Dependable Computing and Fault Tolerance Research Group

http://www.laas.fr/TSF

contact: mohamed.kaaniche@laas.fr

Team Composition

Dependable Computing and Fault Tolerance

Permanent Researchers (20)

- Mohamed Kaâniche (DR), Head.
- Guillaume Auriol (MCF)
- Eric Alata (MCF)
- Jean Arlat (DR)
- Jacques Collet (DR, emeritous)
- Alain Costes (PR, emeritous)
- Yves Crouzet (CR)
- Agnan de Bonneval (MCF)
- Jean-Charles Fabre (PR)
- Jérémie Guiochet (MCF)
- Karama Kanoun (DR)
- Marc-Olivier Killijian (DR)
- Michael Lauer (MCF)
- Vincent Nicomette (PR)
- Gilles Motet (PR)
- Nicolas Rivière (MCF)
- Matthieu Roy (CR)
- Pascale Thévenod (DR)
- Gilles Tredan (CR)
- Hélène Waeselynck (DR)

PhDs (13)

- Ulrich Matchi Aivodji
- Matthieu Amy
- Guillaume Averlant
- Joris Barrier
- Christophe Bertero
- Julien Duchêne
- William Escoffon
- Lola Masson
- Roberto Pasqua
- Jonathan Roux
- Carla Sauvanaud
- Thierry Sotiropoulos
- Rui Wang

Research Objectives and Positioning

- Context
  - Large, networked, evolving systems, interconnecting servers, mobile computers, and embedded devices to form complex information infrastructures → *ubiquitous systems*

    ⇒ Resilience: the persistence of dependability when facing changes
- Major challenges
  - Mobility
  - Evolvability and autonomy
  - Openness
  - Reactivity
- Scope of Faults
  - Physical faults
  - Development (SW and HW) faults
  - Malicious interaction faults (intrusions)

- Viewpoints
  - Architecture
  - Analysis

Research overview

Mobility

- Modeling interactions in a mobile context
- Geo-Privacy protection and assessment

Evolvability and autonomy

- Adaptive fault tolerance for resilient computing
- Safety monitoring and software testing of autonomous critical systems

Openness

- Hardware assisted protection
- Model-based intrusion detection
- Vulnerability analysis and automated security assessment
- Private Information retrieval

