Security Measures for Industrial Fieldbus Systems - State of the Art and Solutions for IP-based Approaches

Albert Treytl [1], Thilo Sauter [1,2], Christian Schwaiger [3]
[treytl, sauter]@ict.tuwien.ac.at, christian schwaiger@austriacard.at

[1]Vienna University of Technology
Institute of Computer Technology
Gußhausstraße 27-29/E384
A-1040 Vienna, Austria

[2]Austrian Academy of Sciences
Res. Unit for Integrated Sensor Systems
Viktor Kaplan Strasse 2
A-2700 Wiener Neustadt

[3]Austria Card
Lamezangasse 4-8
A-1232 Vienna,
Austria

Abstract

With the success of IP-based networks in the office world and the Internet as such the application of this technology also became attractive for the automation area. The design of next-generation fieldbus systems already picked up this idea. With the trend towards vertical integration in the field area and the seamless communication facilities IP-based networks offer, security gains importance. However, while security is already a topic for LANs and IP networks, the topic is only slowly gaining attention in the fieldbus segment.

This paper analyses the current situation of security measures for industrial fieldbus systems. With respect to IP-based systems the focus is set to the measures that are offered for the (TCP/)IP protocol and their applicability for the special situation of industrial fieldbusses. It will be shown where automation networks differ from communication relations in the Internet, and solutions for the particular security problems on the field level and the interconnection with higher levels will be proposed.

1. Introduction

During the last decade IP (Internet protocol)-based local area networks (LAN) and more recently the Internet have gained a leading position for communication systems. With the ubiquity of IP-based networks the idea of full vertical integration in plant communication (following the old CIM pyramid model) became feasible and more attractive. Today IP-based networks are already widely (in fact practically exclusively) used at management level and as backbones to connect remote fieldbus segments. As a logical consequence IP and LAN technologies have started to penetrate the field level. “Fieldbusses” like PROFInet already demonstrate this idea, and the ongoing standardization work on real-time extensions for Industrial Ethernet underpins the importance and especially the market relevance of the topic.

The trend towards a homogenous communication platform and the increasing internetworking between different automation entities and levels on the one hand remove communication barriers but on the other hand introduce the need for implementing security measures. While in the past fieldbus systems in industry automation where typically operated in closed environments and access was restricted physically, today’s possibilities of remote control and networking call for (advanced) security measures.

This paper will first analyse today’s industrial fieldbus systems (with a focus on those standardized by IEC) with respect to available security concepts and will discuss the applicability and security level of the implemented measures (section 2 and 3). Section 4 looks at security measurements for the remote monitoring and/or configuration of distributed fieldbus systems over the Internet. Especially, security protocols are of interest that go beyond the simple, but nonetheless very common use of <*username, password*> transmitted in plain text. Finally, enhancements for IP-based fieldbus systems will be shown in section 5. The implications of security measures available for the TCP/IP protocol family on IP-based fieldbus systems will be discussed.

2. Security Goals

IP-based networks become very attractive means for remote installation, monitoring, control, and management of a fieldbus network. Taking into account the quite miserable reputation of the Internet and its underlying IP protocol stack in regards of security, the importance of security is cleary shown by many initiatives to make IP-based networks secure.

For fieldbus systems the awareness still needs to be strengthened. While for remote control the need for security measures is commonly agreed upon, security issues in the field area itself are still neglected. The usual argument to defend the lack of security is that fieldbus systems were always seen and developed as isolated networks. Still, from a historical perspective, this is not fully true. After all, one of the major stimuli for the

Proceedings of International Workshop on Factory Communication Systems
2004, 201-209, (C) IEEE 2004

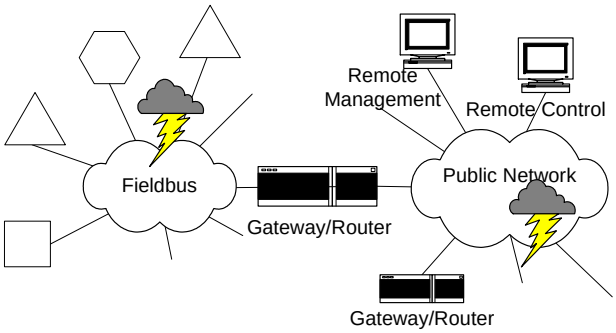

Figure 1: Security threats to a fieldbus

development of fieldbus systems was the introduction of CIM and the recognition that in this comprehensive networking model the lowest level could not be covered by available solutions. So, originally the interconnection to other networks was indeed a focal point in the early days of the fieldbus concept [1]. What practice made out of it, however, was in most cases something different. The bottom-up evolution of dozens of different solutions did not really care much about network interconnections, and fieldbus systems grew to be what they are today: isolated networks.

