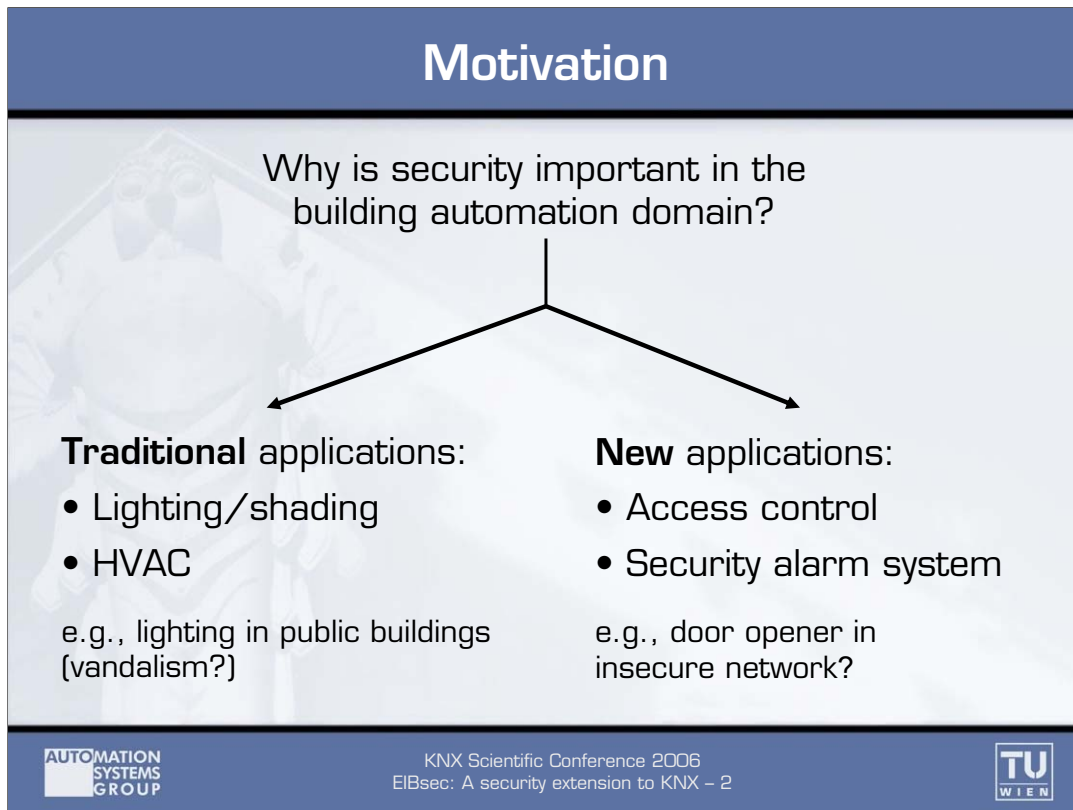


### Abstract

The core application area of KNX is environmental control with the traditional service types lighting/shading and Heating, Ventilation and Air conditioning (HVAC). Extending KNX towards new application areas leads to increasing demands. This is especially true for the integration of applications from the security domain (e.g., access control and security alarm systems). They require the underlying control system to be reliable and robust against malicious manipulations (security attacks) to fulfil their purpose.

For this reason, it is necessary to protect the exchanged process data (secure group communication) as well as prevent unauthorized use of the management services which are used for configuration and maintenance purposes (secure management communication).

Since KNX was not designed for use in security critical environments, a security extension to KNX called EIBsec has been developed. EIBsec supports mechanisms to guarantee data confidentiality, integrity and freshness as well as an authentication service. Relevant configuration related issues such as key management and distribution are also addressed. An important feature of EIBsec is compatibility to standard KNX technology.



When talking about security in building automation systems (BAS), it is important to discuss why protection against security attacks is strictly necessary. On the one hand, integrating security mechanisms will improve already existing installations. As will be shown later, traditional applications (i.e., the control of lighting/shading and Heating, Ventilation and Air Conditioning (HVAC) systems) are not protected against security attacks. Nevertheless, a protection of these service types is desirable since a security attack may have significant economic impact. Consider, for example, a company wide attack on the lighting system. The economic impact of such a vandalism act can be compared to attacking the web server. Therefore, it seems reasonable to protect these systems against such vandalism attacks – just as it is already standard in the IT domain.

On the other hand, a secure BAS will be able to cover an extended application area. Up to now, security critical applications like access control and security alarm systems were implemented by stand-alone systems with no or only limited interaction with the BAS. Using a secure BAS, these security critical applications can also be provided. Thus, it will be possible to replace the multiple stand-alone systems of today by a single, unified system.

