Institut
Mines-Telecom

SysML-Sec: A model Driven Approach for Designing Safe and Secure Systems

Ludovic Apvrille, Yves Roudier
ludovic.apvrille@telecom-paristech.fr
yves.roudier@eurecom.fr

SPIE'2015

Outline

Context

Security for embedded systems and cyber-physical systems

Contribution: SysML-Sec

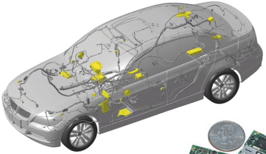
- Overall methodology
- Security Requirements and HW/SW Partitioning
- Design of Cryptographic Protocols

Context

Embedded systems?

- "Computer system with a dedicated function within a larger mechanical or electrical system" [Wikipedia]
- Designed on-purpose for specific control functions
- Integrated: Software + Hardware
  - Many technologies, increasingly distributed and communicating systems

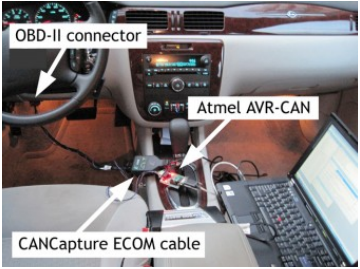





Embedded Systems: Example of Threats

Automotive systems

- Tire Pressure Monitoring System wireless link [Rouf 2010]
- Keyfob authentication [Francillon 2011]
- Vulnerabilities of onboard network [Koscher 2010]
- HU remotely exploitable vulnerabilities [Checkoway 2011]
- Locksmith tool (CAN/LIN injection) [MultiPick 2012]



Embedded Systems: Example of Threats (Cont.)

Avionics Systems

- Abusing the Automatic Dependent Surveillance Broadcast (ADS-B) protocol [Costin 2012]
- Use of exploits in Flight Management System (FMS) to control ADS-B/ACARS [Teso 2013]

Internet of Things

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

Our Proposal: SysML-Sec (and TTool)

Bring together system engineers & security experts

Security is not supported by SysML

- Yet, security is not an add-on
- Can have adverse effects on safety/real-time properties

Security requirements

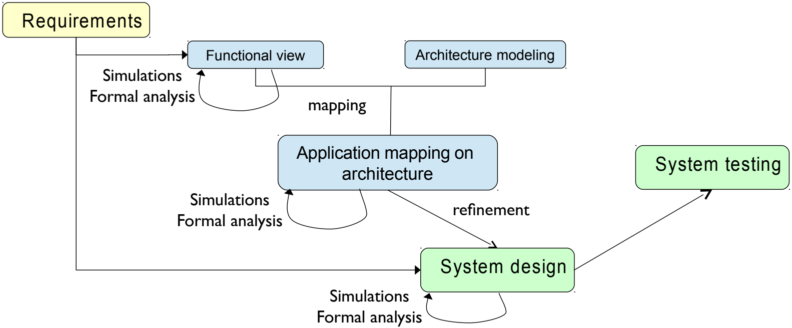
- Lack of functional and safety requirements
- Some tools directly address security mechanisms configuration
- No hardware capabilities

Hw/Sw partitioning is central

- Support in MDE approaches not common
- Complex Architecture = CPUs, middleware, ...
- No security concerns

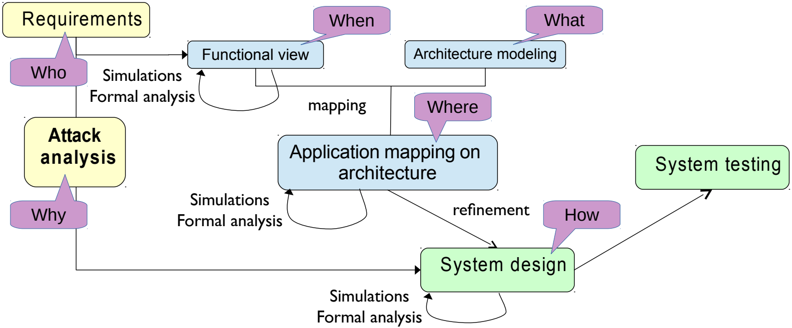
Y-Chart and V-Cycle

- Mapping process
  - Objective is to optimize the system w.r.t. various criteria (cost, area, power, performance, flexibility?)
- Fully supported by the free and open-source UML/SysML toolkit "TTool"



The Y-Chart Revisited

- **Who**: Stakeholders + attackers & capabilities (risk analysis)
- **When**: Attacks envisioned that motivate security countermeasures
- **Why**: Attacks envisioned that motivate security countermeasures
- **What**: Assets to be protected
- **Where**: Architecture mapping of functions involving those assets
- **How**: Security architecture (e.g., network topology, process isolation, etc.)



