Institut
Mines-Telecom

SysML-Sec Attack Graphs: Compact Representations for Complex Attacks

Ludovic Apvrille
ludovic.apvrille@telecom-paristech.fr

Yves Roudier
yves.roudier@eurecom.fr

GraMSec'2015

Outline

Context: Security for Embedded Systems
- Embedded systems
- SysML-Sec

Attack trees

Contribution

Conclusion

Examples of Threats

Transport systems

Use of exploits in Flight Management System (FMS) to control ADS-B/ACARS [Teso 2013]

(C) aviationweek.com

Internet of Things

Proof of concept of attack on IZON camera [Stanislav 2013]

Medical appliances

Infusion pump vulnerability, April 2015. http://www.scip.ch/en/?vuldb.75158

(C) Hospira

Designing Safe and Secure Embedded Systems: SysML-Sec

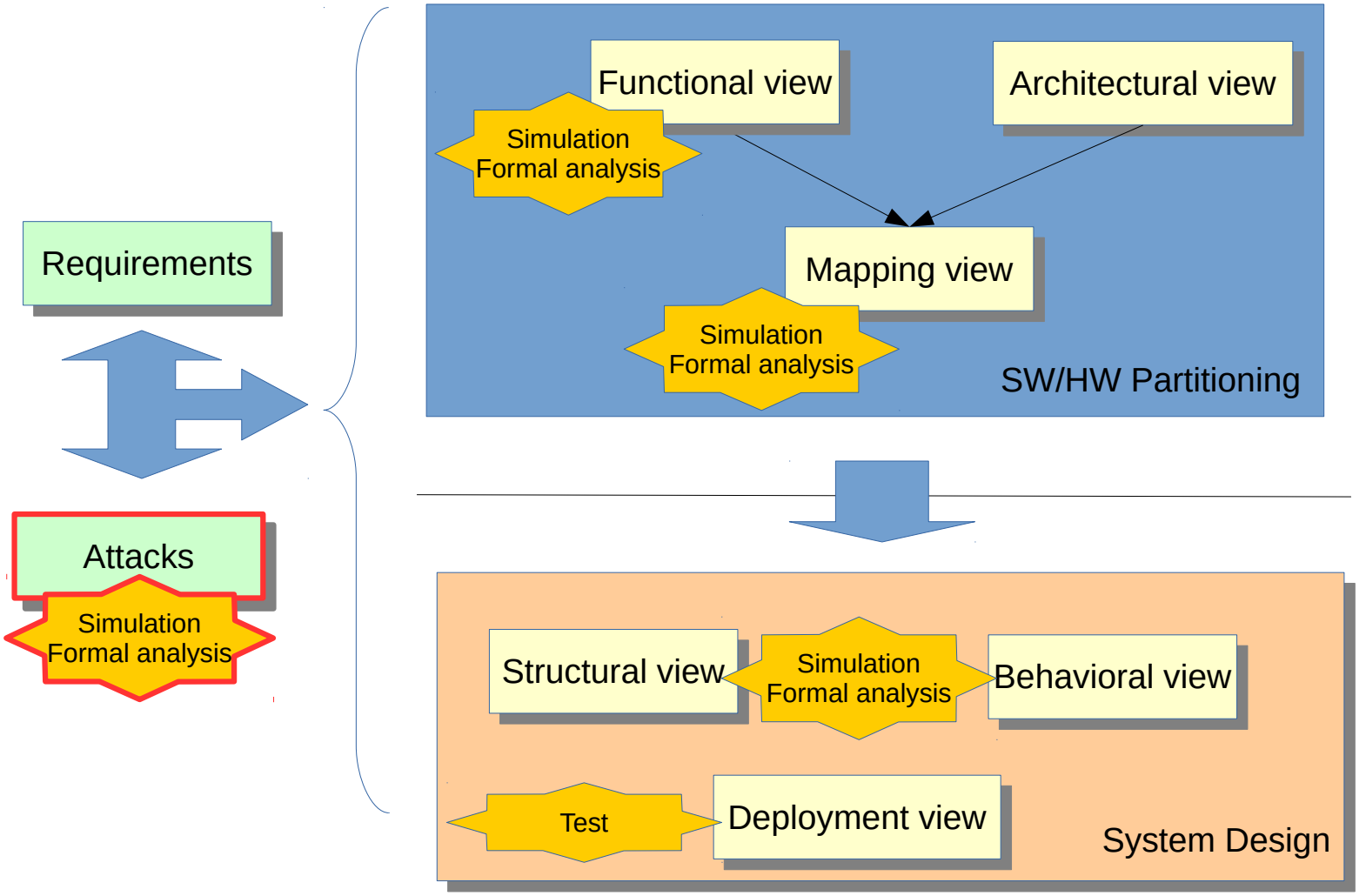
Main idea

- **Holistic approach**: bring together experts in embedded system architects, system designers and security experts