But even if interconnectivity had played a stronger role in the practical implementation of the fieldbus idea, it can be doubted whether security issues would have received more attention. By the time the work on fieldbus systems was started (i.e., in the mid 1980s), network security was a rather elitist topic: The first computer viruses had just been programmed, the first Internet worm was yet to come, and having access to computer networks was still a rare exception. It is thus no wonder that security had no prominent role in the development of fieldbus systems, and nobody actually is to blame for that.

Moreover, security threats from the inside were not considered, though it is known today that many violations of security policies come from the inside. The best we can say is that security was only an add-on in fieldbus design.

Today this point of view slowly changes partly because of the increasing connection between the field and the management level and partly because fieldbus systems were also introduced in areas where many parties may have (and need to have) access to such a system (e.g., in building automation).

Speaking about security, we can identify four big goals that are should be achieved:

- *confidentiality*, meaning that only authorized entities must be able to read confidential data,
- *integrity*, stating that no unauthorized entity must be able to change data without being detected,
- *availability*, mandating that data is on-hand when needed, and
- *authentication*, stating that an entity is which it claims to be,

or CIAA for short. Availability is a well-known problem and is covered by most of the systems, but usually no malicious attacks are considered. Likewise, integrity is one of the big goals of fieldbus protocol design, although active malicious manipulation is not taken into account. If provided at all, "security" services should rather protect against accidental errors, malfunction, or natural sources of errors like noise or interferences than against active manipulation.

Figure 1 outlines a common scenario for the use of fieldbusses and identifies security threats within the fieldbus and from the public network. The next section will analyse security measures offered by common industrial fieldbusses to reach the security goals. Section 4 will then look at the protection of the access to the fieldbus from outside.

3. Security of Industrial Fieldbus Systems

It is a common prejudice that today's fieldbus systems do not exhibit any security measures. There are such concepts in communication systems for building automation [2], and there are even traces in fieldbus systems for industrial and process automation, which are the focus here. It is true, though, that these approaches are quite limited in scope and capabilities. Usually they do not even deserve to be called security measures if we use the term in the strict sense of an IT context which is the usual backdrop for security discussions.

Nevertheless, this section will give an overview of the security measures planned and/or implemented in fieldbus systems covered by IEC 61784 [3] and the underlying IEC 61158 [4]. In general, we have to distinguish between two classes of systems: traditional fieldbus systems and Industrial Ethernet approaches. The latter are based on the IP protocol suite and naturally offer better possibilities. The peculiarities of TCP/UDP/IP are treated in the next section.

It has been argued that security measures can be introduced in every layer of the OSI model [5]. Accordingly, the survey will follow the layer structure of the individual fieldbus systems. The physical layer, however, is excluded since there are no security concepts whatsoever defined in IEC 61158-2.

3.1. CPF 1 – Foundation Fieldbus

The Foundation Fieldbus *Profile 1/1 (H1)* consists of the data link layer type 1 and the application layer type 9. It is meant as a fieldbus for the lower automation levels (typical sensor/actuator applications) and was designed for efficiency and resource conservation. The data link layer service definitions do not contain any security-relevant definitions. There exists the term "authentication", however this is rather a QoS attribute controlling the addressing information used for data transfer. This is a feature relevant for safety applications, but is not related to data security at all.

The application layer foresees simple access protection mechanisms like the definition of access groups with associated access rights and the usage of passwords. This protection mechanism stems originally from MMS and was historically introduced via the FIP application layer. The security model is inspired by the owner/group/world access rights management in, e.g., UNIX-based systems. Every object has a password associated with it (8 bits long) as well as a list of access groups (also an 8-bit word, corresponding to eight different groups). Furthermore, there are – depending on the type of object – several access rights defined (like read, write, execute, delete, etc.) that may be activated for the password (equivalent to the owner in UNIX), the groups, and all communication partners without restriction.

Unfortunately, these security means are not mandatory for implementation, which limits their usability. The password itself is simply an 8 bit word without any explicit protection, let alone encryption. This concept resembles weak security measures known from, e.g., SNMP, where a community string is defined (even mandatory) to protect data access. Alas, this string is transmitted in clear text and hence rarely used at all (the default value "public" is hardly ever changed).

