Diplomarbeitspräsentation

Highly Available KNX Networks

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

AUTOMATION SYSTEMS GROUP

Master- / Diplomstudium
Technische Informatik

Harald Glanzer

Technische Universität Wien
Institute of Computer Aided Automation
Automation Systems Group
Advisors: Ao.-Univ. Prof. Dr. Wolfgang Kastner
DI Dr. Lukas Krammer

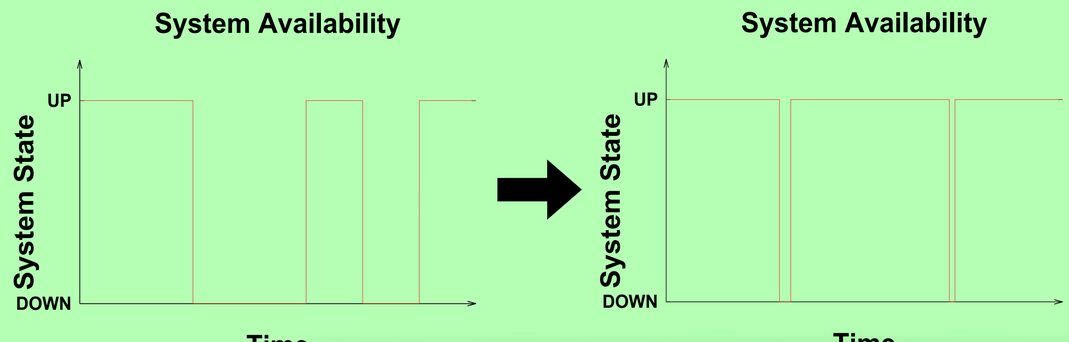
Problem and Motivation

- KNX: Home and building automation system used for services considered 'uncritical' like Heating, Ventilation and Air Conditioning (HVAC)
- Critical applications like elevation control, access control or burglar alarms are based on dedicated systems
- Idea: unify critical and uncritical systems into one system to reduce maintenance costs
- Problem: no unified concept for providing the full CIA triad AND high availability at disposal

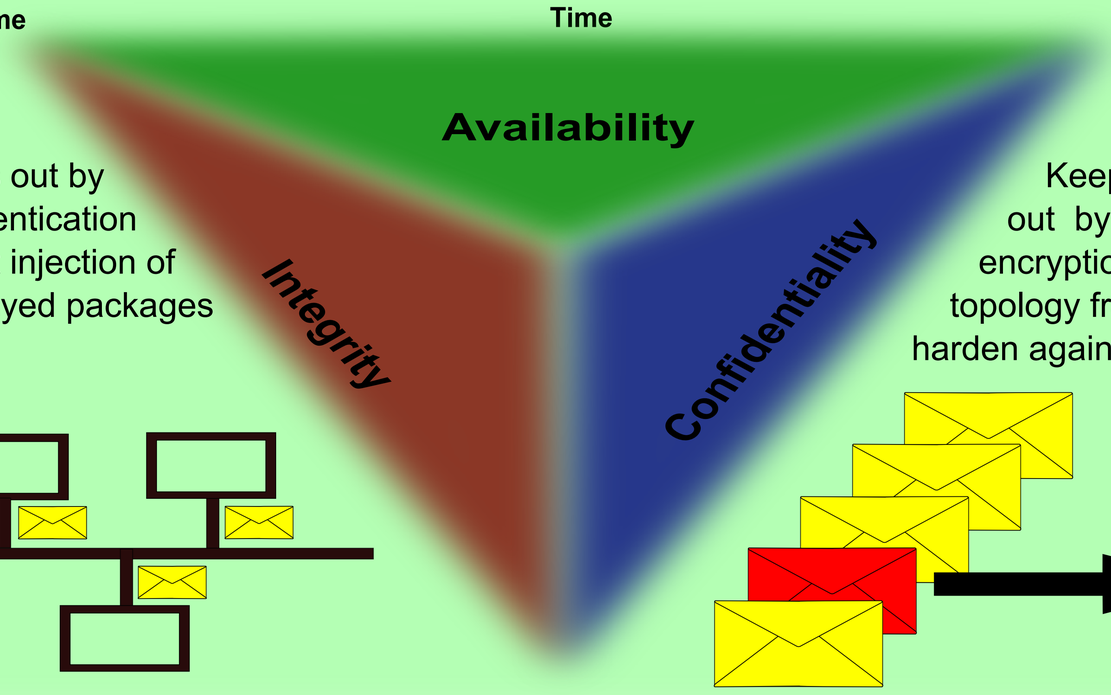
Design Goals

- Provide high-availability by utilizing independent communication lines and independent bus interfaces
- Assure confidentiality and integrity by implementing strong cryptographic mechanisms with end-to-end encryption
- Keep interoperability in mind by using 'plug-and-play' functionality
- Restrict protocol overhead
- Provide a prototype as proof-of-concept