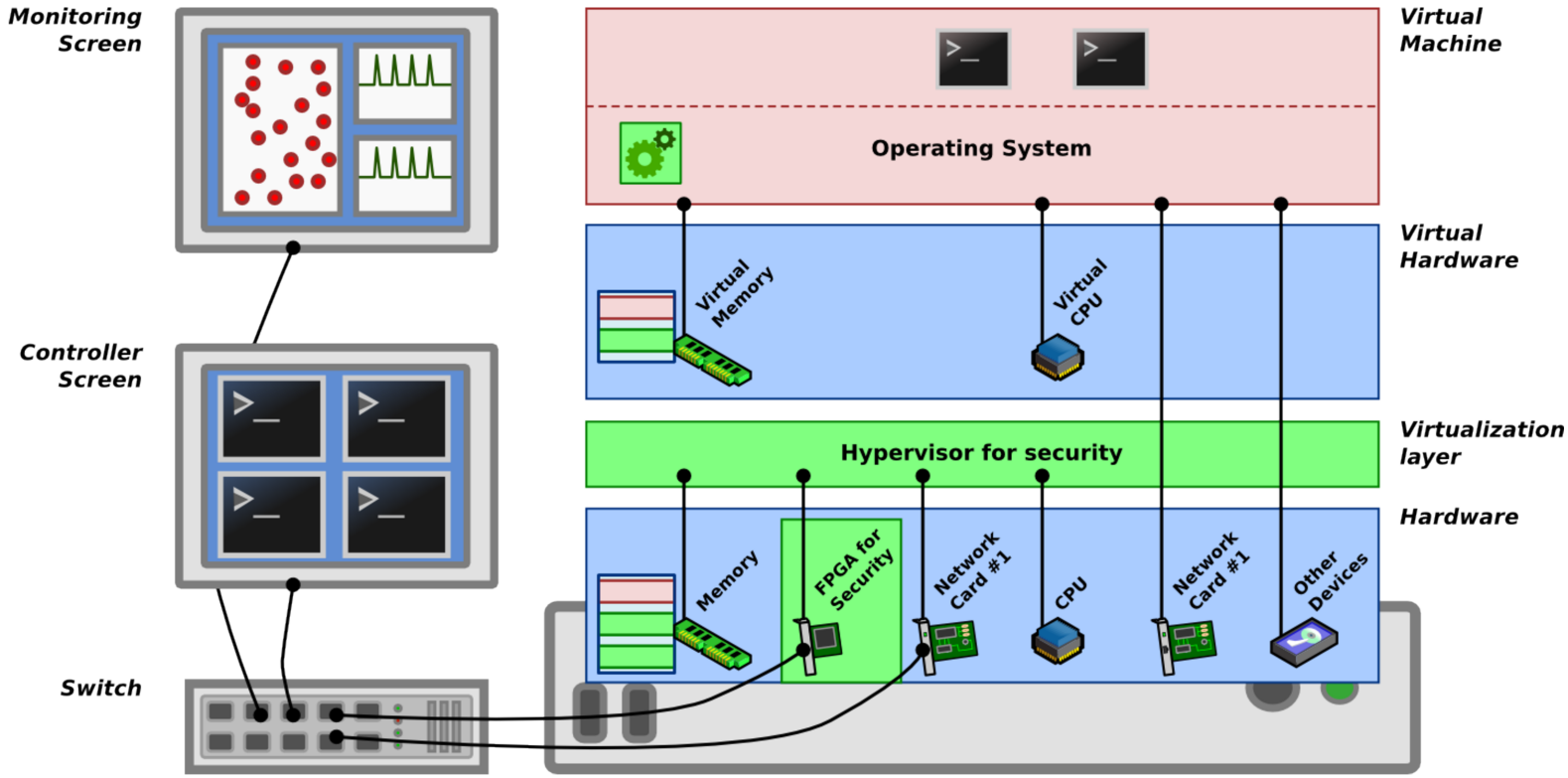
Reactivity

- Safe execution of mixed criticality systems on multicore architectures
- Monitoring and anomaly detection for virtualized infrastructures
- Integrated (SW & HW) approach for cyber-physical systems testing

Research Topics in Security

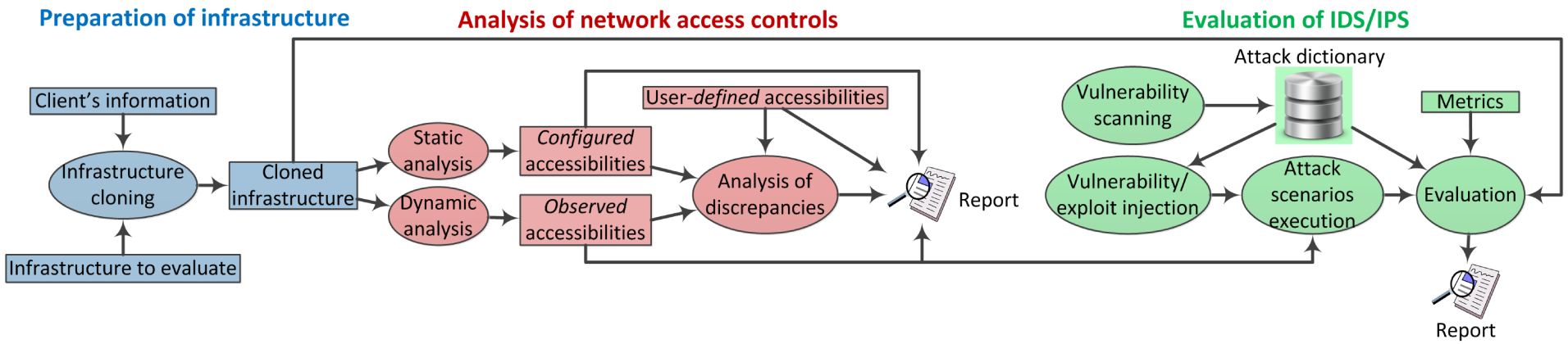
- Vulnerability assessment and protection mechanisms
  - **Operating systems (x86, ARM)**
    - Hardware assisted protection mechanisms facing Rootkit Kernels
    - I/O attacks and countermeasures
  - **Embedded systems**
    - Avionics: intrusion tolerance, vulnerability analyses of RT embedded OS
    - Automotive: model-based IDS on the CAN bus
  - **Connected smart devices (IAD, smart TVs, IoT)**
    - Experimental analyses of attack surfaces and countermeasures, low level communication protocols (Lora, Sigfox, etc.),
  - **Cloud infrastructures**
    - Secure virtualized architectures relying on Trusted hardware components
    - Automated assessment of security protection mechanisms
  - **Web applications**
    - Automated identification of injection-based vulnerabilities (SQL, …), formalization
- Privacy protection
  - Inference attacks on geolocated data
  - Geo-Privacy protection based on cryptography techniques
  - Private Information Retrieval