The *Profile 1/2 (High Speed Ethernet, HSE)* is meant as a backbone solution and builds on Ethernet. The data link layer specifies ISO/IEC 8802-3 (Ethernet), the LLC sublayer ISO/IEC 8802-2 (CSMA/CD), and it is explicitly noted that for security requirements ISO/IEC 8802-10 (Standards for Interoperable LAN/MAN Security) can be used optionally.

The network layer of HSE is RFC 791 (IP), the transport layer uses RFC 768 (UDP) and RFC 793 (TCP) where necessary, all in their standard form without any special features.

The application layer is compiled from type 5 and type 9 and contains no specific security provisions. There are however simple access protection means like in H1. This means that possible security extensions for HSE could rely on secure versions of TCP/UDP/IP as described in section 3.

Finally, FF *Profile 1/3 (H2)* is very similar to H1 and also consists of the data link layer type 1 and application layer type 9. In fact it is a migration path for WorldFIP installations (Profile 5/1) and not really used in practice. With respect to security, it is identical to H1.

3.2. CPF 2 – ControlNet

Profile 2/1 (ControlNet) uses type 2 data link layer and application layer. The data link layer uses a "connection originator password" to secure connections. This password provides a means of authentication for access control. However, it is not transmitted over the network and used only locally. It is defined by the configuration tool during system setup.

The application layer uses "electronic keys" to verify the connected devices (very much like a device ID) and to provide some sort of authentication for a connection. Nevertheless, the keys themselves or their handling are not particularly secured. What the application layer does foresee are simple access rights for individual objects.

The data link layer of *Profile 2/2 (EtherNet/IP)* uses parts of the type 2 definition, but apart from that builds on ISO/IEC 8802-3. The application layer is identical with ControlNet and uses the Control Information Protocol (CIP). All application layer services and the protocol are mapped onto TCP/UDP/IP. One detail explicitly noted in the document deserves mention: The standard defines no requirements for the management of the TCP connection, such as inactivity timeouts, or closing the TCP connection when all native connections are closed. It is up to the implementations to implement these if necessary.

3.3. CPF 3 – PROFIBUS

Profile 3/1 (PROFIBUS DP) uses type 3 for both layers. The data link layer provides basic access control for a few management functions. This is achieved by statically limiting access to selected and preconfigured station addresses.

The application layer also exhibits some rudimentary access protection for process data objects, load region objects, and function invocations, but without any special security precautions. Interestingly enough, there is a note in the document confirming the impression of the security-aware reader: "This is not a protection against intentional misuse of the communication facilities of a field device but helps to protect a system for accidental erroneous use of Process Data". This statement is in fact a generic one and is true for all traditional fieldbus systems in industrial and process automation.

Profile 3/2 (PROFIBUS PA) is basically identical with the DP version, except for other options in the data link layer protocol and of course the modified physical layer. From the security viewpoint, there is no difference to DP.

Profile 3/3 (PROFInet) is the third Industrial Ethernet solution in the IEC fieldbus standard and uses plain ISO/IEC 8802-3 on the data link layer.

The application layer (type 10) builds on ORPC as middleware to provide services and protocols. Commands and date are actually transferred via the ORPC Wire Protocol or the DCOM/DCE-RPC wire-protocol. The protocol stack includes from top down DCOM/DCE, RPC, and finally TCP/UDP/IP. On the application layer level, no additional security precautions are defined.

For the sake of completeness, it should be noted that the original PROFIBUS version FMS, which has come of age and is no longer explicitly included in the profile definitions of IEC 61784, also included the security

model already described for Foundation Fieldbus. The reason is that FMS was also derived from MMS.

3.4. CPF 4 – P-NET

There are two P-NET profiles that differ only in the interface used on the physical layer: *Profile 4/1 (RS-485)* and *Profile 4/2 (RS-232)*. Both layers use the type 4 definitions. And even though P-NET was among the first fieldbusses to address really distributed systems, there are no security concepts, apart from a simple write protection of remote variables that can be activated.

3.5. CPF 5 – WorldFIP

The WorldFIP communication protocol family consists of three profiles compiled from different subsets of the data link and application layer types 7. As it stands, the profiles 5/1 to 5/3 defined in IEC 61784 do not contain any special security concepts. The protocol specifications of WorldFIP described in the IEC 61158 series, however, are substantially more comprehensive than what is covered in the profile definitions.

