Institut für Steuerungs- und Regelungssysteme
Professur für Vernetzte Sichere Automatisierungstechnik
Univ.-Prof. Dr.-Ing. Mike Barth
Fritz-Haber-Weg 1 (Geb. 30.33), 76131 Karlsruhe

Formal Modeling and Verification of Certificate Management for Modular Automation

Masterthesis

This thesis aims to formally evaluate industrial certificate management concepts.

Motivation

Formal verification has become a key tool to rigorously assess the security of industrial cyber-physical systems. At the same time, new decentralized PKI approaches are emerging to overcome single points of failure and transparency limitations of traditional CA hierarchies. In modular automation scenarios (e.g., module type package), concepts try to decouple the certificate management from a single operator PKI. This modularization promises flexibility and scalability, but it also introduces new attack surfaces and complex trust relationships that are not yet formally understood.
This thesis offers a highly topical research opportunity at the intersection of industrial security, PKI design, and formal methods. You will gain hands-on experience with state-of-the-art verification tools, contribute to more secure modular automation architectures, and explore how future decentralized PKI concepts can be applied and validated in real industrial settings.
In particular, the outcome of the thesis might influence standardization of the security aspects of the module type package.

```
let IAComponent(iacManufCertPath: certificate) =
    in(c, xCE_nonce: bitstring); (* Nonce exchange *)
    new IAC_nonce: bitstring; out(c, IAC_nonce);
    event acceptAuthIAC(xCE_nonce, IAC_nonce);
    out(c, iacManufCertPath); (* Send own manuf. cert *)
    new IAC_keyExKey: privateKeyExKey;
    out(c, signKeyEx(iacManufSecret, pkKeyExKey(
     IAC_keyExKey), xCE_nonce, IAC_nonce));
    event termAuthIAC(xCE_nonce, IAC_nonce);
    [...] (* Authenticated key agreement *)
    (* Control domain credential provisioning *)
    new iacControlDomainSecret: privateKey;
    let iacControlDomainPublicKey =
     returnPublicKeyFromPrivateKey(iacControlDomainSecret)
    event startOnboardingIAC(iacControlDomainPublicKey,
     symSessKey_enc, symSessKey_mac);
    out(c, AEAD_EtM_Enc(iacControlDomainPublicKey, [...]));
    in(c, xIACControlDomainCertificate_protected:bitstring)
     [precise];
    [...]
    if ((AEAD_EtM_Verify(
     xIACControlDomainCertificate_protected, xCEnonce_AEAD1,
      xCE_ad, symSessKey_mac) = true) && (xCEnonce_AEAD1 <>
     IACnonce_AEAD1)) then
    let xIACControlDomainCertificate = AEAD_EtM_Dec([...])
    [...] (* Receive control domain CA public key *)
    event termOnboardingIAC(xIACControlDomainCertificate).
```

Figure 1: Formal Verification

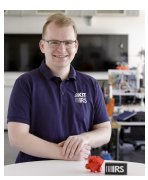
Goals

- Translate emerging concepts to formal models
- Specify and verify key properties using a tool like ProVerif or Tamarin
- Compare centralized vs. decentralized designs

Figure 2: Current Security Demonstrator

Interests and Helpful Prior Knowledge

- Basic Understanding of Industrial Automation
- Interest to get familiar with emerging security concepts



Supervisor
Marwin Madsen, M. Sc.
Build. 30.33, Room 118
Phone: 0721/608-42642
marwin.madsen@kit.edu

Thesis: Master
Date of Announcement: 24.02.2026
Tags: *Security, Industrial Control Systems, Fomal Verification*