Common issues (addressed by SysML-Sec):

- Adverse effects of **security over safety/real-time/performance** properties
  - Commonly: only the design of security mechanisms
- **Hardware/Software partitioning**
  - Commonly: no support for this in tools/approaches in MDE and security approaches

SysML-Sec: Methodology



Fully supported by TTool

Outline

Context: Security for Embedded Systems

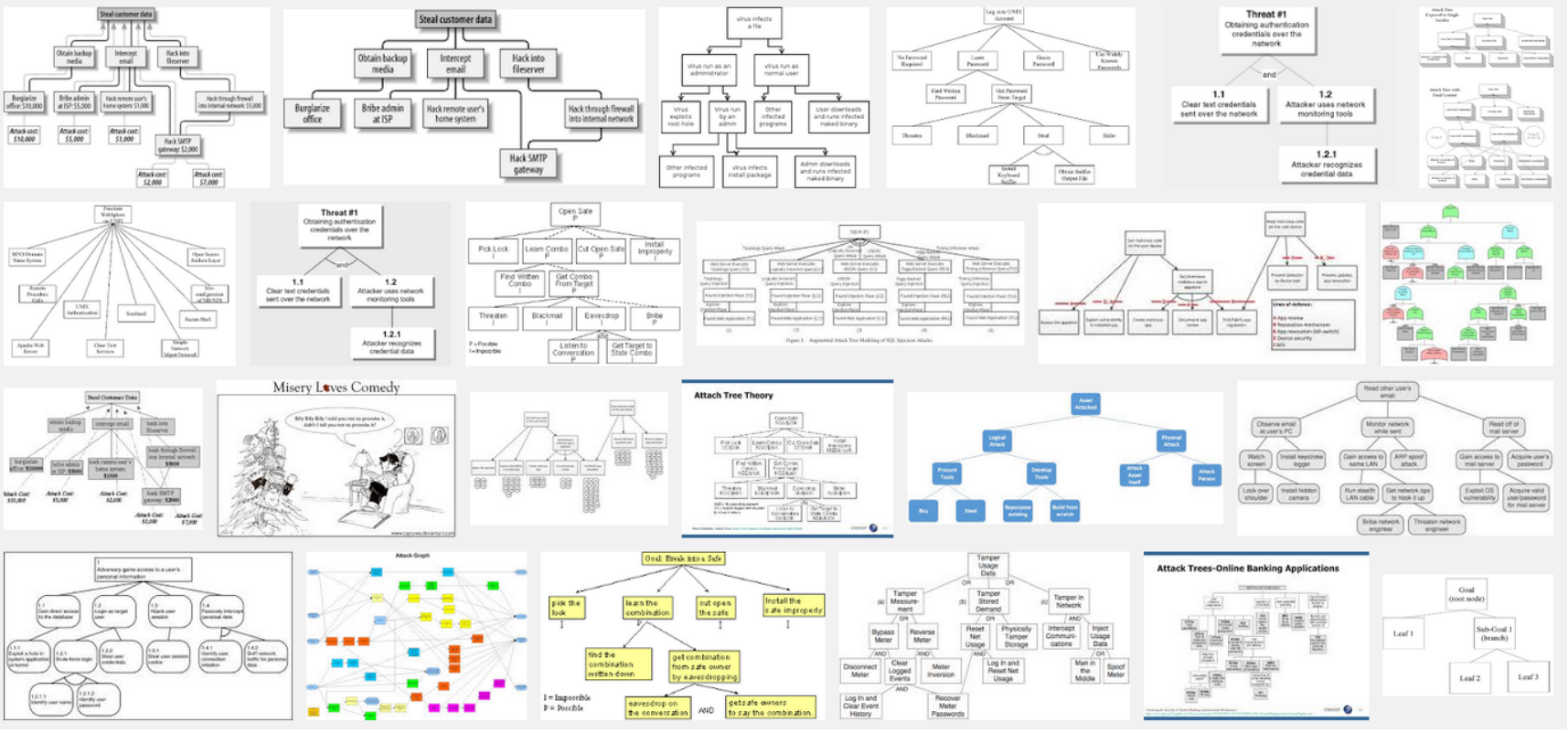
Attack trees

Attack trees

Contribution

Conclusion

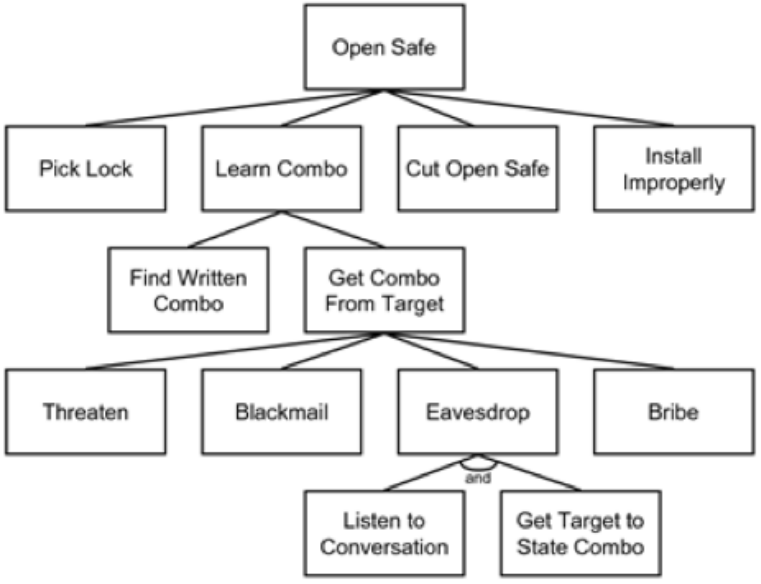
Google-izing Attack Trees



Attack Trees

Definition and purpose

- Originate from fault trees, introduced by Bruce Schneier (1999)
- Depict how a system element can be attacked
  - Helps finding attack countermeasures
- Root attack, children, leaves
- OR and AND relations between children



Attack Trees: Related Work

- Generation of ATs from other formalisms [Vigo 2014]
- Semantics extensions
  - [Khand 2009]
    - *PAND*, *k-out-of-n*, *CSUB*, *SEQ*, ...
  - [Zhao 2014]
    - Permissions and capabilities on nodes
    - Applied to malware analysis
- Security assessment
  - Privilege graphs [Dacier 1996]
  - Petri nets [Dalton 2006] [Pudar 2009]
  - Markov processes [Piètre-Cambacédès 2010]

Attack Trees: A Few Issues

Semantics

- Semantics of AND and OR is limited to express complex attack scenarios
  - No ordering between attacks
  - No temporal operators

Relation with other development stages

- No relation with (security) requirements
  - More generally, not integrated into methodologies
- No relation between attacks and the HW/SW components of the system
  - Difficult to figure out the where and which of countermeasures

