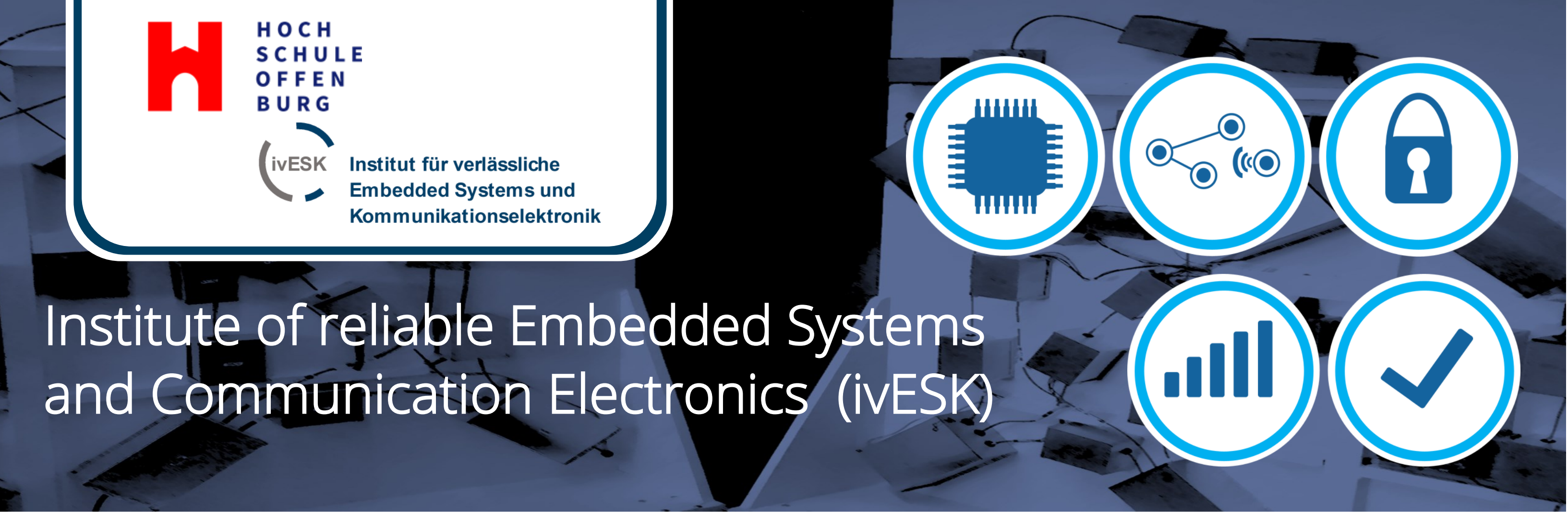
HOCHSCHULE OFFENBURG

ivESK Institut für verlässliche Embedded Systems und Kommunikationselektronik



Institute of reliable Embedded Systems and Communication Electronics (ivESK)

The Institute of reliable Embedded Systems and Communication Electronics (ivESK) at the University of Applied Sciences Offenburg designs, develops and verifies algorithms, protocols and platforms for efficient, secure and reliable wired and wireless communication systems on embedded devices. Therefore, we describe a task for the

Comparative Analysis of Certificate Revocation Mechanisms for Industrial Automation Networks

The ivESK currently works on various projects in the field of security extensions for industrial automation (IA) communication protocols. Originally, communication networks for IA were operated as separate networks with limited connectivity to the outside. However, nowadays facing the ever-growing connectivity of devices and the wish for global accessibility, also IA systems are no longer self-contained.

Required countermeasures to protect those systems often involve public-key-certificate-based authentication mechanisms. In turn, this requires the continuous management of device-granular public-key certificates in the communication endpoints.

Among other things, certificate management processes also include the revocation of certificates (e.g., prior to reselling a component, its certificate must be invalidated). However, traditional revocation mechanisms that originate from the Information Technology domain have certain characteristics which often render them unsuitable for their use in IA networks. Traditional revocation mechanisms comprise e.g., the use of certificate revocation lists (CRL), the Online Certificate Status Protocol (OCSP), OCSP Stapling, as well as short -lived certificates. Typical constraints of IA components and systems are e.g., the highly limited memory resources of devices, the lack of secure and synchronized time information within the network, or the unwanted dependency on an always online responder entity.

Therefore, the goal of this project is to develop a comparative analysis that evaluates the applicability of traditional revocation mechanisms in IA networks. Comparative properties are, for example, the consumption of persistent memory, network bandwidth, or the number of required service requests.

This project includes the following tasks:

- familiarize with IA networks and traditional revocation mechanisms
- analyze and compare the applicability of traditional revocation mechanisms in IA networks
- develop a decisioning process which revocation mechanism fits best to a concrete network and Public-Key Infrastructure (PKI) hierarchy

This task delivers and improves skills in secure communication of IA networks. Furthermore, it teaches the usage of certificate revocation mechanisms.

To successfully complete the tasks, a basic understanding of public-key infrastructures is mandatory.

Institute of Reliable Embedded Systems
and Communication Electronics (ivESK)
Offenburg University of Applied Sciences

For applications please contact:

Prof. Dr.-Ing. Axel Sikora
Dipl.-Ing. Dipl. Wirt.-Ing.
Scientific Director

axel.sikora@hs-offenburg.de
+49 (0)781 / 205 416

For questions please contact:

M. Sc. Julian Göppert
julian.goeppert@hs-offenburg.de
+49 (0)781 / 205 4957