Safety Properties: Model and Proof

Model

- Parametric diagrams
- Observers in block diagrams
- CTL formulaes

Proof

- Functional view: deadlock, reachability
- Partioning: Same as in the functional view, plus the time constraints
  - Restriction of traces from the functional view
  - Takes into account the underlying hadrware / software resources
- Design: deadlock, reachability, time constraints

TELECOM ParisTech

Security Properties: Model and Proof

Model

- Partitioning: Security mechanisms
- Design: pragmas expressing confidentiality and authenticity properties

Proof

- Partitioning: Compatibility of security mechanisms w.r.t. safety properties
  - Respect of real time deadlines
  - System latency
  - Usage of the platform: computation power, the load of buses, . . .
- Design: Proof of authenticity and confidentiality properties
  - Automated translation to ProVerif specifications

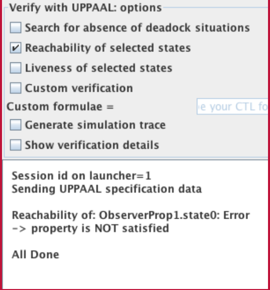
TELECOM ParisTech

SysML-Sec Design Formal Verification

- Push button approach, both for safety and security properties!

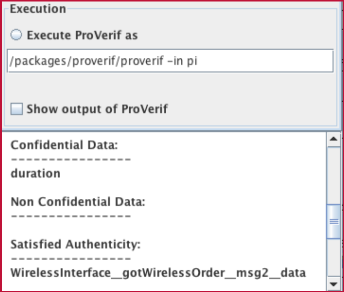
Safety properties

UPPAAL based



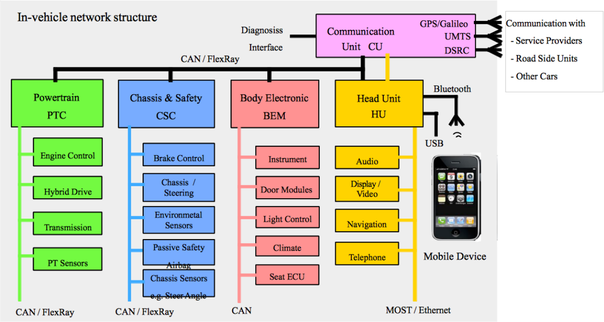
Security properties

ProVerif based



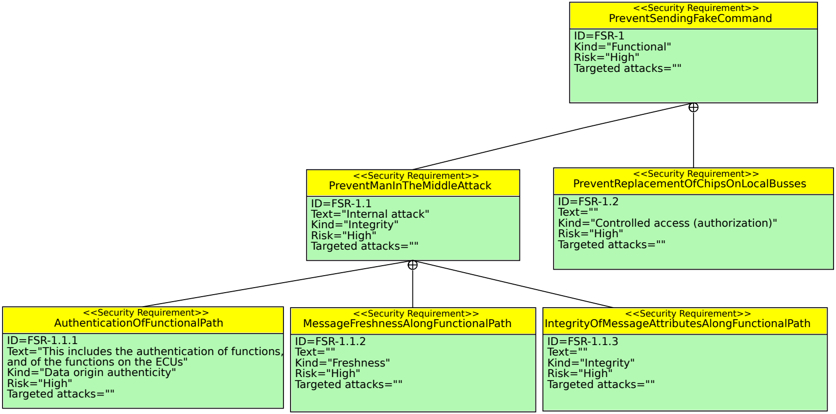
Demonstration

- Example taken from the EVITA european project
  - First generic security architecture for automotive communicating systems