Trusted architecture for virtualized infrastructures protection



- **Contribution : a security hypervisor …**
  - virtualizing the VMM + Enabling detection of the VMM compromission
- **… and a dedicated trusted hardware component (FPGA board)**
  - Periodically assessing the hypervisor integrity

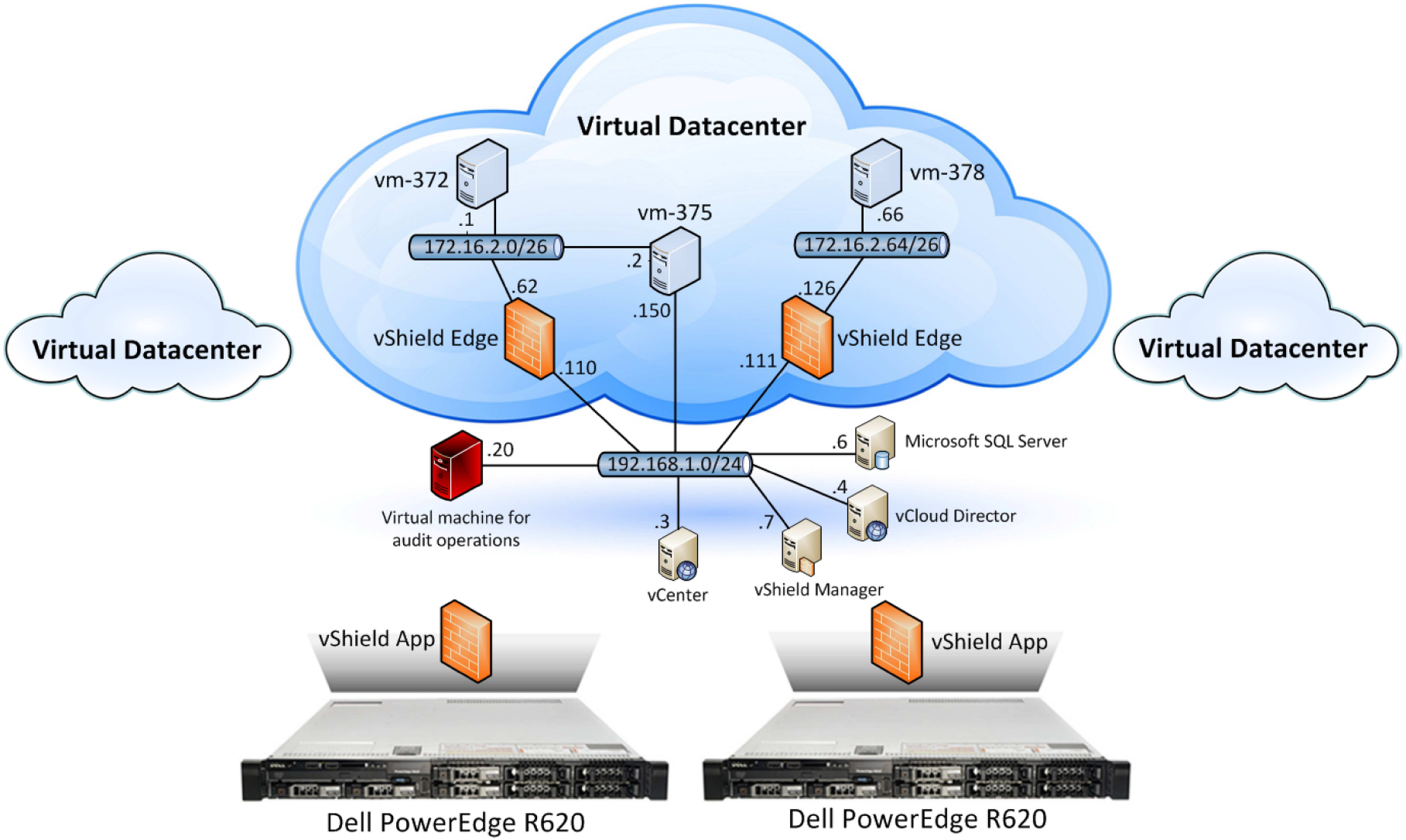
Automated assessment of cloud infrastructure security