## Benefits of a secure KNX protocol

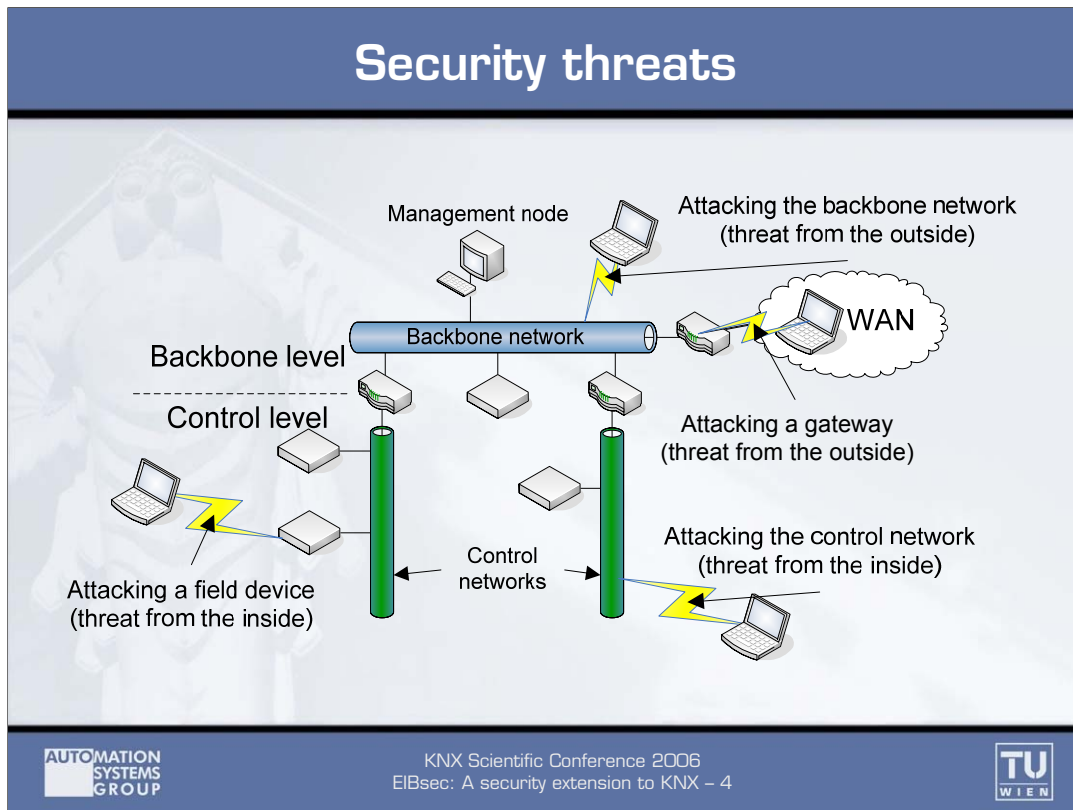
- Improve security in core domain
  - Even with wireless communication
- Extending the application area
  - Security critical applications
- Tighter integration → “All-in-One System”
  - Global configuration and maintenance
  - Cost reductions (single network)
- Head start over competing technologies
  - KNX will be secure
  - LonWorks and BACnet are not

The integration of security mechanisms into KNX has a lot of benefits. Already existing installations will be improved since a secure variant of the KNX protocol will provide protection against security attacks (e.g., vandalism). Once the communication protocol provides protection against unauthorized network access, system security no longer depends on physical isolation of the installation. Thus, wireless technologies can easily be integrated without compromising the security of the overall system.

Another benefit of a secure KNX protocol will be an extended range of applications. KNX will no longer be limited to the lighting and HVAC domains. Security critical applications like access control and security alarm systems could also be provided by KNX systems.

Thus, the integration of security concepts into the KNX protocol will provide the opportunity to use KNX as an “All-in-One system”. Management of such a tightly integrated system becomes easier since a variety of different management solutions can be replaced by a single tool. Furthermore, installation costs will be reduced since only a single network is needed.

As will be shown later, other solutions do not implement sophisticated security mechanisms yet. Therefore, securing KNX will strengthen its market position with respect to competing system technologies.



Obviously, providing a secure BAS increases the demands on the system design. This is especially true for networked BAS where protection of the underlying network against security attacks is a key challenge. To be able to identify these security demands, the opportunities to compromise the security must be investigated (security threats).

