FAKULTÄT FÜR !NFORMATIK

Faculty of Informatics

Proposal

Highly available KNX networks

Author: B.Sc. Harald Glanzer
Advisor: Ao.Univ.Prof. Dr. techn. Wolfgang Kastner
Assistance: Dr. techn. Lukas Krammer

Department: Institute of Computer Aided Automation
Automation Systems Group

Vienna, 25.8.2014

(Signature of Author) (Signature of Advisor)

Problem statement

KNX is an open communications protocol for Building Automation (BA). It uses a layered structure and supports wired communication over twisted pair and power line as well as wireless communication by radio transmission. Additionally, it supports communication with TCP/IP hosts by special gateways. As such, it can be used for controlling traditional services like Heating, Ventilation and Air Conditioning (HVAC), but also for more sophisticated applications like surveillance or fire alarm systems of buildings [1].

Given these potential applications, a wide range of attacks would be possible. For example, Denial of Service (DOS) attacks to disable all directly connected KNX devices can be conducted by simply physically shortcutting a line connection, rendering the corresponding network segment unavailable. Replay attacks by intercepting and replaying datagrams are also possible, allowing an adversary to introduce arbitrary KNX traffic, switching doors or disabling burglar alarms. Passive attackers can monitor the bus traffic to analyze the types of KNX devices within the network, gathering knowledge that can be used to develop further attack strategies.

Availability, in general, can only be achieved by redundancy, i.e. by using replicated resources. Therefore, all resources needed for transmitting data between two points must exist redundantly and independently from each other.

The countermeasure against eavesdropping and replay attacks, providing integrity, confidentiality and authenticity, consists of authentication between the sender and receiver of a message, and encryption of these messages, combined in a security scheme called Authenticated Encryption (AE).

The basic KNX Standard is regarded as insufficient because the standard simply doesn't provide any encryption, authentication or availability mechanisms [2]. To address the cryptographic issues, extensions are available, but no solution is disposable for improved availability with integrated security mechanisms.

Expected results

The overall goal of this work is to develop a concept for a secure and high-available KNX network that also considers interoperability and compatibility, allowing the usage in environments with increased safety-critical requirements. To achieve this, so called security gateways will be used. These gateways will possess two kinds of KNX interfaces: one kind of interface will be connected to standard, unsecured KNX networks. The second interface constitutes the entry point to a secured KNX network which is connected to the secure interfaces of other security gateways. To achieve higher availability, these secure interfaces and the respective communication lines must exist redundantly. This ensures that even in case of a DOS attack, communication within the segment is possible.

To show the feasibility of the solution by a proof of concept, a demonstration network shall be built. For the security gateways, RaspberryPis in combination with KNX-USB-dongles will be used. Therefore, the RasperryPis are acting as gateways between the secure and the insecure KNX networks, each of them running a master daemon responsible for reading datagrams from the KNX insecure world, encrypting and authenticating them and sending them over the secure KNX lines.

It is important to note that the practical part of this work will only handle the twisted-pair media of KNX (i.e. KNX TP-1), although the basic principles can be deployed in a modified manner in wireless and power-line networks as well.

A threat analysis will be conducted to prove that the system can withstand the defined attacks and is robust, i.e. that it can recover from erroneous states. This will be done by exposing the demonstration network to the various defined attacks.

Methodological approach

Every secure system will just work within some defined barriers - it is impossible to build a system that is secure under all circumstances. So, the very first step will be to define a realistic threat scenario by studying typical attacks against Building Automation Systems (BAS) [3]. Ensuring security in a network is a complex and comprehensive topic. Fortunately, canonical ways how to employ authenticated encryption exist. Therefore, the next step is to research state-of-the-art techniques in order to decide which ciphers should be used. After that, the key exchange mechanism must be defined, as well as the message format used.

Also, a reasonable concept has to be found how to guarantee high availability, considering the limited resources of standard KNX devices and the limited bandwidth of KNX TP-1.