Outline

Context: Security for Embedded Systems

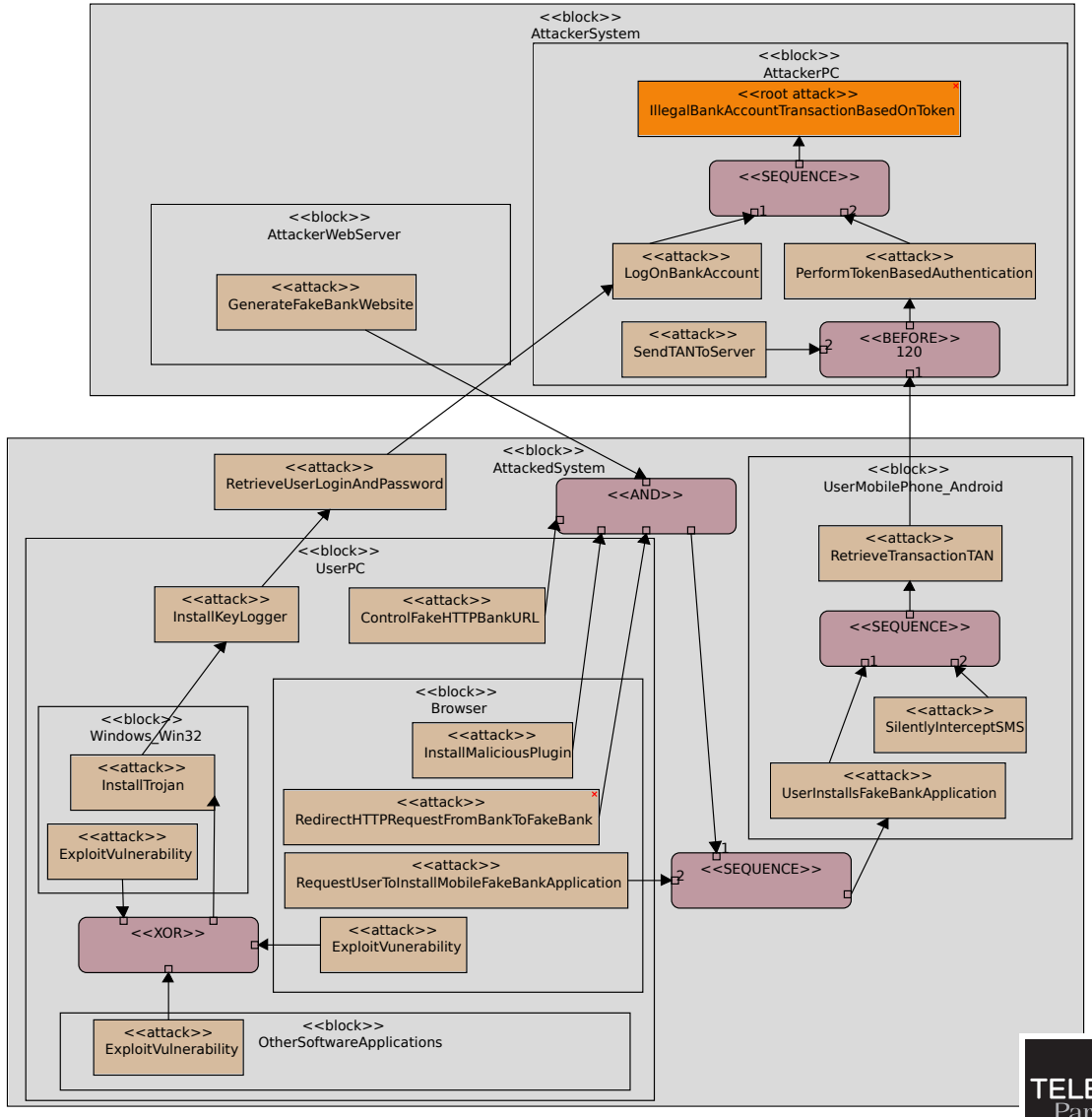
Attack trees

Contribution
- New operators

Conclusion

Overview (with an Example)

- SysML Parametric diagram
- Asset = Block
- Attacks = Attributes of blocks