- **Automated assessment and analysis of security mechanisms deployed in Infrastructure as a Service (IaaS) cloud environements**
  - security reports on network accessibilities and IDS/IPS performance
- **Three phase approach**
  - Retrieval of information and infrastructure cloning
  - Static and dynamic identification of accessibilities
  - Elaboration and execution of attack campaigns

SVC « Secured Virtual Infrastructure project »

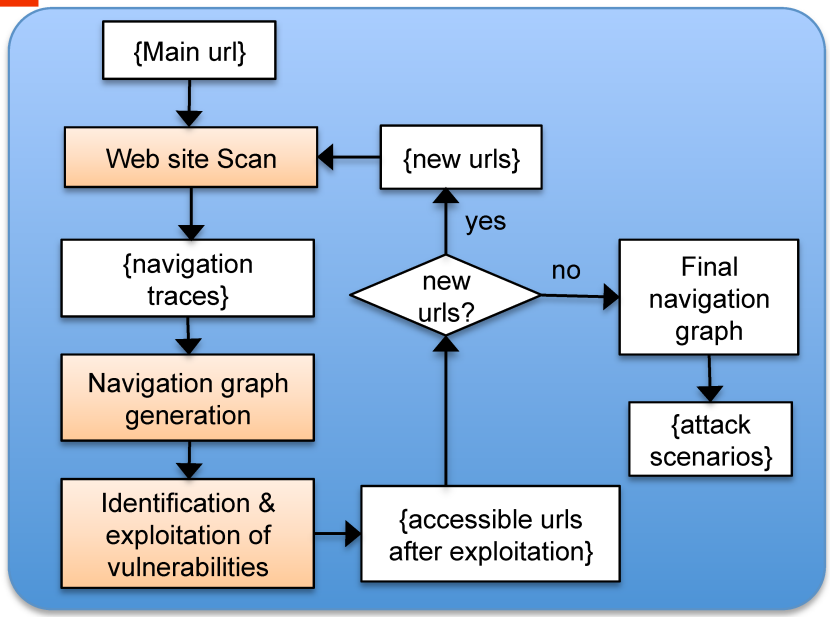
Automated assessment of cloud infrastructure security



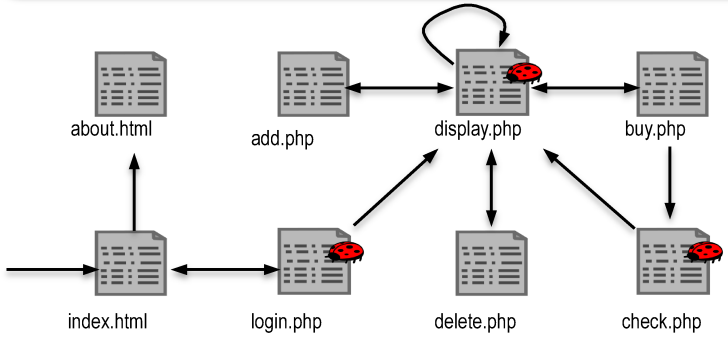
Experimental Test-bed

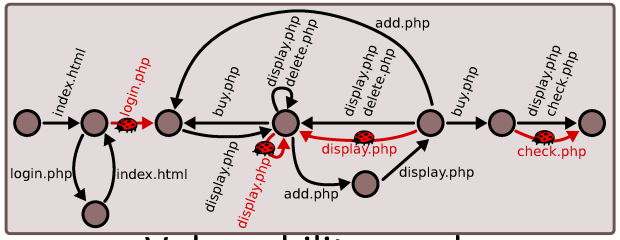
Web application security assessment

- **Objective**
  - Generation of attack scenarios
  - Identification and exploitation of injection-based vulnerabilities (SQL, …)
  - Automated experimental approaches



- **Approach**
  - Grammar for the generation of relevant inputs + web page clustering for vulnerability detection
  - Tool: Wasapy
  - DALI ANR Project