The application layer document comprises basically the same access protection based on passwords or access groups as Foundation Fieldbus. Again this is no wonder because the WorldFIP application layer is a subset of MMS. Permission is checked when an association on a device is initiated and for operations on the domain object, for program invocation, certain variable accesses, and access to events. Both the password and access group definition are each eight bit long and are transferred in plain. If password or access group match for a specific request, the additional access rights parameter further details allowed operations. The specification states that “on a channel with access protection, the access protection parameters provided during the opening of the association (negotiated or pre-negotiated) are analyzed with respect to the values of the password, access rights and access groups attributes of the object. If there is inconsistency, the operation is not performed and a negative report is transmitted”. Implementation of these security mechanisms is not mandatory except for the highest conformance class 5.

3.6. CPF 6 – Interbus

Interbus is present with three profiles, all of which make use of type 8 of both data link and application layer. On the data link layer, no security concepts are foreseen. On the application layer, access protection is again based on the MMS model already discussed. Historically, this evolved because the Peripherals Message Specification (PMS) of Interbus is basically identical with FMS of PROFIBUS. Again, this access protection scheme is optional, but there are applications where it is being used.

As an enhancement to the traditional fieldbus, *Profile 6/2 (Interbus TCP/IP)* gives the possibility to tunnel TCP/IP traffic over conventional Interbus. However, as this comes down to a simple encapsulation of IP frames in the Interbus protocol, it does not count as true Industrial Ethernet solution. Furthermore, because of the encapsulation, the security features of TCP/IP cannot be exploited for the fieldbus. On an end-to-end level, one could make use of them, provided that the application on the fieldbus node is properly set up; but on the fieldbus itself, the encapsulation shields the TCP/IP mechanisms.

3.7. CPF 7 - SwiftNet

SwiftNet is mostly use in aviation, i.e., truly closed systems, and is included in two versions. *Profile 7/1* contains only the data link layer (type 6) and omits the application layer. The full stack version *Profile 7/2* also comprises the type 6 application layer. Both specifications, however, do not contain any particular security mechanisms.

3.8. Prospects

Table 1 gives an overview of the available security measures. Compared to security measures of IT systems fieldbus systems have to be considered insecure. With little effort plain-text passwords can be recorded and the short length also do not allow applying modern cryptographic algorithms to (re-)use these fields for security extensions.

Table 1 Security Services for Industrial Fieldbus Systems

System	Security Services
Foundation Fieldbus	8 groups, access rights, 8 bit plain-text passwords
Control Net	Connection authentication, plain-text electronic keys
Profibus	Access protection, limited to preconfigured addr.
P-Net	Simple write-protection of variables
World-FIP	8 groups, access rights, 8 bit plain-text passwords
Interbus	8 groups, access rights, 8 bit plain-text passwords
Swift-Net	n/a

Although these measures are not sufficient for today’s security needs (sometime they were not even intended to fulfil them; see section 3.3) they already indicate that there is a focus on authentication. Access protection is a kind of user authentication. A comparison with fieldbus systems in building automation (refer to [2] for a review of relevant security measures) points out the importance of cryptographically secure integrity protection. Encryption to protect confidentiality is almost totally neglected in building automation systems.

Security measures (CIAA) must be selected and applied according to the (security) needs of the individual fieldbus installation and application. Security is always a trade-off between costs of threats and

overhead due to security. The experience of the authors points to a gaining importance of secure integrity and authentication services for typical usage scenarios. On the other hand research also shows that security can introduce big overheads [6].

Looking at today's situation only a trend of growing awareness for security on the field level can be observed. Security often stops at gateways that connect the fieldbus to the internet. Fieldbus systems mostly are still believed to be secure because they are "isolated" networks. If we consider the increasing importance of vertical integration, this can be an expensive misbelieve.

4. Security for Remote Fieldbus Access

Apart from securing fieldbus communication itself the topic of securing remote fieldbus access for monitoring or configuration purposes is of interest as well. Today it is the main focus of most security measures although the implemented measures such as username/password or MD5 authentication (for his algorithm weaknesses are already found and is not recommended for installation in new devices) are weak.

In the case of a fieldbus system that uses TCP/IP the Internet is the natural communication channel for this task as the necessary equipment is already available. For fieldbus systems not based on TCP/IP the same holds because the Internet is readily available world-wide and solutions based on private networking infrastructures are too expensive. Additionally, Web-based solutions have the advantage that training for users becomes less difficult because they already know and use similar mechanisms. In both cases some combination of a router/firewall which connects via a gateway to the fieldbus is a natural solution [7]. In the first of TCP/IP-based fieldbusses the gateway will mostly be used to separate the fieldbus from the publicly reachable Internet. For other fieldbusses the gateway will be more complex and translate between the fieldbus protocol and the TCP/IP protocol. This distinction is of little importance for (the following) considerations regarding security.