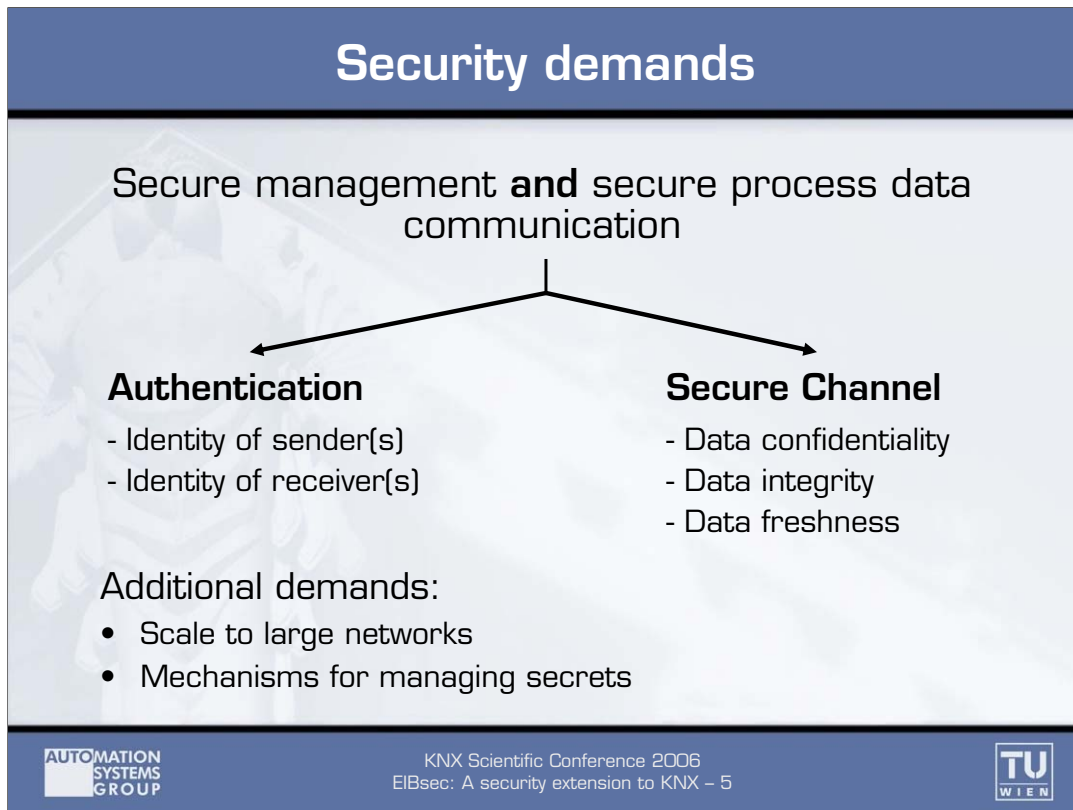
The security threats analysis shown here is based on a two-tier model. The control level consists of control networks containing intelligent sensors and actuators. The backbone network interconnects multiple control networks as well as possible foreign networks (e.g., the Internet). Additionally, the backbone level is also home to management nodes (e.g., logging server).

To guarantee the security of a BAS, the control level as well as the backbone level must be protected against security attacks. This includes protection against attacks from public networks (threats from the outside) as well as protection against local attacks (threats from the inside).

In both scenarios, an attacker has two possibilities. First, he can try to manipulate the network traffic by attacking the network medium. Secondly, he can directly gain unauthorized access to physical devices.

Protecting IP based backbones as well as IP gateways can be achieved by using well-established schemes from the IT world (e.g., SSL/TLS or VPN). However, due to resource limitations (e.g., processing power and memory capacity of field devices) deploying these security mechanisms at the control level is not possible.

Up to now, this problem has been “solved” by physically isolating the control level. It is obvious that such an isolation cannot provide effective protection, since an attacker who has gained physical access to the control network medium has full access to the whole system. Furthermore, an effective isolation is not easy to achieve (e.g., public buildings), sometimes even impossible. In order to deal with these restrictions, new security schemes which are applicable to the control level have to be developed.



To provide effective protection against the security threats shown, a malicious manipulation of the exchanged process data (i.e., sensor data and actuator commands) as well as unauthorized use of management services (e.g., changing configuration parameters) must be avoided.

To secure both types of communication, two essential elements are necessary. First, an authentication services is required to verify the identities of the involved communication partners. This is important for both sender(s) and receiver(s) since it must be verified whether the receiving nodes are authorized to receive the request as well as it must be proven whether the request originates from the correct sender(s). Furthermore, stealing or faking of identities must be avoided.

Second, the transmission of data must be protected using a secure transmission channel. The main objective of such a channel is to provide data confidentiality (i.e., unwanted disclosure of confidential data must be avoided), data integrity (i.e., unauthorized manipulation must be avoided) and data freshness (i.e., the data must be valid at the current point in time to prevent replay attacks).

Since BAS may consist of hundreds or even thousands of devices, good scalability of the implemented services is strictly necessary. Especially managing the necessary secrets (e.g., cryptographic keys) is not a trivial task in large networks. Moreover, special attention has to be paid to security threats which cannot be handled using cryptographic methods (e.g., software bugs, Denial-of-Service attacks, and the protection of field devices against physical tampering).

## Security in open standards

	Authentication	Integrity	Confidentiality	Freshness
<b>KNX</b>	32 Bit Password	—	—	—
<b>LonWorks</b>	64 Bit MAC (48 Bit Key)	64 Bit MAC (48 Bit Key)	—	Random Number
<b>BACnet</b>	DES	DES	DES	Random Number

**Sources:**

Schwaiger, Treytl, "Smart Card Based Security for Fieldbus Systems", ETFA 2003.  
 Holmberg, "BACnet Wide Area Network Security Threat Assessment", NIST, 2003.  
 Granzer, "Security in Networked Building Automation Systems", Master's thesis, 2005.