- Relation between attacks = Constraints
- Formal semantics
  - Timed automata

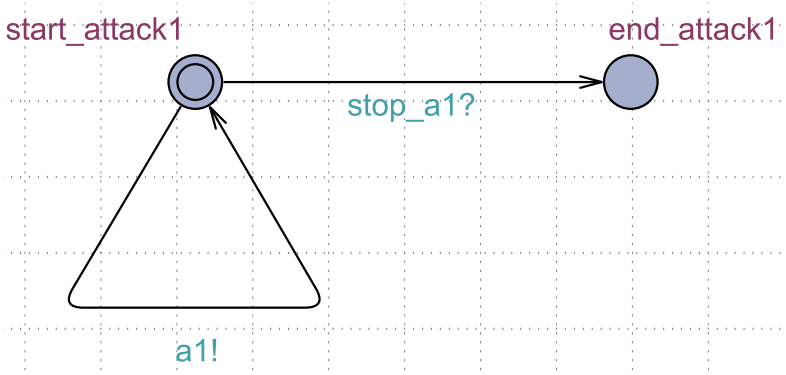


Semantics

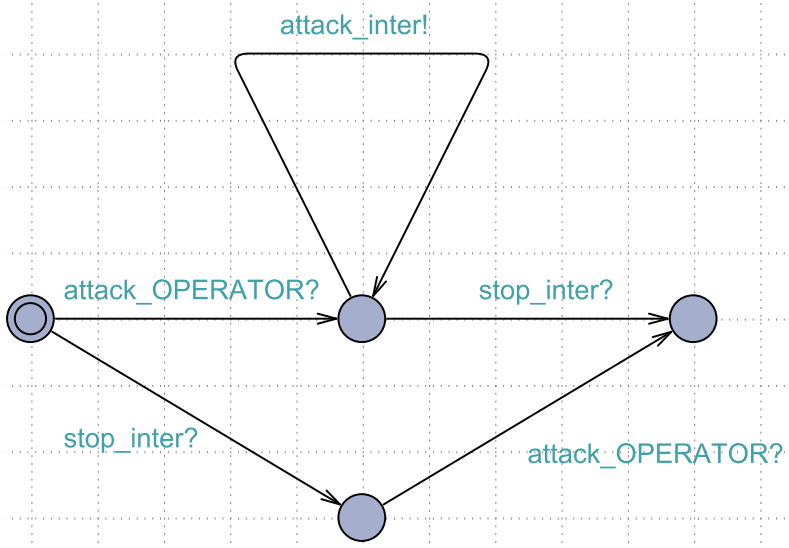
- Attacks
- Intermediate attacks
- Root attack
- Constraints
  - AND, OR, XOR, SEQUENCE, BEFORE, AFTER