Before we discuss a possible solution based on the TLS [8, 9] protocol we look at differences between usual Web-based security mechanisms and those needed for access to a fieldbus. We note that other secure authentication mechanisms are available such as the Simple Authentication and Security Layer (SASL) which provides a framework for the provision of authentication and data security services. We still concentrate on TLS because it is already integrated in all common Web browsers and widely accepted. For Web-based access TLS also seems preferable over IPSec. Although it does not offer more security, again its integration in all common Web browsers as well as the easier usage makes it our favourite choice.

Usage of TLS is most often encountered in Web-shops in e-commerce: Here, the server uses a certificate to authenticate itself against the client, which gives the client confidence that it is really talking to the Web-shop of the company it intends to. The client itself has no need to authenticate itself. For secure connection to a fieldbus this scenario is of little use: Here, we want the user of the client to be authenticated before gaining access to the fieldbus resources. Looking at another example, Web-banking, we usually have the following scenario: A TLS session between client and server is established and the server authenticated. Before the user gets access to his bank account he has to provide some or more of *username*, *password* or *PIN* (personal identification number) to additionally authenticate himself to the server.

In the case of remote access to a fieldbus, the gateway and/or firewall acts as a "server". In the sequel, we will retain this standard terminology to facilitate comparison with the standard approaches known from the Internet. For fieldbus systems a scenario similar to Web-banking is applicable since the server must identify the legitimate user by authentication. Authentication of the server protects the user's credentials (password etc.) from adversaries. While this scenario seems to fit the needs of remote access to a fieldbus system, it does not necessarily fit in practice. The reason for this lies in the fact that one user may be responsible for many fieldbus installations, maybe even from different companies. Using one single password for all installations is a bad idea and using a different password for every installation is in fact infeasible. Therefore, users of a server need some other means for authentication. This can easily be achieved if every user of the fieldbus has his own certificate which he can use to authenticate against the server.

Certificate-based authentication is done during the TLS handshake using an optional client certificate that allows the server to authenticate the user before granting access to the fieldbus. While this approach is secure and scalable, certificate management is not trivial. In essence it means that a fieldbus operator has to establish his own private public key infrastructure (PKI) to generate and distribute client and server certificates. Such a deployment is not trivial and has to be planned carefully, in advance. A good starting point for exploring this option is [10]. While designing, implementing and maintaining a PKI is no easy task, certificates for clients can offer better security than password-based solutions because cryptographic keys used during authentication can be stored in a dedicated, secure, tamper-proof token, such as a smart card. The main disadvantage for the deployment in gateways is the fact that the TLS handshake is very computing intensive. Negotiation of security services usually uses asymmetric cryptography to establish shared symmetric session keys for authenticating and encrypting transferred data. While big

Web servers for e-commerce can easily do this by using load-balancing between multiple machines and/or by using special hardware that accelerates asymmetric cryptography, this will not be possible for access to a fieldbus. Providing comparable infrastructure is simply too expensive, especially when the number of fieldbus installations grows. This makes a server potentially vulnerable to a denial of service (DOS) attack: By repeatedly sending connection requests the server is overloaded. To mitigate this situation an approach that uses only symmetric cryptography which is much faster might be desirable. At the same time the advantages of the solution described above should be retained, namely:

- No need to remember many passwords.
- Possibility to use secure hardware.

Fortunately, this is possible using TLS. As discussed for IPSec (section 5), TLS was also designed in a way that makes it possible to specify additional algorithms in the future[1]. Indeed, [11] did exactly this. Instead of asymmetric authentication during the TLS handshake, Kerberos [12, 13] is used for authentication of the user. Kerberos uses Key Distribution Centers (KDC) to issue encrypted tickets to prove the identity of both end users and network servers. To this end Kerberos uses only symmetric cryptography. While the effort to establish a Kerberos infrastructure is comparable to that of establishing a PKI, it might be better suited for the kind of servers that can be expected for remote fieldbus access.

Shielding the fieldbus is a vital topic if possible threats are considered. Nevertheless, today the strength of security mechanisms deployed at this side is in most cases not equal to comparable IT measures. Replacement of the existing weak mechanisms by stronger and easier-to-use security mechanisms such as certificates should be a focus for future activities.