KNX Scientific Conference 2006  
EIBsec: A security extension to KNX – 6

As a next step, the security aspects of KNX as well as of LonWorks and BACnet were analyzed [Granzer, 2005]. KNX was not designed for the use in security critical environments. In KNX, only an access protection mechanism is available which is used to avoid unauthorized access to management services on BCU 2. Since clear text passwords are used, this mechanism provides only limited security.

The suitability of LonWorks for security critical applications is also limited. LonWorks supports a four-step challenge-response mechanism to prove the identity of the sender as well as provide data integrity and data freshness. The mechanism is based on a hash function which is used to calculate a 64 Bit MAC (Message Authentication Code) using a 48 bit secret key. Due to the short key length, this hash function must be assumed as being weak. Furthermore, the disclosure of confidential data cannot be avoided and the protocol itself suffers several security flaws [Schwaiger, Treytl, 2003].

The security features of BACnet are more advanced. BACnet provides an authentication service as well as services for guaranteeing data confidentiality, integrity and freshness. To provide these services, BACnet uses the symmetric encryption algorithm DES. Managing the required secrets is done by a central key server. Since DES is not secure anymore and the protocol itself is vulnerable to several security attacks, the security mechanisms of BACnet must be improved to be suitable for security critical environments [Holmberg, 2003].

None of the available standards thus satisfies the demands of security critical applications. To be suitable for security critical environments, the available solutions must be improved. Therefore, we decided to develop a security extension to KNX called EIBsec.

## Security extension to KNX: EIBsec

- Authentication and secure channel
  - Both for group communication and unicast connections
  - Authentication of all group members
- Sophisticated key management
  - Generation and distribution of required keys
  - Key revocation and lifetime limitation
  - Key forwarding
  - Management of group membership
  - Guidelines for initial key distribution
- Compatibility to standard KNX

The main goal of EIBsec is to protect the control network against local attacks. To guarantee secure data transmission, an authentication service as well as services for providing a secure channel are supported. The authentication mechanism allows to verify the identities of the involved communication partners including all receivers and senders. After having proved the identities of the involved devices, the data are transmitted through a secure channel which guarantees data confidentiality, integrity and freshness. The main advantage of EIBsec is that management services as well as the exchange of group messages can be secured.

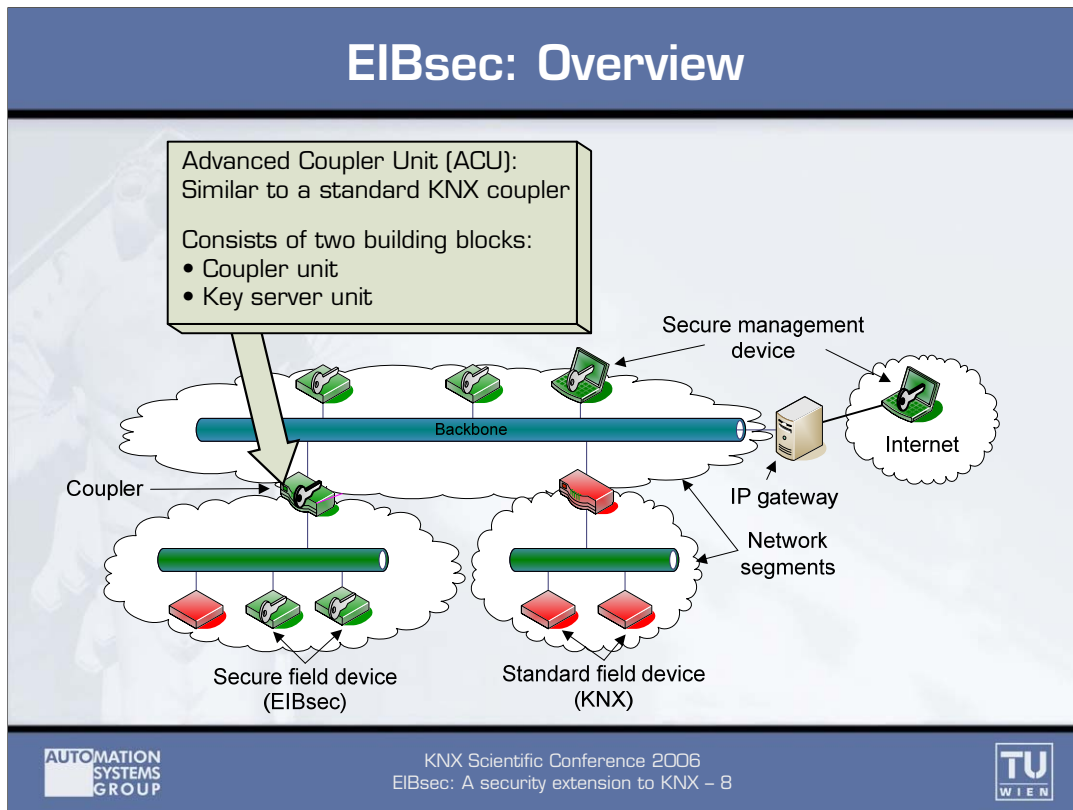
Besides these basic security services, a sophisticated key management is also provided. Using the supported key management services, the required secret keys can be generated and distributed in a secure manner. To be able to revoke insecure keys (e.g., when a device of a communication group has been compromised), the revocation of compromised keys as well as a regeneration of a new one can be initiated. Using this revocation service, it is also possible to limit the lifetime of the used secret keys.