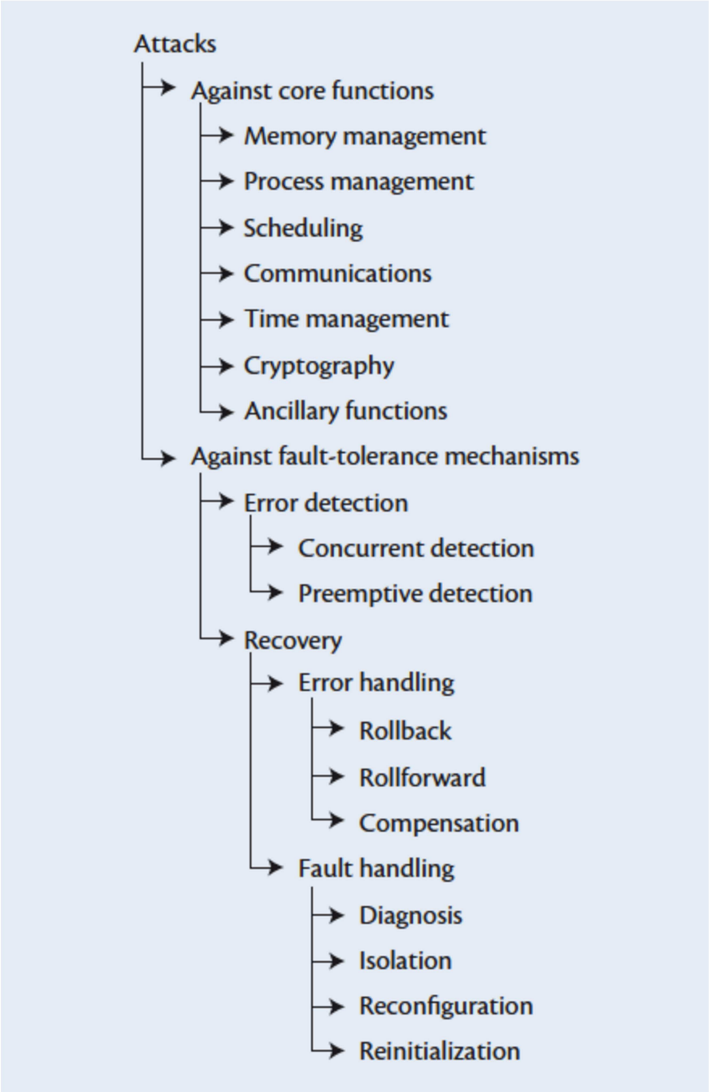




Vulnerability graph

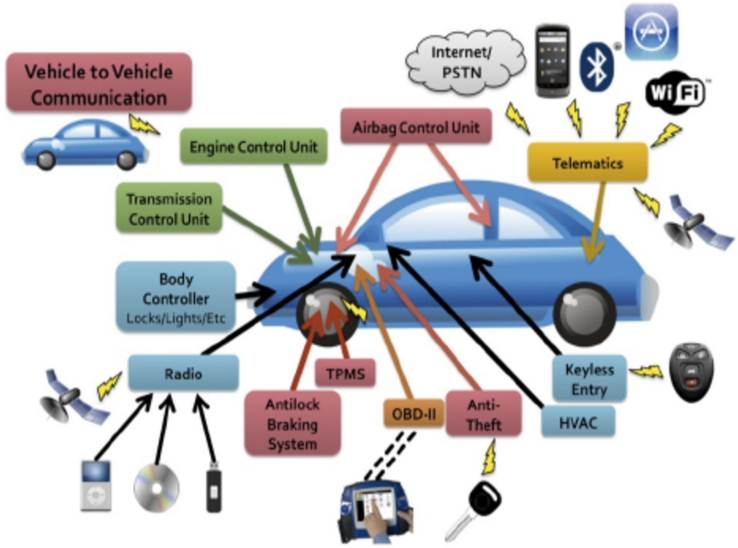
Embedded Safety-Critical Systems Security

- **Avionics**
  - Vulnerability analysis and countermeasures (SW-HW lower layers)
    - Attack Classification
      - Core Functions
      - Fault Tolerance mechanisms
    - Case Study : experimental embedded OS (P4080), minimalist, provided by Airbus.
  - ANR Project SOBAS Securing On-Board Aerospace Systems
  - PhD: Antony Dessiatnikoff