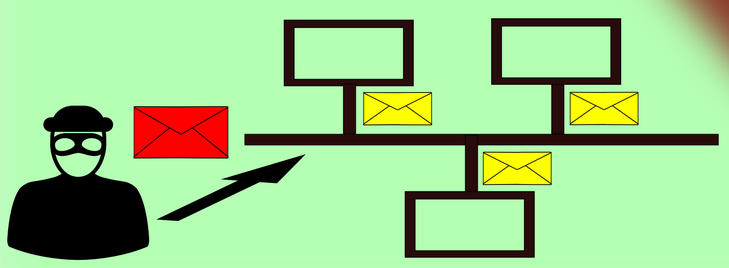
Computational Security - the 'CIA Triad'



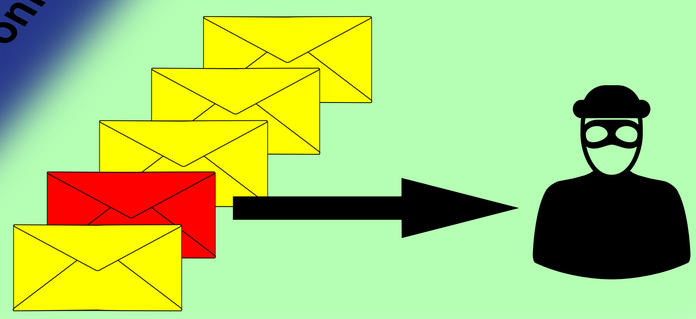
To increase availability:
- Achieve high reliability
- Keep 'mean-time-to-repair' low
- Protect network from DOS attacks
- Guard against transient hardware faults



Keep active attackers out by using message authentication codes to detect injection of arbitrary or replayed packages



Keep passive attackers out by utilizing strong encryption to hide exact topology from attacker and harden against traffic analysis

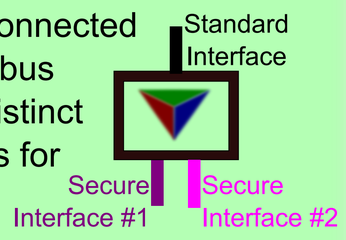


Methodology

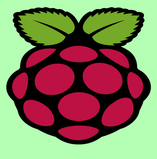
- Evaluation of different ways for fault-handling
- Analysis of state-of-the-art high-availability technogologies
- Study the KNX standard to gather fundamental insights into the protocol design - what kind of redundancy suits the KNX topology best?
- Determine what cryptographic primitives to use: weigh up level of security against overhead
- Design the basic layout of the protocol extension
- Implementation and evaluation of the prototype

Results

- Divide KNX network into 'secure' and unsecured part
- Gateway is connected to redundant bus lines with 2 distinct bus interfaces for secure part



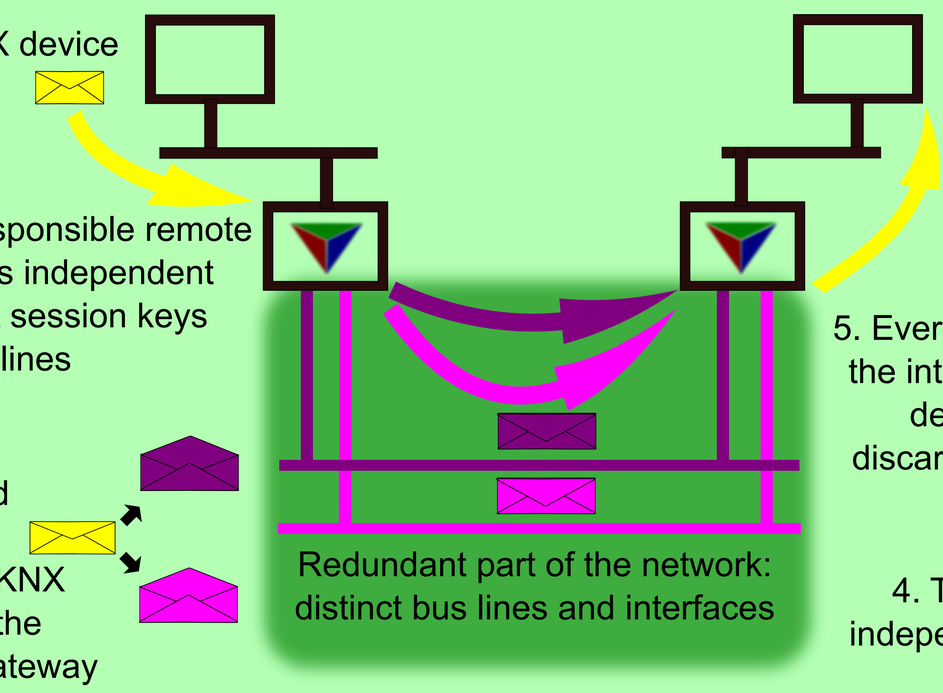
- Diffie-Hellmann Elliptic curve key negotiation with Perfect Forward Secrecy (PFS)
- Prototype network implemented on RasperryPi single board computers



- Open-source library OpenSSL for cryptographic routines

Operational Overview

1. Standard KNX device sends packet
2. Gateway determines responsible remote gateways and negotiates independent symmetric point-to-point session keys for both communication lines
3. Gateway encrypts and wraps original packet into two independent KNX packets, destined for the responsible remote gateway



4. The two packets are sent independently from each other
5. Every responsible gateway checks the integrity of the received packets, decrypts and unwraps them and discards one of them, depending on the contained counter values
6. The gateway forwards the original packet to its third interface

Contact: hglanzer@powpow.at