As shown later, the key management services are implemented by several key servers. Each key server is responsible for a dedicated subset of secret keys. To be able to exchange secret keys between different key servers, appropriate key forwarding is also possible in EIBsec.

Another benefit of key management in EIBsec is that it is possible to maintain the membership of communication groups. Since all group messages are encrypted in EIBsec, sending and receiving of a group messages is only possible if the group members are sharing the same group key. Therefore, the key servers are able to control membership in communication groups by simply allowing or denying the group key retrieval.

To be able to communicate with the corresponding key server in a secure manner, each device must share a secret key with its key server (initial secret key). Since these initial secret keys must be distributed in a secure environment, EIBsec also defines guidelines for a secure initial key distribution.

Another important benefit of EIBsec is that it is downward compatible to standard KNX. The EIBsec frame format allows standard KNX devices to route secure messages. Since it is thus possible to use EIBsec and standard KNX devices simultaneously, without mutual interference, it is not necessary to replace already existing installations.



A KNX network is divided into different network segments which can be arranged in a three-level hierarchy. To interconnect these network segments, couplers are used. In EIBsec, the functionality of the EIBsec specific components is distributed across these couplers. Due to this additional functionality, they are called Advanced Coupler Units (ACU). Since couplers are already necessary in KNX networks as soon as more than one network segment is used, EIBsec does not require additional system components in most cases.

Compared to a standard KNX coupler, an ACU must perform additional tasks. Therefore, each ACU consists of two different building blocks:

- Coupler unit: This unit is responsible for routing the network traffic. It implements the functionality of a standard KNX coupler.
- Key management unit: This unit provides the necessary key management services like key generation and distribution, key revocation and key lifetime limitation.

In EIBsec, each ACU is responsible for maintaining the secret key of its network segment. If a device wants to retrieve a secret key, it must request it from the ACU which is responsible for its network segment. Due to this distributed approach, a single point of failure is avoided. If an ACU is successfully attacked or fails, only a single network segment will be affected.

Another benefit is that this approach can help to minimize the consequences of Denial-of-Service (DoS) attacks. If the ACU detects a DoS attack in its network segment, it can try to isolate the affected segment and block the attacker from accessing the rest of the network.

## EIBsec: Secure Communication

- AES 128 encryption
- Based on Secure Network Encryption Protocol (SNEP) and Secure EIB (SEIB) protocol

**Normal Mode**

6	7	8	...	21
TCF	ACF	User data		

ACF: Application Control Field  
TCF: Transport Control Field

**Counter Mode**

6	7	8	...	17	18	...	21
TCF	ACF	User data			CRC signature		

Counter → ⊕

**Sources:**  
 Perrig, Szewczyk, Tygar, Wen, Culler, "SNEP", MobiCom 2001  
 Westermeir, Werthschulte, Schneider, "SEIB", EIB Event 2001

**AUTOMATION  
SYSTEMS  
GROUP**

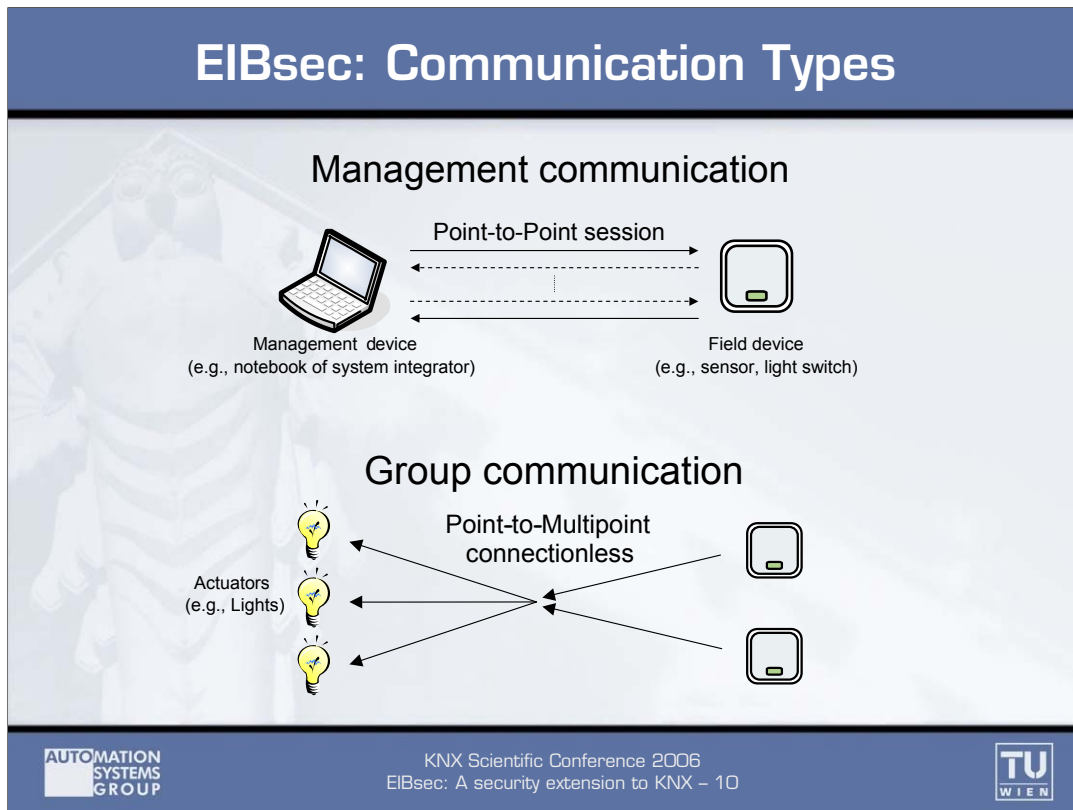
KNX Scientific Conference 2006  
EIBsec: A security extension to KNX – 9