Following the design paradigm of "divide et impera", security and availability related tasks will be implemented by two distinct layers. This design allows the modification of one layer without the need to modify the other layer.

After implementation, it is evaluated whether the demonstration network withstands the defined attacks, and whether the protocol works in practice.

State of the art

The rapid growth of electronic data processing and digital communication enforces the need for secure and available systems. Information security, consisting of the triad confidentiality, integrity and availability, tries to achieve such systems. Cryptography uses ciphers to achieve integrity and confidentiality and is also a prerequisite for availability. To improve the latter one, replication is used. A replicated service uses redundant components, providing multiple outcomes. A voter mechanism is used to determine which outcome is used.

Modern cryptography, emerged from primitive ciphers over thousands of years, is nowadays a well-studied topic. Basic properties of all cryptographic systems are the data format, the kind of keys used, the mode of operation and the maximum lifetime of the keys:

cryptographic data can be processed in the form of blocks or in the form of continuous data streams. Stream ciphers can be provable "perfect secret" in principle and can be implemented as simple as bitwise xor'ing the key and the data (i.e., the one-time pad).

Block ciphers come in 2 flavors: Pseudo Random Functions (PRF), and Pseudo Random Permutations (PRP). While the latter one is reversible, this is not true for the first one. Therefor, PRFs are only used in constructions which do not depend on a reverse function, for example "Feistel Networks". A widely used encryption standard is the Advanced Encryption Standard (AES), derived from a block cipher called "Rijndel". This construction is reversible (i.e. is a PRP) and is also called a "substitution-permutation-network", named after it's 2 basic building blocks.

Two kinds of keys are distinguished: until the introduction of public key cryptography, all ciphers were symmetric ciphers. Well known examples of asymmetric or public key ciphers are "RSA" [4] and Diffie-Helmann (DH) [5]. While DH was originally based on exponentiation, a new method based on elliptic curves has been found which can achieve the same level of security with shorter keys. Prominent protocols like TLS [6] use a mixture of symmetric and asymmetric ciphers.

The mode of operation defines how large messages of arbitrary size are processed. Modes for encryption and authentication exist, some modes can also be used for booth tasks (i.e. cipher block chaining, CBC). Additionally, this property decides the order of authenticating and encrypting the data. Depending on this ordering and what modes are used for authentication and encryption, attacks like padding oracles may be possible [7]. Correct ordering mitigates such attacks [8] and leads to a combined security scheme called Authenticated Encryption (AE) [9].

Open source, high-level APIs like OpenSSL or Crypto++ offer a wide range of authentication, encryption and key exchange modes. These libraries are widely used and actively maintained, so there is no need to reimplement these primitives.

Depending on the mode of operation and the length of the used keys, there exists an upper bound on how many messages can be sent securely without changing the key. Therefore, it must be either made sure that this number cannot be achieved in a reasonable time, or some kind of key-renegotiation has to be used, which is the task of the key management algorithm. Nevertheless, if a session key and the corresponding traffic gets known to an adversary, all the past data will be disclosed (and all future traffic if no new key is used). Protocols like Off The Record Messaging (OTR) [10] avoid this problem by using short term session keys, thus providing Perfect Forward Secrecy (PFS). This property ensures that, even if a key is known to an adversary, no future and no past messages can be decrypted (beside of one single message).

As stated earlier, KNX defines no methods for securing datagrams in the original proposal - a situation comparable to the origin IPv4 [11] standard:

IPv4, which is until today one of the basic building blocks for worldwide internet communication, suffers a serious limitation because it does not offer confidentiality and integrity on the network level. The problem was mitigated in 2 ways: one solution was the introduction of another layer - TLS - above the IPv4 layer, responsible for handling security. The second way was the design of the IPsec [12] extension, which authenticates and encrypts data sent with IPv4 by defining two security services, namely the Authentication Header (AH) to provide authenticity, and the Encapsulating Security Payload (ESP) for confidentiality. Internet Key Exchange (IKE) is used as key negotiating protocol. This way, IPsec can provide end-to-end encryption and protect the payload of higher level protocols like TCP or UDP.