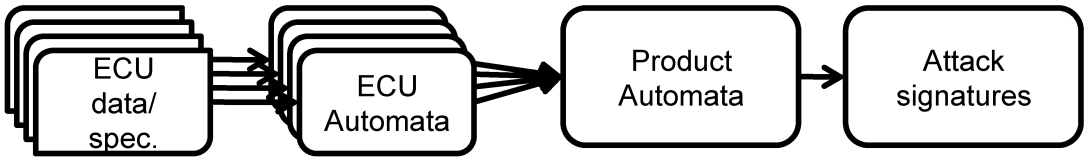


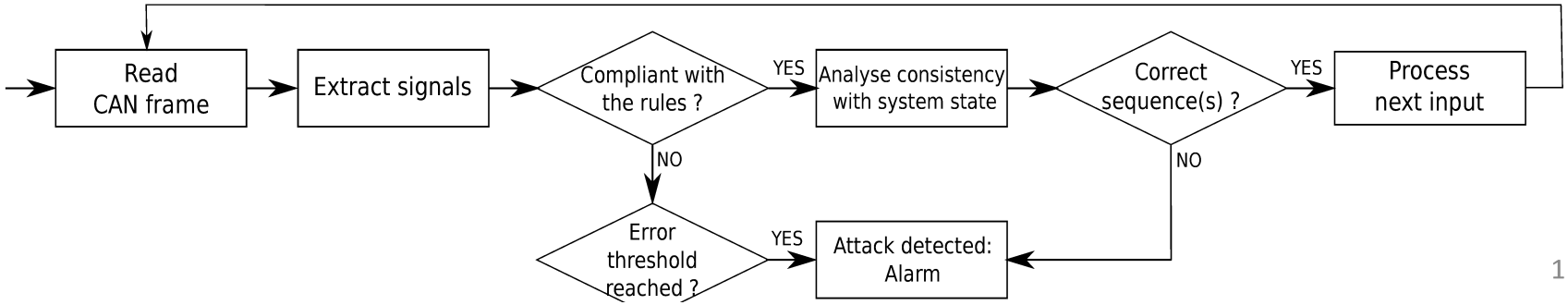
Embedded automotive networks security

- **Context**
  - Increasing connectivity (ODB port, USB port, Bluetooth, Wifi, Car2Car, etc.) and complexity
  - → Higher attack surface - Many documented attacks
- **Contributions**
  - Stateful IDS on the CAN network
    - Attack signatures derived from the compositi behavioral models of ECUs
    - Without altering ECUs architectures
  - Ivan Studnia PhD - Renault



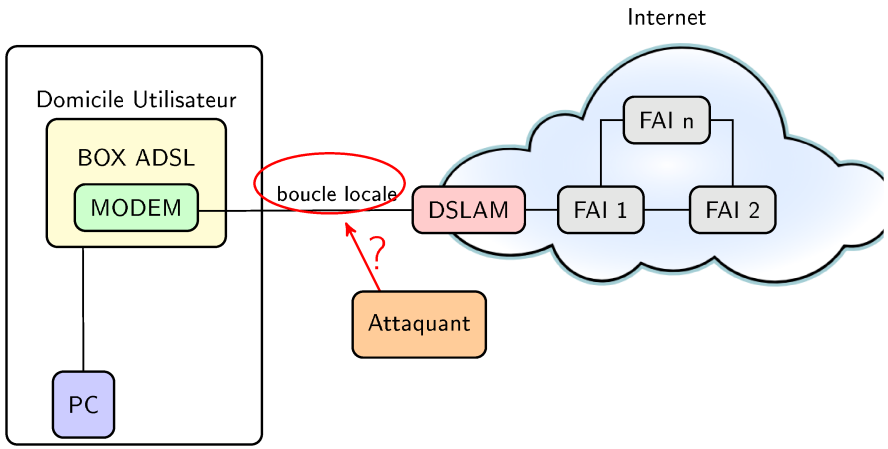
[Checkoway et al., 2011]