**TU  
WIEN**

To be able to provide a secure channel, an encryption algorithm is necessary. Due to the limited processing power and memory capacity of the used embedded microcontrollers, asymmetric algorithms cannot be used. Therefore, a symmetric algorithm must be chosen. Since DES is not secure anymore, EIBsec uses the Advanced Encryption Standard (AES).

In EIBsec, two different encryption modes are available. The first mode, called normal mode, is used during session establishment and group key retrieval. In normal mode, only encryption of the user data is performed. This means that the service using this mode is itself responsible for guaranteeing data integrity and data freshness (e.g., by adding a counter and a Message Authentication Code (MAC)). Therefore, all 14 octets of user data are available in this mode.

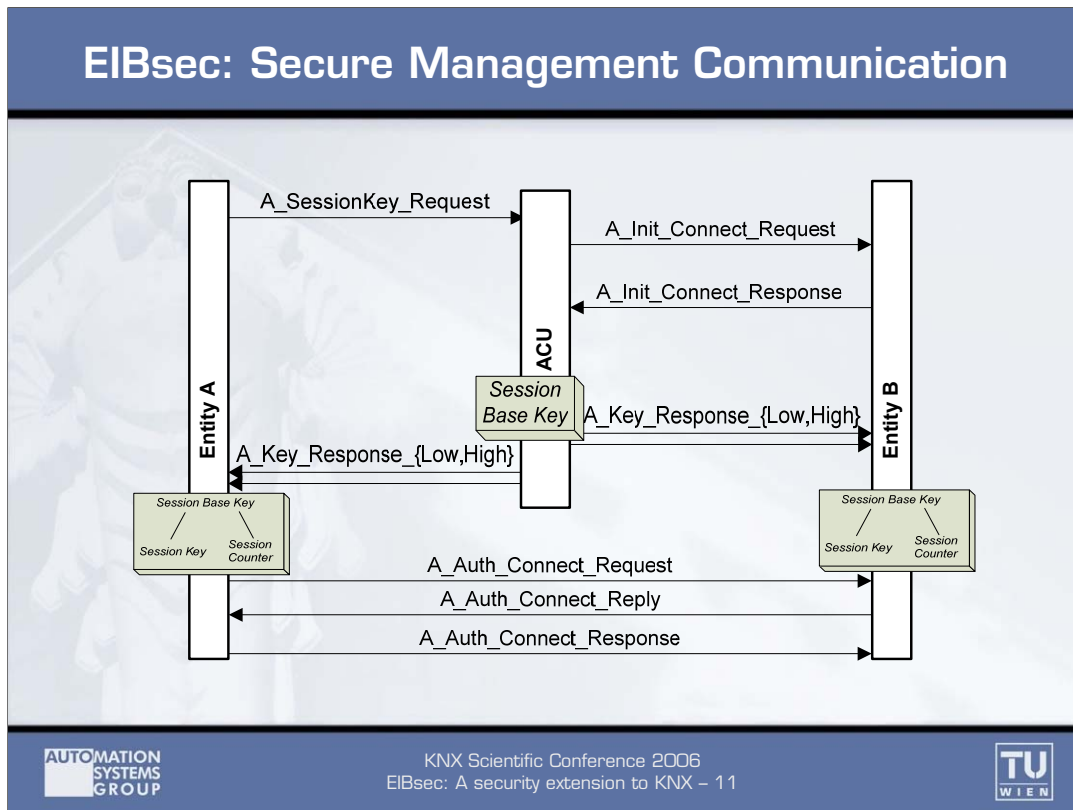
The second mode, called counter mode, is used for transmitting management (unicast) and process (group) data once the secure channel is established. It is based on the Secure Network Encryption Protocol [Perrig, 2001] and Secure EIB [Westermeir, 2001]. To guarantee data freshness, a 128 bit counter is used. Since this counter is XOR-ed to the message and encrypted afterwards, it can be guaranteed that two messages with the same user data are always different. Due to the fact that the counter is long enough to guarantee uniqueness, the use of this counter prevents replay attacks. To avoid unauthorized modification of the message, a 32 bit CRC checksum is added to the user data. Obviously, a CRC checksum does not fulfill the demands of a cryptographic hash function. However, since the checksum is encrypted together with the user data, the bits are scrambled in a way that an attacker cannot modify the message without forcing a CRC mismatch. Therefore, this form of "CRC signature" can be used to provide data integrity. Since 4 octets are used by this signature, only 10 octets are available for user data in counter mode.



