FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

Proposal

KNX For Safety Critical Environments

Building a Dependability Layer for the KNX Communication Protocol

Advisor: Ao.Univ.Prof.Dr. Wolfgang Kastner
Assistance: Dipl. Ing. Lukas Krammer

Department: Institute of Computer Aided Automation
Automation Systems Group

Vienna, 25.8.2014

(Signature of Author) (Signature of Advisor)

Motivation and problem statement

KNX is an open communications protocol for industrial building automation. It uses a layered structure and supports wired communication over twisted pair and power line as well wireless communication by radio or infrared transmission. Additionally, it defines gateways to the TCP/IP world. As such, it can be used for remotely controlling traditional services like HVAC, shortcut for heating, ventilation and air conditioning, but also for more sophisticated applications[1] like surveillance or fire alarm systems of buildings - ranging in size from private homes to huge office buildings.
Given these potential applications, such a communications protocol would be a weak point an adversary could exploit if there are no countermeasures deployed. Possible attacks range from DOS attacks by simply physically shortcutting a twisted line connection to replay attacks or eavesdropping, interception, altering and injecting of arbitrary telegrams. One countermeasure providing integrity, confidentiality and authenticity consists of authentication between sender and receiver of a message, and encryption of these messages, combined in a security scheme called 'Authenticated Encryption'.
Encryption uses block or stream ciphers to garble the cleartext message into a line of pseudo-random binary zeros and ones, unreadable for anyone not knowing the decryption key.
Authenticity, on the other side, takes the input data and produces a short 'MAC' (shortcut for 'message authentication code') for this data, which will be sent along with the encrypted data. This way, tampering of the sent data can be detected and the corresponding datagram will be discarded.
Availability, in general, can only be achieved by redundancy, by using replicated resources. Therefore, all resources needed for transmitting data between two points must exists redundant and independent from each other.

This work's overall topic is to provide an extension for KNX which adds an dependability layer, allowing to use KNX in a security-critical environment. As will be shown, the security concept defined in the actual KNX Standard must be regarded as insufficient because the methods for encryption used can be attacked easily.
It is important to note that this work will only handle the twisted-pair variant of KNX, although the authenticated encryption methods can be deployed in wireless networks as well.

Expected results

The final goal of this work is to build a prototype of a secure and dependable KNX network. This network will consist of 2 raspberry pi single board computers, connected to each other with 2 KNX-usb-dongles, constituting the dependable section of the KNX network. Additionally, each raspberry pi is connected by another usb dongle to another KNX network in the standard, unsecured way. Therefore, the 2 rasperry pi's are gateways between a secure and an unsecured KNX network, each of them running a master daemon responsible for reading datagrams from the KNX 'unsecured' world, encrypting them and sending them over the secured KNX lines. On the counterpart, the message will be decrypted and checked for integrity and sent on its further way if the message is found to be untampered. Additionally the daemon monitors the state of the 2 replicated KNX channels.
While it is not obvious that confidentiality cannot be achieved without authenticity and vice versa, it will be shown that one concept without its counterpart is useless. Consequently, the dependability layer will use strong encryption *and* authentication to guard against attacks.
To gain availability, a handshake protocol will be used, as well as some kind of 'heartbeat' mech-

anism to detect outages of one communication line as soon as possible, allowing to switch to the replicated line instantaneously .
While it would be possible to encrypt and authenticate only the actual payloads, and leave the status datagrams unencrypted, a cleaner and more elegant solution is to encrypt and authenticate booth message types. This makes it possible to use the concept of *divide et impera* in an uncompromising way. Additionally, attacks against the heartbeat - mechanism become impossible.

Methodological approach

The methodological approach will be broken down into these steps:

- Setup of the working environment
  As stated, rasperry pi's will be used. These are small but powerful single board computers, based on ARM processors, using a Linux kernel as operating system. A C++ KNX API named 'eibd' exists and will be used for the KNX/USB interface. When this first step is completed, a gateway from KNX to usb is available which provides a data link layer to be used by other layers.

- Literature Review
  Avoiding eavesdropping of and tampering with messages in a network is a complex and comprehensive topic. Fortunately, canonical ways how to employ authenticated encryption exists, therefore the first step is to decide which ciphers should be used, how the keys will be distributed and what kind of MAC to use.

- Design of the security layer
  This step will use the results of the literature review to properly implement the security concept found.

- Design of the dependability layer and heartbeat protocol
  The dependability layer will be built upon the security layer, consisting of the handshake protocol and an additional heartbeat protocol, signaling faulty conditions to the master daemon.

Structure of the work

1. Introduction
2. KNX
   - Specification
   - Security Concept used
   - Attacks on KNX Encryption
3. Computer Security
   - Definition of Security
   - Types of Attacks
   - Basic Concepts of Number Theory used(Fermat, Euler)
   - Basic Concepts of Propability Theory used

   - Encryption Schemes
   - Authentication Schemes
   - Authenticated Encryption
   - Distribution of Keys
   - Symmetric vs. Asymmetric Encryption
   - Actual Concept used
4. Availability
   - Handshake Protocol Used
   - Heartbeat Mechanism Used
   - Types of Datagrams
5. Codelistings

State of the art

As stated earlier, KNX already defines a method for securing datagrams, but unfortunately this method is to be considered insecure and can be attacked easily. On the other hand, some proposals which promise to fix this issue exist, nevertheless these projects didn't make it further than any theoretical level:

- 'eibsec'[2] defines a security extension to KNX which uses AES encryption and dedicated key servers
- In [3]Salvatore Cavalieri and Giovanni Cutuli propose another way how to authenticate and encrypt KNX traffic.

Instead of self-implementing the needed crypto-primitives, the use of a API like 'crypto++' or ' Keyczar' is favored because these libraries are widely used, open source, maintained and have proven to be secure in the field.

Relatedness to Computer Engineering

Modern cryptography relies heavily on number theory and probabilistic theory and is the basis of this work. To correctly implement this cryptosystem, the kernel on the target platform will be interfaced by low level programming constructs, thus combining two major topics of the academic program.

Related lectures:

- 104.271 VO Discrete Mathematics
- 104.272 UE Discrete Mathematics
- 184.189 VU Cryptography
- 182.721 VO Embedded Systems Engineering
- 182.722 LU Embedded Systems Engineering

- 389.152 VO Network Security
- 389.166 VU Signal Processing 1
- 183.624 VU Home and Building Automation

Bibliography

[1] KNX Association LaTeX: *Introducing Security and Authentication in KNX* . http://www.knx.org/fileadmin/downloads/08%20-%20KNX%20Flyers/KNX%20Solutions/KNX_Solutions_English.pdf

[2] Granzer, Kastner, Neugschwandtner LaTeX:*EIBSEC: A Security Extension to KNX*. http://www.knx.org/fileadmin/downloads/05%20-%20KNX%20Partners/03%20-%20Becoming%20a%20KNX%20Scientific%20Partner/2006-11%20Scientific%20Conference%20Papers%20Vienna/05_granzer-eibsec_security-knxsci06-website.pdf 2006.

[3] Salvatore Cavalieri, Giovanni Cutuli LaTeX: *Introducing Security and Authentication in KNX* . http://www.knx.org/fileadmin/downloads/05%20-%20KNX%20Partners/03%20-%20Becoming%20a%20KNX%20Scientific%20Partner/2008-11%20Conference/presentations/session2.pdf