Security Architecture for Multi-Embbeded-Agent Systems

Arthur Baudet†‡, Oum-El-Kheir Aktouf†
Philippe Elbaz-Vincent‡, Annabelle Mercier†

†Laboratoire de Conception et d’Intégration des Systèmes,
‡Institut Fourier

This work is supported by the French National Research Agency in the framework of the “Investissements d’avenir” program (ANR-15-IDEX-02). Reproduction prohibited without written permission of the authors.
Outline

Multi-Embedded-Agent System (MEAS)

Security in MEAS
Multi-Embedded-Agent System (MEAS)

Security in MEAS
Agent — Definition

**Agent**
- Physical or software entity
- Autonomous (proactive or/and reactive)

**Embedded agent**
- Resources limitation
- Communication limitation
- Mobility

Wooldridge et al., Russell et al. [1, 2]
Agent — Definition

Agent
- Physical or software entity
- Autonomous (proactive or/and reactive)

Embedded agent
- Resources limitation
- Communication limitation
- Mobility

Wooldridge et al., Russell et al. [1, 2]
Multi-agent-system
- > 2 agents
- Decentralized
- Global problem divided in smaller problems
- Cooperation between agents
- Open
Multi-embedded-agent systems — Example

Simulation of a forest fires following MEAS

- **Rectangle** follows fire fronts
- **Triangle** scouts for fires
- **Star** oversees the organization (relays information)
Outline

Multi-Embedded-Agent System (MEAS)

Security in MEAS
Attack vectors

Hardware attacks
- Side-attacks
- Fault-injection

Software attacks
- Malware spreading
- Protocols abuse

Communication attacks
- Eavesdropping
- Communication tampering
- Jamming
- Routing tampering

Multi-agent attacks
- Cooperation abuse
- Sybil attack
Multi-agent attacks

Trust management system & Cryptography \rightarrow Detecting & blacklisting agents with malicious behavior.

E.g.: Ma et al., Anguraj et al. [3, 4]
Limits

- No real consideration for lower layers of security (e.g.: cryptographic requirements)
  - Not always appropriate for open and decentralized systems
    - Preloaded keys or certificates;
    - Access to a remote trusted authority.
Some possible solutions

Decentralizing Public Key Infrastructure using Blockchain (Singla et al. [5])
A blockchain stores the Certificate Authority but still weights on the system (in memory and computing power).

Decentralizing Attribute-Based Encryption using multi-authority (Okamoto et al. [6])
Agents can decide to become authority and create keys for certain attributes. Keys can be used separately to encrypt a message with attributes of multiple authorities.
A secure by design architecture

- Starting from a trust anchor;
- And ending with a strong cryptographic scheme to support MEAS defense mechanisms.
Thank you for listening!
See you in poster session