For KNX, the following extensions exist:

KNX Application Note 157 specifies an optional security layer for KNX networks [13], comparable to TLS. KNX Application Note 158 improves security for KNX/IP networks [14]. EIBsec uses key servers to provide secure management and group communication and implements a proof of concept [15]. Salvatore Cavalieri and Giovanni Cutuli propose another way how to authenticate and encrypt KNX traffic [16].

Relatedness to Computer Engineering

Modern cryptography relies heavily on number theory and probabilistic theory and is the basis of this work. The practical work will be to implement the multi-threaded daemons on the RaspberryPis, written in the low-level programming language C, by using the C++ API offered by EIBD.

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
- 389.166 VU Signal Processing 1
- 183.624 VU Home and Building Automation

Bibliography

[1] KNX Association. "KNX Applications". URL: http://www.knx.org/fileadmin/downloads/08%20-%20KNX%20Flyers/KNX%20Solutions/KNX_Solutions_English.pdf.

[2] KNX Association. "System Specifications, Overview". URL: http://www.knx.org/knx-en/knx/technology/specifications/index.php.

[3] W. Granzer et al. "Security in networked building automation systems". In: *Proceedings of the IEEE International Workshop on Factory Communication Systems (WFCS)*. 2006, pp. 283–292. DOI: 10.1109/WFCS.2006.1704168.

[4] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126.

[5] W. Diffie and M.E. Hellman. "New directions in cryptography". In: *Information Theory, IEEE Transactions on* 22.6 (1976), pp. 644–654.

[6] T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. RFC 2246. RFC Editor, 1999, pp. 1–80. URL: https://www.ietf.org/rfc/rfc2246.txt.

[7] S. Vaudenay. "Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS". In: *Proceedings of In Advances in Cryptology*. Springer-Verlag, 2002, pp. 534–546.

[8] Hugo Krawczyk. *The order of encryption and authentication for protecting communications (Or: how secure is SSL?)* Cryptology ePrint Archive, Report 2001/045. http://eprint.iacr.org/. 2001.

[9] Phillip Rogaway, Mihir Bellare, and John Black. "OCB: A Block-cipher Mode of Operation for Efficient Authenticated Encryption". In: *ACM Trans. Inf. Syst. Secur.* 6.3 (Aug. 2003), pp. 365–403.

[10] N. Borisov, I. Goldberg, and E. Brewer. "Off-the-record Communication, or, Why Not to Use PGP". In: *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*. Washington DC, USA: ACM, 2004, pp. 77–84.

[11] J. Postel. *INTERNET PROTOCOL*. RFC 791. RFC Editor, 1981, pp. 1–44. URL: https://tools.ietf.org/html/rfc791.

[12] S. Kent and K. Seo. *Security Architecture for the Internet Protocol*. RFC 4301. RFC Editor, 2005, pp. 1–101. URL: http://tools.ietf.org/html/rfc4301.

[13] KNX Association. *Application Note 158 – KNX Data Security*. Status: Draft Proposal. May 2013.

[14] KNX Association. *Application Note 159 – KNXnet/IP Secure*. Status: Draft Proposal. May 2013.

[15] Lukas Krammer et al. "Security Erweiterung fuer den KNX Standard". In: *Tagungsband – innosecure 2013 – Kongress mit Ausstellung fuer Innovationen in den Sicherheitstechnologien Velbert Heiligenhaus*. german. 2013, pp. 31–39.

[16] S. Cavalieri and G. Cutuli. "Implementing encryption and authentication in KNX using Diffie-Hellman and AES algorithms". In: *Industrial Electronics, 2009. IECON '09. 35th Annual Conference of IEEE*. 2009, pp. 2459–2464.