An Approach to Formalise Security Patterns

Luis Sergio da Silva Junior,
École Polytechnique de Montréal

March, 2013
Context

Software Development

- Methods, Techniques and Tools
- Reuse
- Design Patterns
- Security Patterns
## Security Patterns

### Properties

- Group of patterns focused on security context
- Threat, Attack, Attacker, Asset etc
- UML diagrams
- Originally, not formally specified
Example 1

- Single Access Point
- Guard Door
Security Patterns

Example 2

- Roles
- Group of roles
- Restrict Access
Formal Methods (FM) consist of a set of techniques and tools based on mathematical modeling and formal logic that are used to specify and verify requirements and designs for computer systems and software.

- OCL and extensions
- Petri Nets
- ASM
- others
Correct implementation of restrictions and properties
Avoid Threats and bad implementation
Security Improvement
Petri Nets

- Places, Tokens and Arcs
- Different Types (Coloured, Temporized)
- CPN-Tools
- Why Petri Nets?
Study Case

- Sender-Receiver example
- Microarchitecture example
- constraint - **the size of the message cannot be longer than 10**
- Structural analysis - PADL and Reflection structure
- Behavioural analysis - Comparison between the pattern and the Petri Net structure
Structural analysis

- Pattern detection through structural analysis
- Class diagrams
- Send its result to the next step
Structural analysis
Structural analysis

- Create a Pattern Model using PADL
- Comparison with Real objects - using Java Reflection API
- Compare all attributes, associations
- Display accuracy.
Behavioural analysis
Create Coloured Petri Net Model by CPN-Tools

Using XML extractor from the .cpn file

Using Classes, Interfaces to keep the information on Java structure

Extract method internal structure from .java file

Compare expressions and attributions from the java source code with the Petri net arc inscription.

Display accuracy
Expressions and Attributions
Future Work

- Testing with a Real System
- Single Access Point, Roles, Session
- Evaluate Version with Simulation of Petri Net model
- More Formal Methods
- Provide running analysis.
Future Work

- Find the pattern in some complex structure
- Petri Net restriction - named places and transitions
- Different calls, same idea (length and size)
Acknowledgment