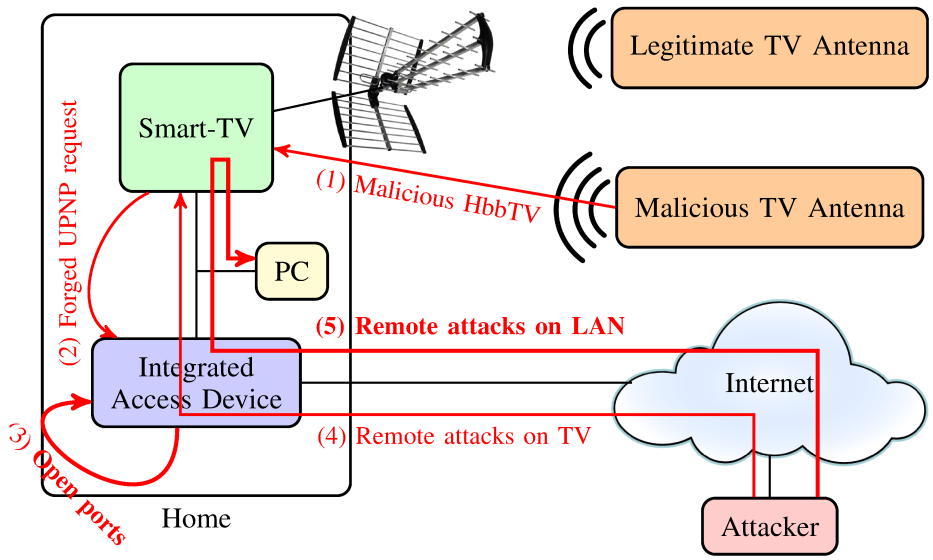




Connected smart-devices

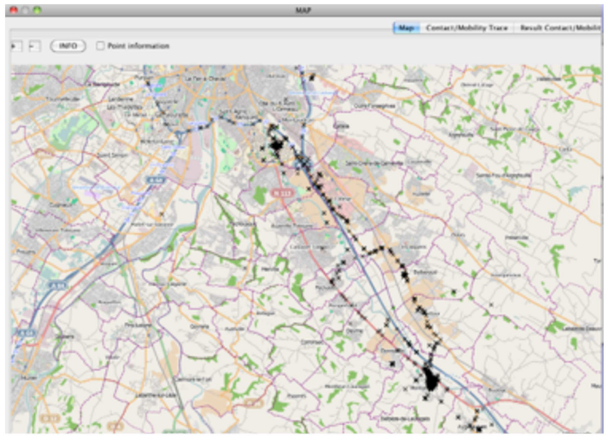
- **IADs, Smart TVs, IoT, …**
  - multiple communication interfaces, heterogeneous protocols, could be used to perform bouncing attacks
  - Vulnerability analyses and counter-measures
  - Yann Bachy PhD (Thales C&S)

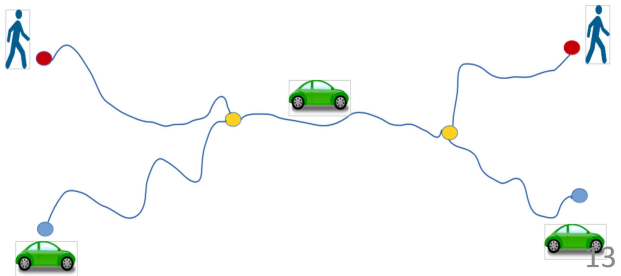




GeoPrivacy

- **Geoprivacy: Mobility + Privacy**
  - Individual location = sensitive information
- **Inference attacks on GeoLocated data**
  - Identify points of interest, predict / learn movement semantics, de-anonymize location data, discover social network,…
    - GEPETO (GEoPrivacy Enhancement Toolkit) – Cecill B
  - Infer social proximity in crowds using co-location information: SOUK
- **GeoPrivacy Protection**
  - Control dissemination of private data, favor local interactions
  - Mechanism-centered:
    - Location-based services that do not need to send location
    - Verified positioning ➨ Cryptographic techniques
  - Data-centered:
    - Sanitization ➨ produce modified location
- **Privacy-Preserving Ridesharing**
  - Based on Distributed computation to avoid single point of trust
  - Approach: Multi-model routing + Secure Multi-Party Computation





Private Information Retrieval

- A protocol allowing a user to retrieve a record from a database without revealing which to the database administrators
- Focus on PIR protocols based on cryptography (cPIR)
- Classic cPIR protocols suffer from low performance and considered as impractical
- **Contribution**
  - XPIR: a highly efficient and usable cPIR protocol using homomorphic cryptography
    - Multi-gigabit throughput on commodity CPU
    - Optimiser to automatically set up the system
  - NFLlib: open-source C++ library for Lattice-based cryptography
- **Applications**
  - Netflix database server
  - IDS: Private Sniffer
  - Genomic research