5. Security Measures for IP-based Fieldbus Systems

Because of the wide dissemination of TCP/IP based on Ethernet as network medium, this combination is becoming increasingly interesting for the field level. It is not yet clear whether Industrial Ethernet will ultimately replace traditional fieldbusses, however there are several good reasons for the use of Ethernet, not only from a marketing perspective:

- TCP/IP and Ethernet are well known technologies.
- The wide dissemination decreases hardware costs.
- Distributed systems, e.g., Web-based access can easier be realized.
- Protocols from the IETF (covering TCP/IP and related Internet protocols), the World Wide Web Consortium (W3C, covering XML and related specifications to promote interoperability for the Web) and other organizations may be utilized.
- Implementations of the above mentioned protocols and specifications are widely available.
- Skilled personal in this field are easily available.

One system that uses TCP/IP over Ethernet is PROFInet which is defined by IEC 61784, section 7.4. PROFInet uses standard ISO 8802-3 on the data link layer. The application layer is of Type 10 according to IEC 61158. Here the DCOM/DCE-RPC protocol is mapped onto the TCP/IP family of protocols which covers the transport layer and the network layer.

While section 3 illustrated that fieldbus systems based on TCP/IP have little or no provisions for security, section 5.2 looks at security protocols already defined for the Internet which might also be used to secure fieldbusses. If possible such protocols should be used to provide security because:

- They are already available.
- Their security has been assessed by the Internet community.
- Secure solutions are hard to design from scratch and the design is very error-prone.

Security measures at layer 7 or above are naturally also of interest, especially where established (security) protocols are not sufficient or applicable. This might be the case, e. g., if hardware is used that already implements the protocol stack up to the application layer or because of real-time constraints. Because such measures will be very specific – and therefore different – for every fieldbus system we will not consider them in this paper.

5.1. General Considerations

The original TCP/IP protocol family was designed without any security considerations. With the commercialisation of the Internet in the 1990s security was discovered as a necessity for e-commerce and related applications. Therefore, security provisions for Internet traffic were designed to alleviate those problems. The result was in development of numerous new protocols. Examples are:

- (Open)PGP (Pretty Good Privacy) or SSH (Secure Shell), operating at the application layer.
- SNMP, version 3 which among others introduced security services to earlier versions of SNMP.
- SSL/TLS operating at/above the transport layer. Web-based interfaces are mainly secured by SSL/TLS (in the following only called TLS). Section 4 discussed its usage for remote access to a fieldbus installation.
- IPSec, operating at the network layer.

In the following we will concentrate mainly on IPSec as a means to secure traffic between fieldbus nodes since it seamlessly integrates the security measures within the network protocol.

[1] This is not unusual for cryptographic protocols because cryptographic schemes thought to be secure might be broken and need to be replaced.

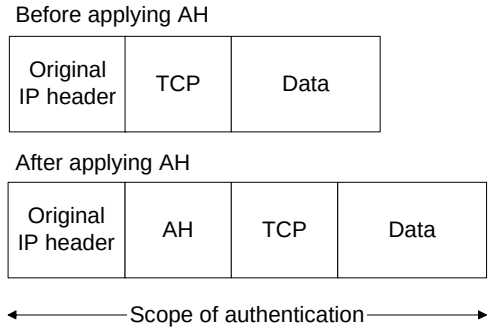

Figure 2: Example of AH in transport mode.

Another issue for fieldbus security is the network topology. For the use of Industrial Ethernet usually a full-duplex switched network is used that supports 100 Mbit/s connections and avoids collisions. From the security view point this switched network is favourable because it prevents eaves-dropping on a shared medium as the used switches transport packets only to the intended destination as long as no broadcast mechanism is used. Despite the fact that such measures increase the effort of an attack they have to be analyses carefully and will only increase security in the context of a well-planed security policy. In case of switched Ethernet the protection is only true if the switched network is organized as a star or a tree topology. In the case of a logical bus organization, which is for example also defined for PROFInet (especially for the real-time variant V3), eaves-dropping by an adversary is still a topic. Moreover, it is assumed that an adversary do not listen on the line between node and switch.

5.2. IPSec

IPSec is a protocol family that aims to secure traffic on TCP/IP networks on the network layer. It has been developed by the IP Security working group of the IETF. The RFCs (Request for Comment) that constitute IPSec [14] are divided into the following subgroups:

- Architecture describes the overall concepts and architecture as well as the security requirements.
- Authentication Header (AH) protocol which may be used for integrity protection of packages.
- Encapsulating Security Payload (ESP) protocol which supports confidentiality and/or integrity services of packages.
- Authentication algorithms for use with AH or ESP as well as encryption algorithms for use with ESP. Using the mechanisms defined in this document set new algorithms for AH and ESP can easily be introduced in the future.
- Documents that cover various key management techniques and schemes.
- Domain of Interpretation which defines values such as encryption or authentication algorithms that are needed to relate the other mentioned documents to each other.

