Meet-up 2019 | Doctorants & Industrie

Secure Optimal Architectures for Autonomous Transportation
Cyber-Physical Systems (CPS)

Jean OUDOT1, 2, 3
Laurent PAUTET2, Arvind EASWARAN3, Etienne BORDE2, Witold KLAUDEL1, 4

1IRT SystemX, Paris-Saclay, France 2LTCI, Telecom Paris, Paris-Saclay, France 3SCSE, Nanyang Technological University, Singapore 4Renault, Guyancourt, France

1. CONTEXT

Transportation CPS are:
- Safety-critical: a failure is life-threatening.
- Highly interconnected: GPS, Internet, V2X ...
- Highly automatized: autonomous cars, trains ...

Hackers can remotely threaten transportation CPS’s safety!

→ Secured architectures are needed to ensure users safety! [1]

2. OBJECTIVES

3. CONTRIBUTION

Evaluation of an attack impact on a CPS’s safety
with Dynamic Bayesian Networks

- Automated Probabilistic Risk Assessment.
- Formal model of a CPS and attacker.
- Formal model of transient vulnerabilities [2]
- Standard-based parametrization.
- Exhaustive analysis of attacks.

4. CASE STUDY: AUTONOMOUS CAR

Safety evaluation of the car’s formal model

5. RESULTS

We show that:
- Transient vulnerabilities are important.
- Architecture’s design has a huge impact.
- Choosing the right attacker is crucial.
- There is a clear safety/security interaction.

6. FUTURE WORK

- Evaluation of safety modes impact on security.
- Analysis of countermeasures impact on a system.
- Improvement of DBN scalability and efficiency [3]
- Framework for design space exploration.

REFERENCES