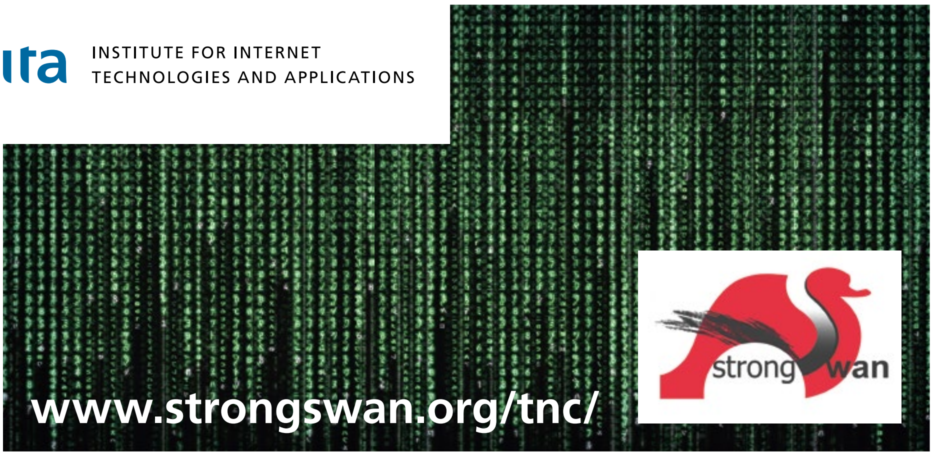
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

ita INSTITUTE FOR INTERNET
TECHNOLOGIES AND APPLICATIONS



www.strongswan.org/tnc/

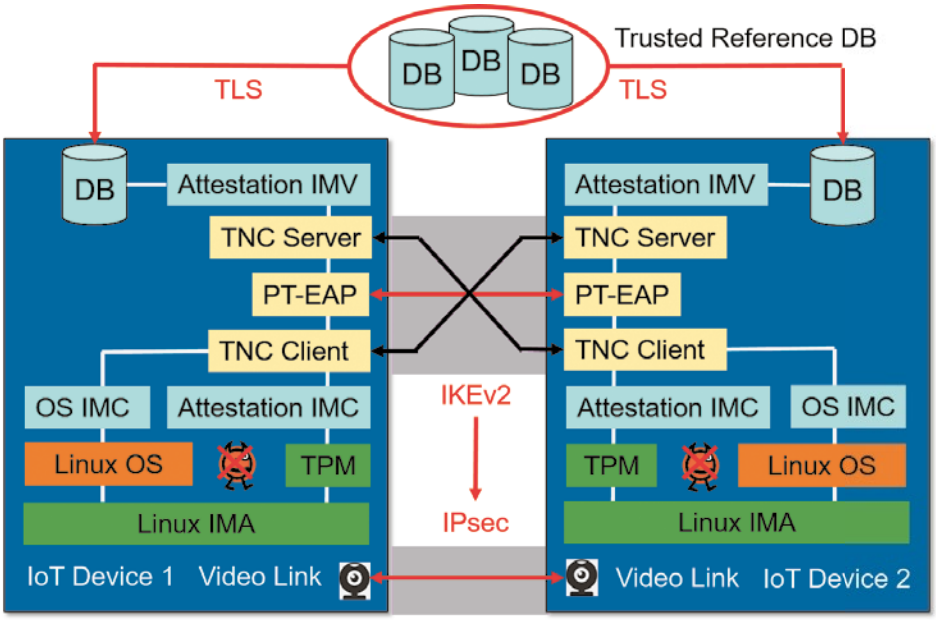
Mutual Attestation of IoT Devices via strongSwan VPN

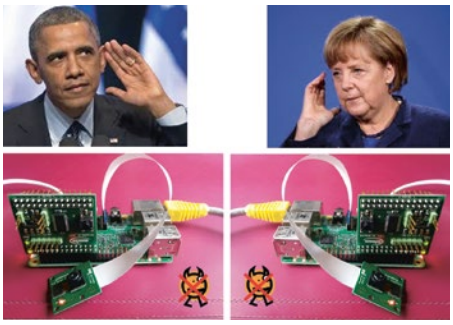
Live Demo: Mutual Attestation of Secure Video Phones

Before a pair of Raspberry Pi 2 based video phones set up a secure IPsec-protected multimedia connection, the IoT devices mutually determine the trustworthiness of their peer by attesting all system libraries and executables installed on the remote firmware platform. The SHA-256 file measurement values are exchanged using the Trusted Network Connect (TNC) protocol suite standardized by the IETF and the Trusted Computing Group (TCG). The TNC PT-EAP transport protocol is protected by an EAP-TTLS tunnel which in turn is embedded into the IKEv2 EAP authentication protocol already used for the IPsec connection setup. A tamper-proof hardware Trusted Platform Module (TPM) certifies the correctness of the measurement values by signing the final checksum with a public key bound to the TPM. This solves the «lying endpoint» problem occurring when an IoT device gets infested by root kit malware. Each IoT device compares the received measurements with reference values from a local database. This reference database is regularly updated from a trusted site in the cloud.

IPsec Software with Quantum-Resistant Cryptography

The open source strongSwan VPN software is ready for the post-quantum-computer age by offering a novel IKEv2 key exchange method based on NTRU encryption as well as authentication based on BLISS public key signatures. Both algorithms use lattices that are known to be resistant against quantum computer attacks.





SUPPORTED STANDARDS

RFC 4301 Security Architecture for the Internet Protocol (IPsec)

RFC 4303 IP Encapsulating Security Payload (ESP)

RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2)

RFC 5281 The EAP-TTLS Authentication Protocol Version 0

RFC 5792 PA-TNC: A Posture Attribute Protocol Compatible with TNC

RFC 5793 PB-TNC: A Posture Broker Protocol Compatible with TNC

RFC 6876 PT-TLS: Posture Transport Protocol over TLS

RFC 7171 PT-EAP: Posture Transport Protocol for EAP Tunnel Methods

TCG TNC IF-IMC 1.3

TCG TNC IF-IMV 1.4

TCG Attestation PTS Protocol: Binding to TNC IF-M (PA-TNC)

TCG TNC SWID Messages and Attributes for IF-M (PA-TNC)

ISO/IEC 19770-2:2015 Software Asset Management Part 2: Software Identification Tag