The actual RFCs defined for IPSec can be found at the homepage of the IP Security working group (http://www.ietf.org/html.charters/ipsec-charter.html) where also new specifications drafts can be found.

The services that can be realised by the use of IPSec are:

- Access control (AH and ESP),
- Connectionless integrity (AH, ESP if authentication is enabled),
- Data origin authentication (AH, ESP if authentication is enabled),
- Anti-replay (AH and ESP),
- Confidentiality (ESP if confidentiality is enabled) and
- (limited) traffic flow confidentiality (ESP if confidentiality is enabled).

One of the main concepts of IPSec is the notion of a security association (SA). An SA is a one-way connection between a sender and a receiver that specifies the security services to apply to the traffic carried over the connection. One SA may be established for the use with either AH or ESP, but not both. Each SA contains the following parameters that may be used to uniquely identify it: A Security Parameter Index (SPI), the IP destination address and the security protocol identifier which may be AH or ESP. Parameters of every SA are stored in an SA Database. As one SA may be either used for AH or ESP it is possible to bundle multiple SAs through which traffic must be processed. SAs either support transport mode for communication between two hosts or tunnel mode for communication between a host and a security gateway or between two security gateways.

5.3. Fieldbus Node Security and IPSec

The use of IPSec for fieldbus systems is particularly appealing for IP-based fieldbus systems because it is compatible with standard IP as regards the services offered to the upper layers[2]. Thus, the actual fieldbus protocols need not be changed. What has to be added, though, is the management of the security features.

For the application of IPSec at the fieldbus level either AH, ESP or a combination of both AH and ESP could be used depending on the required security services. This has to be decided for every deployment of a fieldbus installation according to the security policy of the organisation deploying the fieldbus. For the communication between the nodes transport mode can be used. Transport mode inserts a security header after the IP header and, in the case of ESP, an ESP trailer after the protected packet as shown in Figure 2 for AH[3].

[2] For none-IP-based fieldbusses IPSec can only be used directly for connections where the fieldbus protocol units are transmitted (tunneled) over an IP channel.

[3] This figure shows the use of AH with an IPv4 header. The situation for IPv6 is similar.

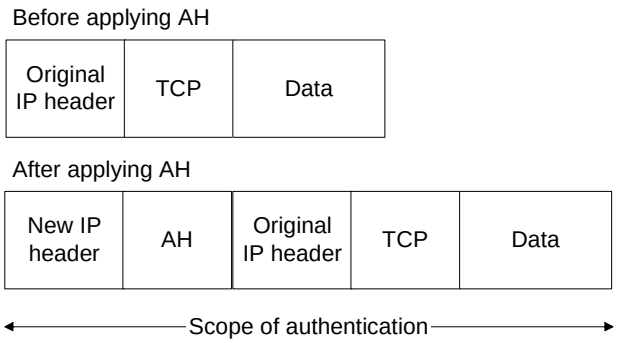

Figure 3: Example of AH in tunnel mode.

The main problem that arises is the establishment of SAs between the nodes. The default Key Establishment Protocol (IKE, Internet Key Exchange) uses an asymmetric mechanism based on the Diffie-Hellmann protocol which is unsuitable for use at a resource-constrained node. Because IKE might be prohibitive, manual key management may be used. A good choice would be to use the same SA in every node for communication with every other node. This also simplifies the management of the SA database. Because nodes are usually parameterized by one organisation which deploys the fieldbus, manual key management can be supported by a (proprietary) tool. As the SA is used by multiple nodes, anti-replay mechanisms, which are based on a window concept, cannot be used. Here, other mechanisms provided by the fieldbus have to be used or the full IPSec specification with one SA between every pair of nodes has to be implemented. In this case any manual key management becomes unwieldy with only a small number of nodes as the number of SAs to establish for n nodes is roughly n^2.

5.4. Distributed Fieldbus Security

If a fieldbus is distributed over different sites and data has to be transported over the public Internet two possibilities arise: transport mode security as described in section 5.3 or security services using tunnel mode.