Semantics of Attacks

Attack

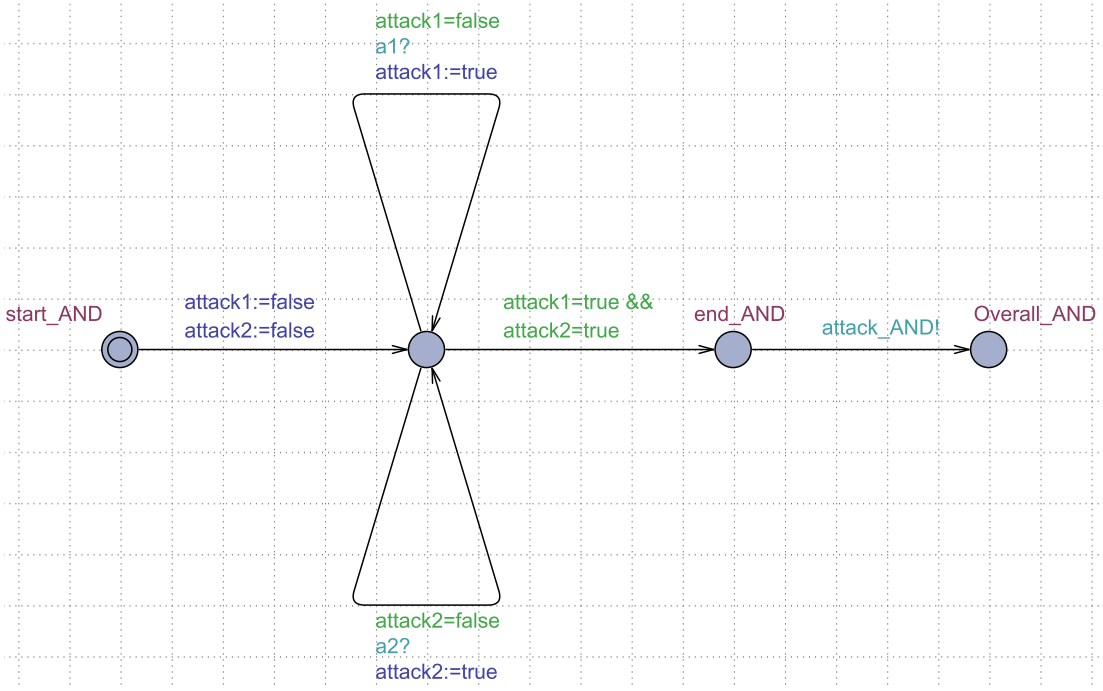


Intermediate Attack

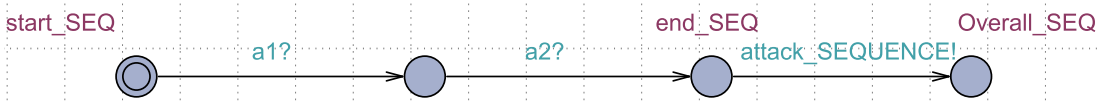


Semantics of Constraints

AND

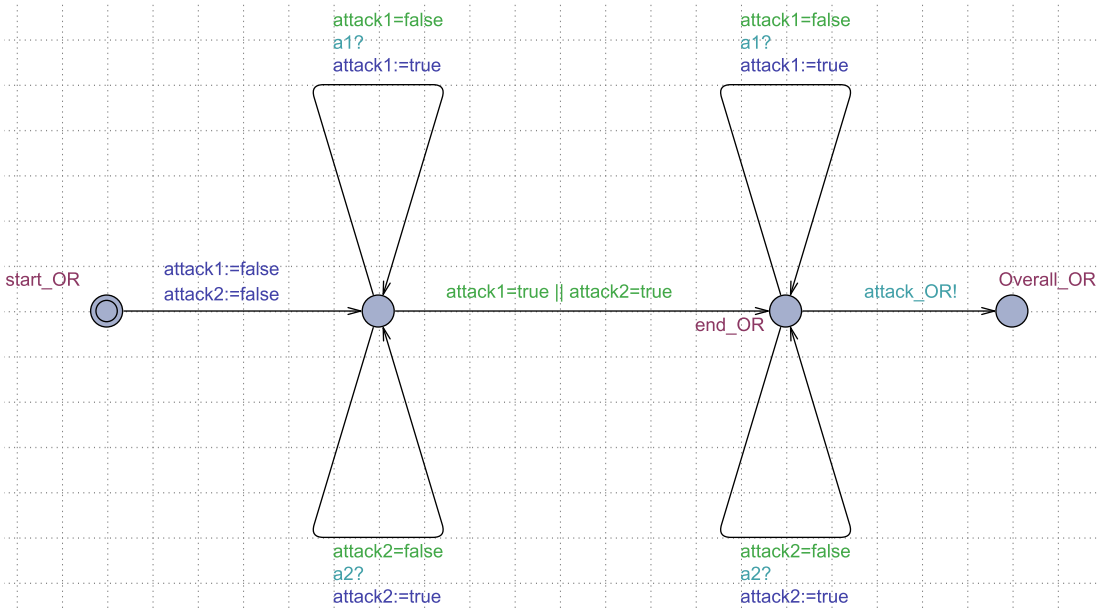


