A Secure Version of RaSTA

TECHNISCHE UNIVERSITÄT DARMSTADT

Bachelor/Master Thesis

Train operation is controlled centrally from so called interlockings (de: Stellwerk). An operator sets train routes on the track and communicates clearances via Signals to the train driver. Rail Safe Transport Application (RaSTA) is a transport protocol that is utilized in railway signalling to communicate commands and reports between interlocking and signals. RaSTA needs to meet certain properties required for safe train operation. Failing to meet these properties could result in the collision or derailment of trains with respective consequences. With the ubiquitous digitalization, commercial off-the-shelf protocols and products are introduced in the signalling networks and RaSTA's environment. This requires a strong security concept that protects railway signalling networks from cyberattacks and thus the safety of people and cargo.

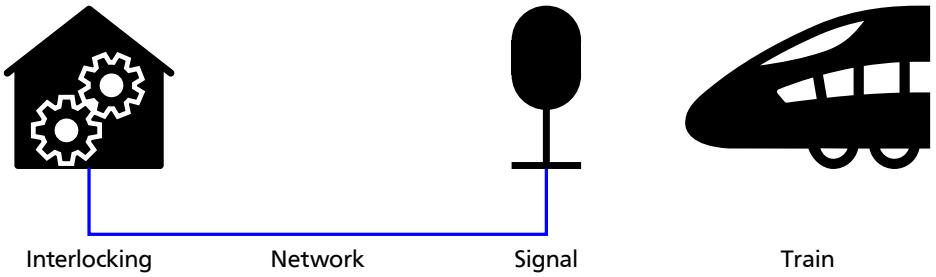

Figure 1: Architecture of a typical signalling network

Tasks

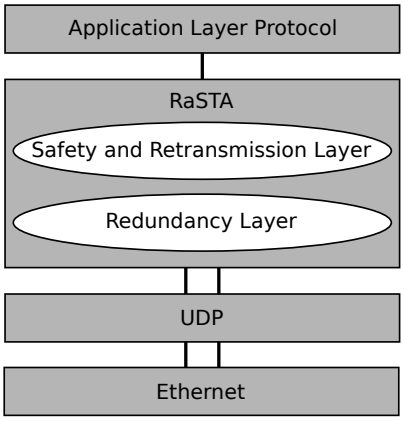

Figure 2: RaSTA in the protocol stack

Your work in this thesis is based on a security analysis of RaSTA[1]. In the analysis we showed that RaSTA's safety code (a hash over the message appended to the packet) can be transformed to a message authentication code (MAC) authenticating the messages for the receiver. You will refine the network architecture towards a practically usable system by setting up a public key infrastructure (PKI) to distribute the shared secret used for the MAC among the network entities. You will define reasonable parameters for the whole lifecycle of the certificates as well as the session keys. The lifecycle includes secure generation, distribution, storage, usage and decommission. You integrate your concept in our railway signalling lab to show its functionality. Our lab provides you with a running RaSTA implementation, written in C, a model of real railway infrastructure and an operator workstation. The RaSTA implementation needs to be adapted to securely handle session keys. The distribution of certificates and the exchange of session keys between the network entities needs to be implemented.

Requirements

- Ability to work independently and be self-driven
- Knowledge in railway signalling is an asset
- Knowledge of IT security. Specifically authentication, symmetric and asymmetric cryptography, PKI
- Experience with programming languages: preferably C, C++, Java or Python
- Language: German or English (existing work is in English)

Markus Heinrich
Security Engineering Group
heinrich@seceng.informatik.tu-darmstadt.de
www.seceng.de

February 7, 2019

[1] https://doi.org/10.1109/ISI.2018.8587371