Technische Universität München
Network Architectures and Services
Prof. Dr. Georg Carle

19.01.2012

Master Thesis / SEP / IDP

Authentication of WSN components towards each other and Data Sink using DTLS/openSSL

Motivation

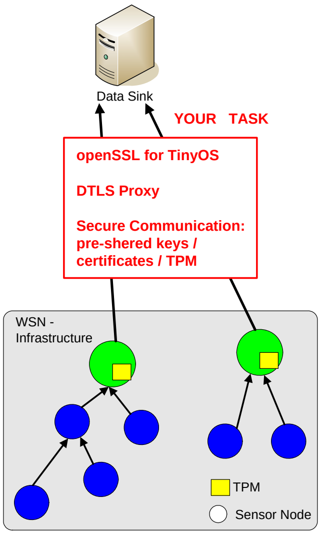
At our department we have established a Wireless Sensor Network (WSN) consisting of sensor nodes which use TinyOS as an operating system. TinyOS it self is a modular constructed. Those modules are programmed with nesC a derivate of C/C++. Our existing infrastructure uses TinyIPFIX for data transmission over BLIP.

Depending on the WSN application security during data transmission rises in the priority as well as the usage of well proofed and evaluated standards. For this task in common P2P-networks openSSL is used for authentication tasks between WSN components and data sink which is the connection to the “global world”. OpenSSL offers all functionality for secure authentication we currently require which make it very interesting for us. But the protocol itself is too powerful for our used WSN hardware with limited resources such as power, memory and computational capacities. Thus, openSSL must be flattened. To optimize the security between the WSN components itself pre-shared key mechanisms can be integrated and combined with certificate strategies.

Your task ...

… is to reduce the openSSL protocol to the features which are needed to authenticate a subscriber and a publisher via a third party in a WSN. Before starting to convert the openSSL protocol to TinyOS it must be flattened to the essential Client- and Server-functionality which is than converted to TinyOS. In a next step pre-shared key and certification mechanisms are integrated combined with the functionality of Trusted Platform Module (TPM)-hardware on one of our sensor nodes. Finally a demonstrator must be established with heterogenous hardware and deeply evaluated.

Regulated by thesis type the complexity will be attached !

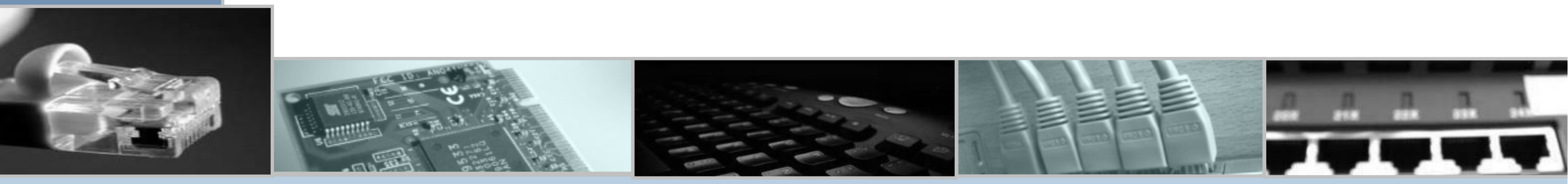


Requirements

- Basic familiarity with security concepts (DTLS, TPM, pre-shared key, certificates) and data management systems
- Knowledge of C and/or Java required, nesC and TinyOS a plus
- Integration with an existing WSN architecture

Keywords

Wireless Sensor Networks, Security, Standardization, Data Management Systems



More information provided by Corinna Schmitt
Contact: schmitt@net.in.tum.de, Room 03.05.059