In control networks, two different types of communication exist. To perform configuration and maintenance tasks (e.g., downloading user applications, changing properties), management services are invoked on the target devices. For this type of communication (called management communication) only point-to-point sessions are useful in the majority of cases. As an example, consider a management device operated by a system integrator (e.g., a notebook with a management software tool) wants to configure a field device (e.g., light switch). To achieve this, the management device establishes a point-to-point connection to the field device. After having performed the desired management tasks, the session, i.e., the point-to-point connection is closed and the field device can resume its normal operation.

In KNX, process data are exchanged in communication groups exclusively. Multiple senders are able to send process data to multiple receivers according to a producer-consumer scheme based on message identifiers where senders and receivers are not aware of each other. Since multiple senders are allowed in a single group, group communication can be seen as multiple point-to-multipoint communication.

To protect both types of communication, the authenticity of the communication partners' identities has to be guaranteed and a secure channel to transmit the relevant data has to be set up. To achieve this, the ACU of the corresponding network segment verifies the identities of the involved communication partners. Depending on the communication type, a session key (for management communication) or a group key (for group communication) is sent to the authenticated devices. Together with the corresponding counter, this key can be used to encrypt and decrypt the messages in counter mode. Thus, a secure channel has been established.

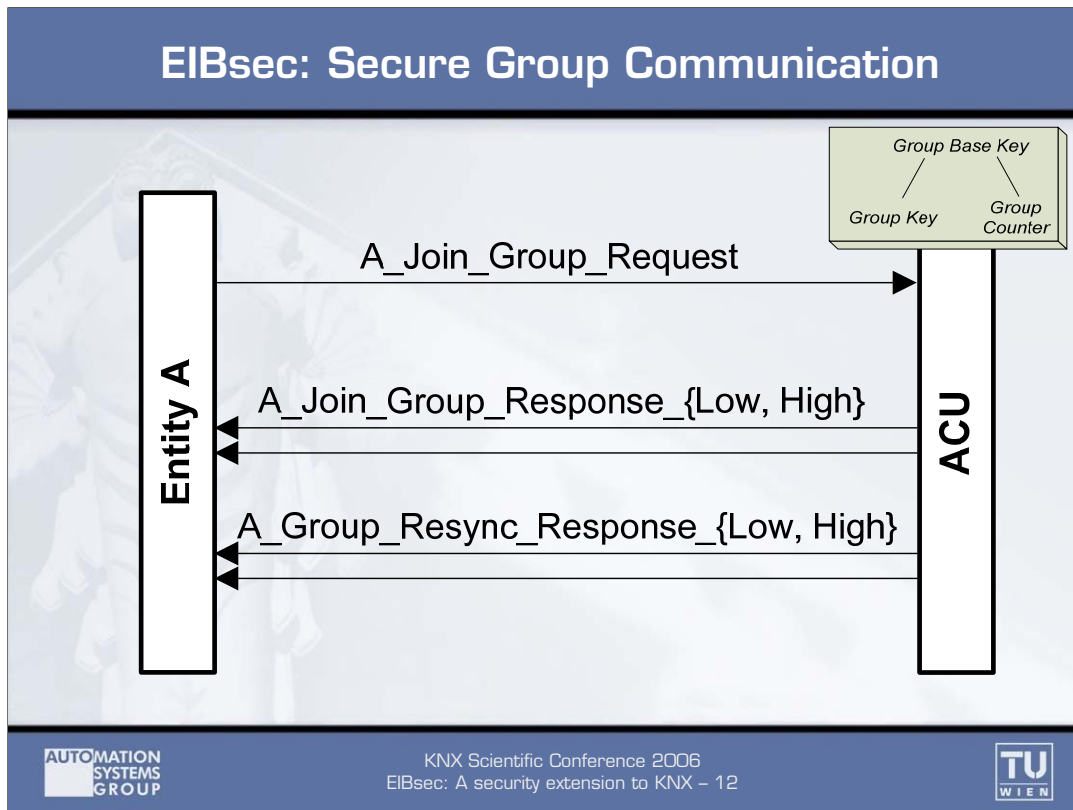


As mentioned before, a session has to be established to allow the secure exchange of management data. EIBsec's protocol for session establishment is based on a secure variant of the Needham-Schroeder protocol. To be able to use the standard KNX frame format in EIBsec, the protocol has been redesigned for the use in KNX. Without this modification, several messages would have to be split, causing unacceptable overhead.