SEQUENCE

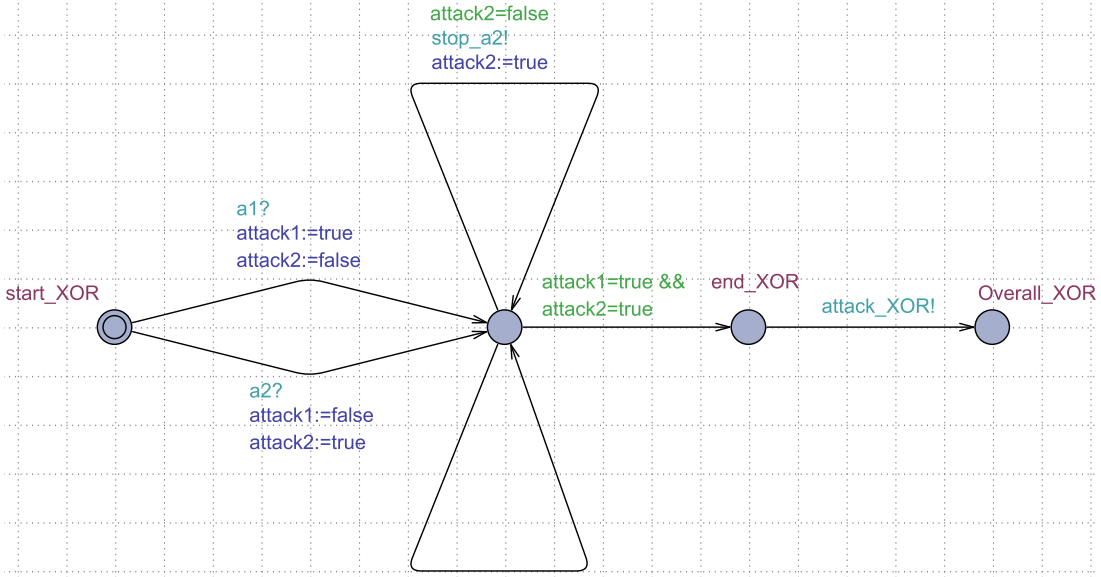


Semantics of Constraints (Cont.)

OR

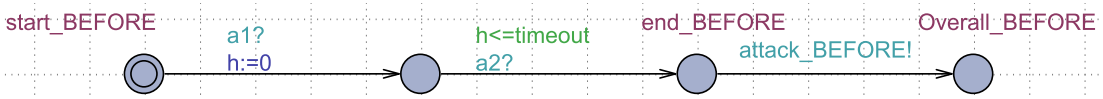


XOR

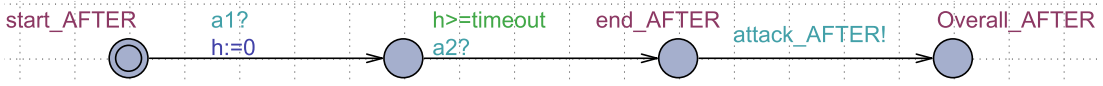


Semantics of Constraints (Cont.)

