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

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