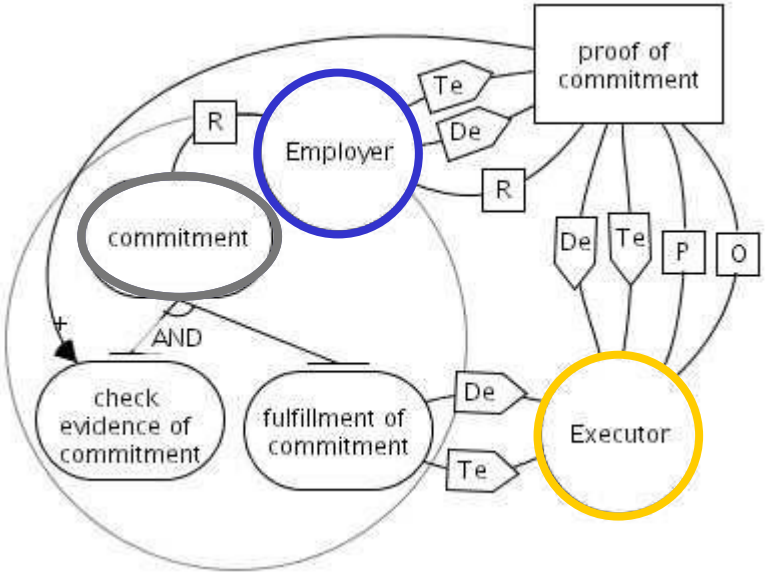
Non repudiation pattern

[Context and Requirement]

Context: The Employer *requests* the achievement of a commitment and *delegates* its *execution* to the Executor.

Requirement: the former has *no warranties* that the latter takes the responsibility of *achieving* the *commitment*

Non repudiation pattern
[Context, Requirement and Solution]



Solution: The Employer refines the commitment into two sub parts.

3. Check the evidence about responsibilities taken by the Executor.
4. Represents the actual desire of fulfilling the commitment.

Conclusion & Future Work

- **System designers are usually neither security nor legal experts**
  - Graphical RE notation useful common ground
- **Idea: a picture is worth a thousand words**
  - Provided you are able to get the picture from the words and the words back from the picture
- **Future Work**
  - Improving model construction from NL
  - Reasoning capability only detect failed properties, should also suggest what is missing to satusfy them
  - Apply to other domains
- **Ack**
  - Supported by the EU through the EU-IST-IP SERENITY