BEFORE

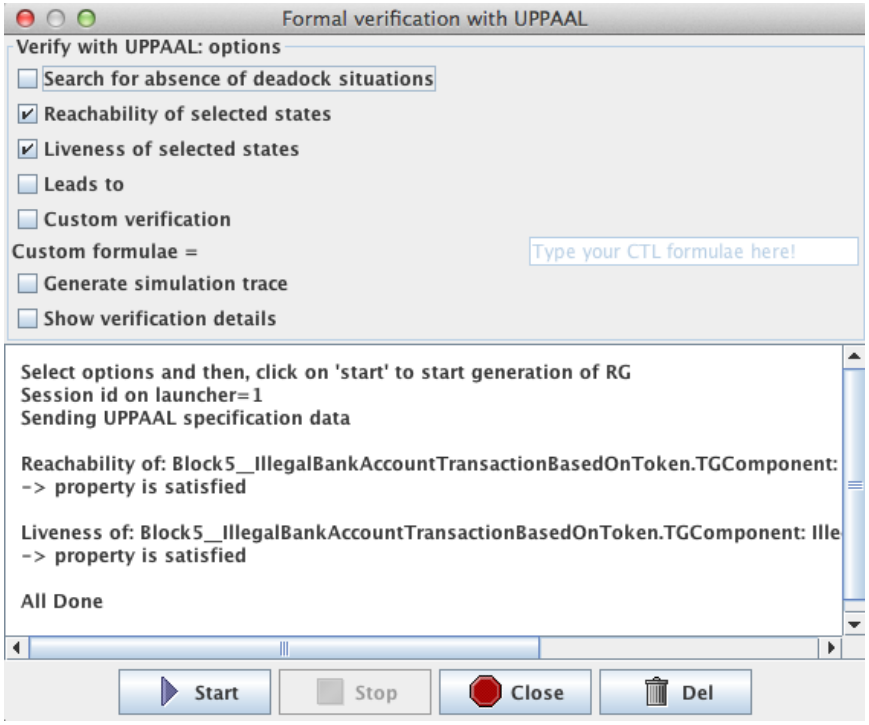


AFTER



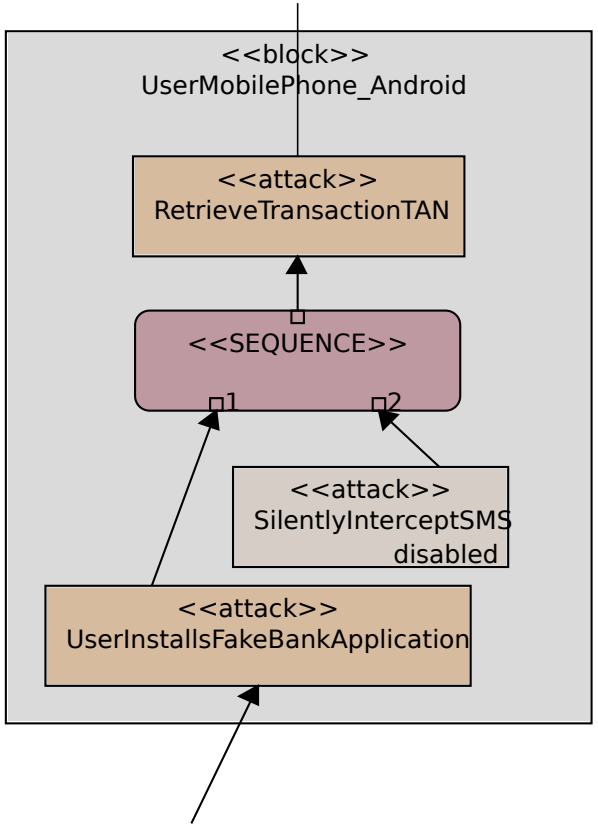
Formal Verification

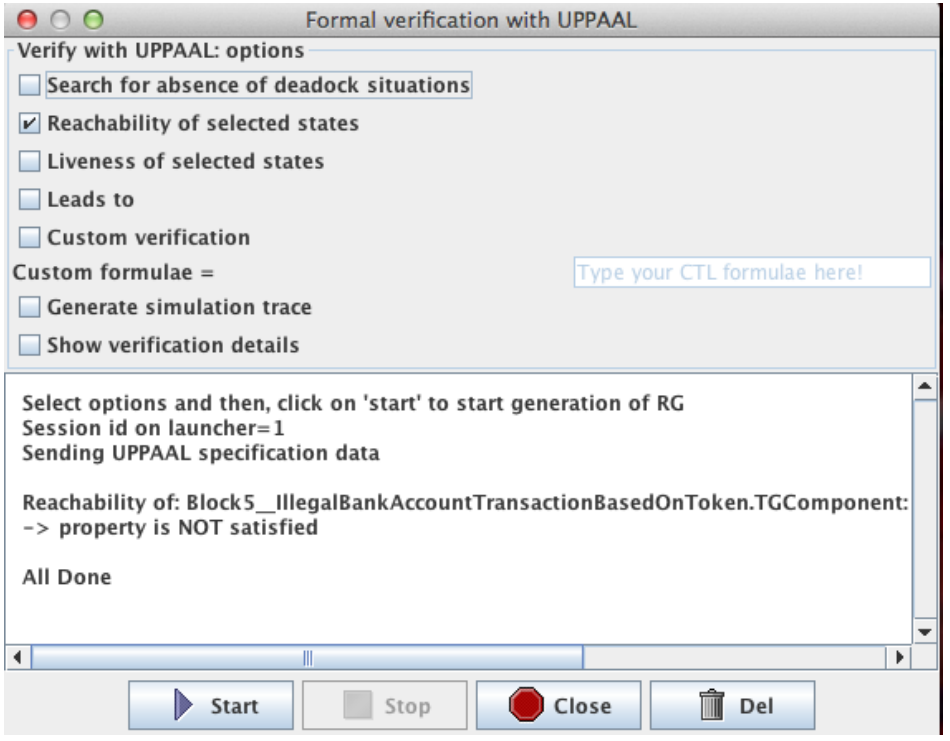
- Reachability of an attack a
- Liveness of an attack a
- a_1 Leads to a_2 ($a_1 \rightsquigarrow a_2$)



Disabling Attacks

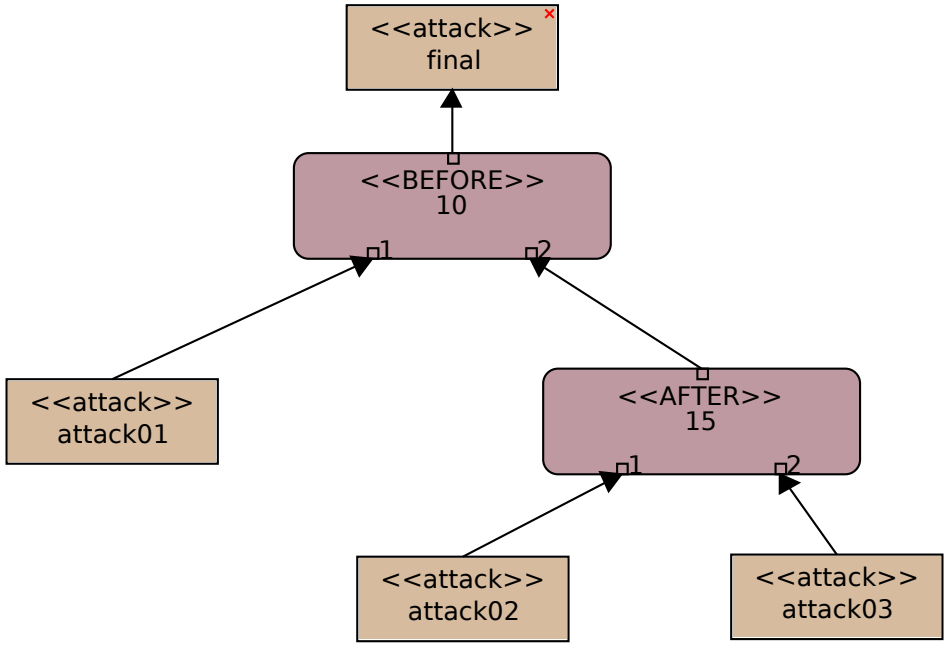
- Right click to disable/enable an attack





Temporal Compatibility

- Temporal constraints may impact attacks reachability/liveness



Outline

Context: Security for Embedded Systems

Attack trees

Contribution

Conclusion

Conclusion, future work and references

Conclusion and Future Work

Achievements

- Extended and formally defined attack trees
- Integrated into SysML-Sec
- Fully supported by TTool
- Applied to different domains, e.g., malware, automotive systems

Future work

- Handling new situations
  - Cycles, nb of iterations, priorities
- Quantitative assessments of threats

To Go Further ...

Web sites

- https://sysml-sec.telecom-paristech.fr
- https://ttool.telecom-paristech.fr

References (SysML-Sec)

- Ludovic Apvrille, Yves Roudier, "SysML-Sec: A SysML Environment for the Design and Development of Secure Embedded Systems", Proceedings of the INCOSE/APCOSEC 2013 Conference on system engineering, Yokohama, Japan, September 8-11, 2013.