Consider, for example, an entity  $A$  wanting to establish a session to entity  $B$ . To initiate the session,  $A$  sends an *A\_SessionKey\_Request* to the corresponding ACU. This message contains the address of  $B$ , a nonce  $N_1$  and a nonce  $N_A^*$ . To prevent replay attacks, a second nonce  $N_2$  is required which is retrieved from  $B$  using an *A\_Init\_Connect\_Request* (including address of  $A$  and a nonce  $N_B^*$ ).  $B$  responds with an encrypted *A\_Init\_Connect\_Response* message which includes the nonce  $N_2$ . Afterwards, the ACU generates a 128 bit session base key which is distributed to  $A$  and  $B$  using a *A\_Key\_Response\_Low* and a *A\_Key\_Response\_High* message. To prevent interception of the keys, these messages are encrypted using a dynamic node key. These dynamic node keys are calculated from the initial node keys (which are distributed at installation time) and the nonces  $N_A^*$  and  $N_B^*$ . Additionally, the previously sent nonces  $N_1$  respectively  $N_2$  are also included to prevent replay attacks.

After having received the session base key,  $A$  and  $B$  are able to calculate the session key and the initial session counter. Using these two values,  $A$  and  $B$  are able to encrypt their messages in counter mode. Thus, a secure channel has been established.

To further improve the robustness of the protocol, another three way handshake is optionally available. This handshake can be used to guarantee that both entities have successfully calculated the session key and the initial session counter. It also replaces an explicit connect message. However, since the identities of  $A$  and  $B$  have already been proven, this handshake is optional, though recommended (*A\_Auth\_Connect\_Request*, *A\_Auth\_Connect\_Reply* and *A\_Auth\_Connect\_Response*).



To protect group communication against security attacks, all group messages are encrypted in counter mode. In contrast to SEIB, it is not necessary to distribute the required group keys at installation time. If a device wants to join a secure communication group, it can retrieve the group key and the actual group counter value from the corresponding ACU. Furthermore, it is possible to revoke old or insecure group keys during runtime. This revocation service can also be used to limit the lifetime of group keys and generate new keys periodically.

In EIBsec, each communication group is assigned to a supervising ACU. This ACU calculates the group key and the initial group counter values using a randomly generated group base key. In order to be able to distribute the current counter value during runtime, the ACU must also keep track of this value.

Consider, for example, a device  $A$  wanting to join a group  $G$ . To retrieve the group key and the current group counter value,  $A$  sends an  $A\_Join\_Group\_Request$  to its ACU. This message contains the address of group  $G$ , a nonce  $N_I$ , and a nonce  $N_A^*$ . After having received this request, the ACU can optionally verify whether the device is allowed to join the group or not. If the device is allowed, the ACU sends the group key to  $A$ . Additionally, the current group counter value is also transmitted to  $A$ . To prevent unauthorized interception of these values, all four messages are encrypted using a dynamic node key which is calculated from  $N_A^*$  and the initial node key of  $A$ . The nonce  $N_I$  is also included in all four messages to prevent replay attacks. After having received these two values,  $A$  can encrypt and decrypt group messages in counter mode.

To successfully encrypt and decrypt group messages in counter mode, the counters of all group members must be synchronized. However, if the current counter value of a device loses synchronization with the group, the device can request the current counter value from the ACU using an  $A\_Group\_Resync\_Request$ . Another possibility is to test a small number of counter increments and decrements.

## Conclusion & Outlook

- Benefits of a secure building automation system:
  - New application areas
  - Protection of traditional applications
- Demands on the network increase
- Available solutions are flawed
- EIBsec: Security extension to KNX
  - Compatible secure management and group communication
- Next steps
  - Validation, evaluation and performance tests
  - Further R&D: Intrusion detection, wireless communication

Incorporating security concepts into traditional BAS offers a double benefit. First, the application area is extended. Using a secure BAS, it is possible to satisfy the demands of security critical applications. The application area of BAS is no longer limited to traditional service types. Second, traditional applications are also improved since protecting them against security attacks like vandalism is made possible.

Obviously, the demands on the underlying network of the BAS increase. The network must be protected against security attacks from the outside as well as from the inside. Protecting the control level is a major challenge. Due to the resource limitations and the use of non IP-based networks, the direct application of IT security mechanisms is not possible. Since available open standards do not provide the necessary mechanisms, work is required in this field.

A security extension to KNX called EIBsec has been proposed. EIBsec provides mechanisms for secure management and group communication. In order to manage the required secret keys in a secure manner, sophisticated key management is also part of EIBsec.

EIBsec is based on cryptographic algorithms and protocols which are commonly accepted as being secure. Nevertheless the presented protocol will benefit from formal validation. Currently, a first prototype implementation is under development which will be used for further evaluation and performance tests. Further steps include the integration of intrusion detection mechanisms as well as detection and handling of denial-of-service attacks, including the automated isolation of segments under attack. Since automation solutions based on radio communication, including KNX RF, rapidly rise in popularity, research regarding their security appears as another important topic.