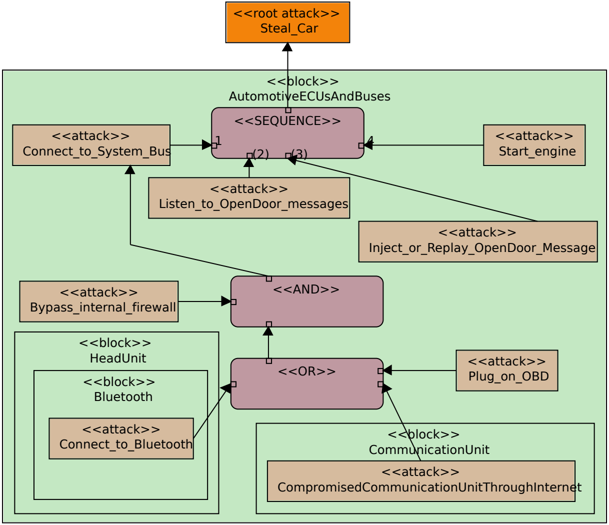


TELECOM ParisTech

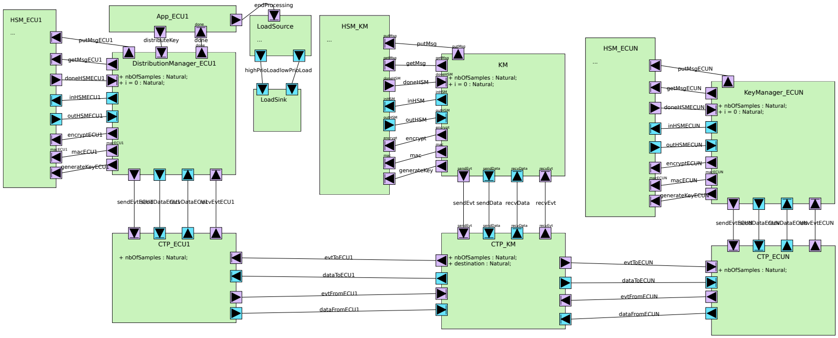
Security Requirements



Threats and Attacks

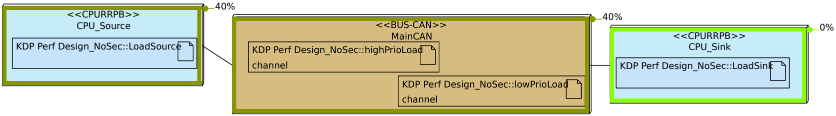


Functional View

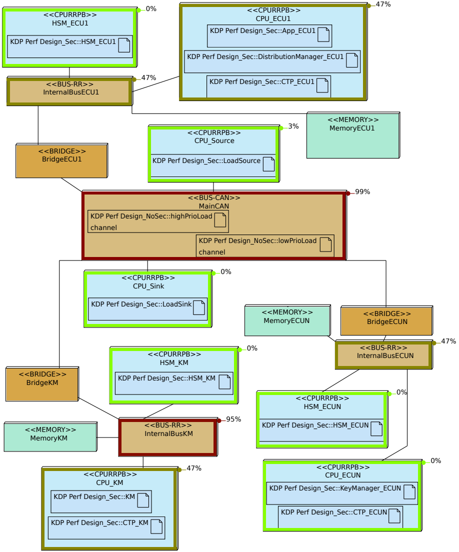


TELECOM ParisTech

Partitioning (No Security Mechanisms)



Partitioning (With Security Mechanisms)



Conclusion

Approach

- Goal-oriented security requirements engineering and attack equations integrated in SysML
- MDE approach: exploits knowledge resulting from HW/SW mapping and model transformation

Results

- Covers the whole methodological development of an embedded system: (security) requirements, attacks, partitioning, design, validation
- Software and hardware semantics
- TTool

Conclusion (Cont.)

Future directions

- Semi-formal checks: requirements consistency / attack coverage
- Combining security and safety requirements

To go further

http://ttool.telecom-paristech.fr

GraMSec'2015

- The Second International Workshop on Graphical Models for Security
- http://gramsec.uni.lu/