Handling risk in safety-critical systems

- Automotive systems, avionics systems, nuclear power plants . . .
- Digital car:
  - Security of over-the-air firmware updates, car control by malware [Koscher 2010], Autonomous vehicle safety (e.g., Google car)
  - Car navigation data spoofing [Andrea et al. 07]
- Drones:
  - Sensitive data protection and communications security and safety
  - Autonomous support system: security and safety (hijacking, secure data fusion and interpretation, fault-tolerant attitude self-control)

Our proposal for security: SysML-Sec ...

- Objective: bring together system engineers and security experts
- Model-Driven Engineering from requirements to code generation
- Centered around a security-aware HW/SW partitioning
- Formal safety and security proofs
- Free software (TTool)

Requirements

- Who and why: stakeholders and security goals

Attacks

- Who and Why: attackers, their capabilities, and objectives (risk analysis)

Application

- When: operation sequences in functions involving those assets

Architecture

- What: assets to be protected

Mapping

- Where: mapping of functions over architecture assets

System design

- How: security objectives due to architecture (e.g., network topology, process isolation, etc.)

Formal verification

- Proof based on ProVerif
- Authenticity, confidentiality
- Press-button approach from TTool

SysML-Sec: Capturing and Formally Proving Safety and Security Properties

Authors

Ludovic Apvrille (Télécom ParisTech)
Ludovic.Apvrille@telecom-paristech.fr
Yves Rouvier (EURECOM)
Tullio Joseph Tani (Télécom ParisTech)
Franck Guarnieri ( Mines ParisTech)

Partners

Institutions