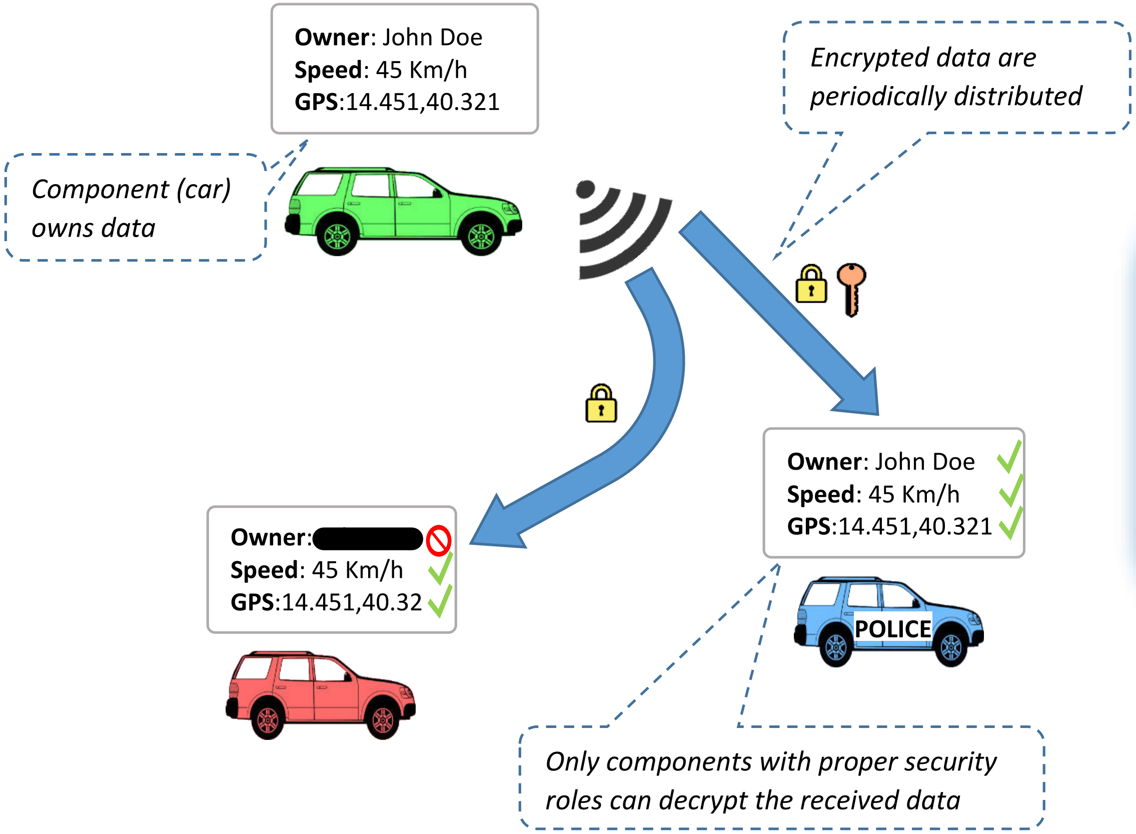
Security and Trust in the DEECo Component Model

Author: Ondřej Štumpf

Supervisor: doc. RNDr. Tomáš Bureš, Ph.D.

About Smart Cyber-Physical Systems (sCPS)

- Open-ended and dynamic distributed systems, consisting of autonomous interconnected components
- DEECo (Distributed Emergent Ensembles of Components) used as a modeling example



Owner: John Doe
Speed: 45 Km/h
GPS:14.451,40.321

Component (car) owns data

Encrypted data are periodically distributed

Owner: John Doe ✓
Speed: 45 Km/h ✓
GPS:14.451,40.321 ✓

Owner:[redacted] ⊘
Speed: 45 Km/h ✓
GPS:14.451,40.32 ✓

Only components with proper security roles can decrypt the received data

Security Issues

- How to introduce scalable access control into a purely distributed, dynamically evolving environment?
- Who should be responsible for defining the security policy, since the components do not know each other at design time?
- How to cope with encryption keys distribution?

Trust Issues

- How to prevent a malicious component from flooding the system with defective data?
- How to preserve data consistency?

PROPOSED SOLUTION

cdRBAC (Context-Dependent Role-Based Access Control)

- Security and trust dealt with together on the architecture level
- Components are assigned security roles
  - Open-endedness – any component may define a new role
  - Context-dependency – roles may be parametrized with component data
- Distributed data ratings to preserve information integrity
- Based on RBAC, Bell-LaPadula model, Clark-Wilson model, distributed ACLs

Publications

- Ondřej Štumpf, Tomáš Bureš, and Vladimír Matěna. 2015. *Security and Trust in Data Sharing Smart Cyber-Physical Systems*. In *Proceedings of the 2015 European Conference on Software Architecture Workshops* (ECSAW '15). ACM, New York, NY, USA.