Tunnel mode is especially of interest if IPSec security services on either side are not necessary, e.g., because of organisational measures that ensure on-site security. In this case only the security gateways that connect the distributed fieldbus installation need to implement the full IPSec standard. The fieldbus nodes themselves need not be changed in any way. In the latter case an anti-replay mechanism may also easily be used, if desired. In tunnel mode the whole IP packet to be transmitted ("inner packet") is enveloped by a new "outer" IP packet. While the inner packet holds the real source and destination addresses the outer packets may (and usually will) contain distinct addresses such as those of security gateways. Figure 3 shows tunnel mode for AH.

If tunnel mode alone is not sufficient because the single nodes also need protection, tunnel mode SAs can be combined with transport mode SAs to enable end-to-end security.

5.5. Summary

Although it is yet too early to say that IPSec will be the solution to fieldbus security issues, it fulfils all requirements to be a prime candidate: It offers all necessary security mechanisms and seamlessly integrates into the IP protocol. Moreover, it is a single solution for securing the fieldbus as well as the Internet connections to remote management stations or other fieldbus networks. Problems to be solved are key distribution and establishment of SAs. Solutions to these problems must exploit the peculiarities of fieldbusses (e.g., parameterisation by one entity) to meet the restricted resource at the field level.

6. Conclusion

Fieldbus technology is established and widely used. During the last years standardization efforts have finally been successful. One deficit of the lengthy standardization process was that the recently emerged need for remote access has not been taken into account properly. As a matter of fact, establishing possibilities to include strong security mechanisms in fieldbus systems has never been an issue, even though it should have been. If security needs should be covered in practice, it appears that secure integrity and authentication services are the ones missing in contemporary fieldbusses.

For IP-based "fieldbus" systems one possibility to get around the lack of native security mechanisms and to still secure fieldbus messages is to use IPSec. This approach works for on-site security as well as for distributed installations. According to the actual security needs SAs can be reused, simplifying the key exchange but sacrificing anti-replay mechanisms, or the full IPSec protocol can be implemented, though the latter requires more computing resources at the fieldbus nodes.

Secure remote access proves to be harder than thought at first sight if <*username, password*> in the plain are not sufficient. The installation and maintenance of an authentication service is no trivial task and still mostly an organizational question. Yet, there is sufficiently mature technology available to finally tackle these problems. The need for such measures is clearly there.

Acknowledgements

The authors would like to thank Eckehardt Klemm for useful hints and information about the security features of MMS and fieldbusses derived from it.

References

[1] G. G. Wood, “Survey of LANs and Standards”, Computer Standards & Interfaces, vol. 6, 1987, pp. 27-36.

[2] C. Schwaiger and A. Treytl, “Smart Card Based Security for Fieldbus Systems”, 2003 IEEE Conference on Emerging Technologies and Factory Automation, Lisbon, 16.-19. Sep. 2003 ,pp. 398-406, 2003.

[3] International Electrotechnical Commission, IEC 61784-1, Digital data communications for measurement and control - Part 1: Profile sets for continuous and discrete manufacturing relative to fieldbus use in industrial control systems, 2003

[4] International Electrotechnical Commission, IEC 61158, Digital data communications for measurement and control - Fieldbus for use in industrial control systems, 2003

[5] Ch. Schwaiger and T. Sauter, “Security Strategies for Field Area Networks”, 28th Annual Conference of the IEEE Industrial Electronics Society (IECON), Sevilla, 5.-8. Nov. 2002, pp. 2915-2920.

[6] A. Treytl, N. Roberts, and G. P. Hancke, “Security Architecture for Power-line Metering System”, 5th IEEE Workshop on Factory Communication Systems, Vienna, 22.-24. September, Work in progress session, 2004

[7] T. Sauter and Ch. Schwaiger, Achievement of secure Internet access to fieldbus systems, Microprocessors and Microsystems, 26 (2002), pp. 331-339.

[8] T. Dierks and C. Allen, “The TLS Protocol Version 1.0“, RFC 2246, January 1999, available from: http://www.ietf.org/html.charters/tls-charter.html

[9] E. Rescorla, “SSL and TLS”, Addison Wesley, ISBN: 0201615983, 2000.

[10] R. Housley and T. Polk, “Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure”, John Wiley & Sons, 2001.

[11] A. Medvinsky and M. Hur, “RFC 2712: Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)”, October 1999, available from: http://www.ietf.org/html.charters/tls-charter.html

[12] J. T. Kohl, B. C. Neuman, and T. Y. Ts'o, "The Evolution of the Kerberos Authentication System", in Distributed Open Systems, pages 78-94, IEEE Computer Society Press, 1994.

[13] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

[14] The RFCs that specify IPSec and working drafts are available from: http://www.ietf.org/html.charters/ipsec-charter.html