D. Dietrich, P. Palensky, A. Treytl
Vienna University of Technology, Austria

Communication in Automation with the emphasis on security

Security is normally an ignored aspect in the field of Field Area Networks (FANs, a.k.a fieldbusses). Home and building automation networks are now the first one to do the first steps towards more security, since security is a key aspect of an automated building. Up to now, the risks of attacks were relatively small. However, this situation will change completely by the dramatic increase of the number of FAN nodes and the increasing interconnection of different FANs. The goal of this paper is to analyze today's situation but also to propose and point out common efficient solutions for different, and especially for high-level security requirements.

1. Introduction

In the past Field Area Networks (FANs) – communication systems for automation purposes – were usually used in closed environments (e.g. industrial and process automation). Independent of the application area and trade FANs were stand-alone systems and isolated networks. With the establishment of the Internet and the wish for total remote control as well as the applicance of FANS in public areas in building automation, security questions gain a new quality. The key question becomes more and more relevant: Are traditional security measures like "firewalls" or physical access restriction enough to secure networks in the automation area? Massive networking and ubiquitous communication cause paradigm shifts in all areas, with dramatic changes, similar to the influence of the personal computer in the 1980s. The Internet offers new opportunities for FANs and embedded systems to interconnect virtually all electrical components of a system, to save energy, to reduce maintenance costs, and to increase functional flexibility while achieving a higher level of quality. However, at the same time this massive interconnection makes systems increasingly vulnerable, because remote access and flexible communication ease the access to the systems. Especially in building automation beside the monetary risk of attacks also human life is affected. Therefore, the question about practical and efficient solutions becomes a very vital one.

To discuss the problematic nature it will be necessary to first state the security basics and the possible attacks, which we have to consider. In the following discussion the state of the art of security in FANs should be explained, and finally the consequences of the ongoing shift to complex systems has to be pointed out, because it is an important factor for ubiquitous computing and security measures. On this base it is possible to show modern solutions and possibilities to reach a

high level of security.

2 Security and attacks on networks

Today accepted principles concerning security are, that 100 % security is impossible and that security should not be dependent on the secrecy of the used algorithm and mechanisms. Rather, security is a function of the value of the protected value and the success of an applied mechanism must only be based on the secrecy of the used keys/passwords (principle of Kerkhoff). Beside these principles the security policy and the used security procedures are only determined by the application and by the value that should be protected.

The three big security goals and services are confidentiality for the sake of protecting data, integrity stating that no unauthorized entity must be able to change data without being detected, and availability in order to be able to offer data or services at any time. Implementing security always starts with a risk analysis and setting up a security policy. In the second step the necessary security mechanisms can be specified and finally implemented. In opposite to this procedure many people entirely focus on complicated encryption algorithms. The resulting “security holes” are difficult and expensive to fix afterwards, because of the missing security policies.

Common security threats are ([1]):

1. Stealing confidential information
2. Tampering information
3. Resource stealing
4. Destroying information and resources (denial of services)

In the automation area stealing confidential information is not so important as integrity of data. Taking in consideration automatic metering for example the most evident aspect will be tampering of information. In this example a reasonable security threat is that customers will reset their energy meter each month via their own network at home. But integrity is also important for the customer to set up a legal base that only the consumed energy must be paid. The SELMA-Project (see http://www.selma-project.de) for instance uses digital signatures for this. In the same sense the threat of resource stealing can be neglected in the area of automation, whereas destroying information as well as blocking resources must be considered as a more crucial security threat especially in building automation. Denial of Services (DoS) attacks do not need to be based on attacks to the physical infrastructure. The IP world knows DoS attacks like the PING of death, smurf attack and other attacks that are for instance based on spoofed IP addresses. Such attacks, as well as buffer overflow attacks, are only successful if the network infrastructure (protocols, software, devices) is faulty. A system with faulty IP stack implementations is naturally vulnerable to DoS attacks. But even if the network infrastructure is safe, it is still possible to attack a for instance password-based protocol with a sniffed plain text password or dictionary, brute-force and social attacks.

In the security policy these aspects have to be worked out with great care and the various services like authentication, data integrity, non-repudiation, confidentiality or access control and the different possible mechanisms like ciphering or data access mechanisms must be adapted to the identified security threats.

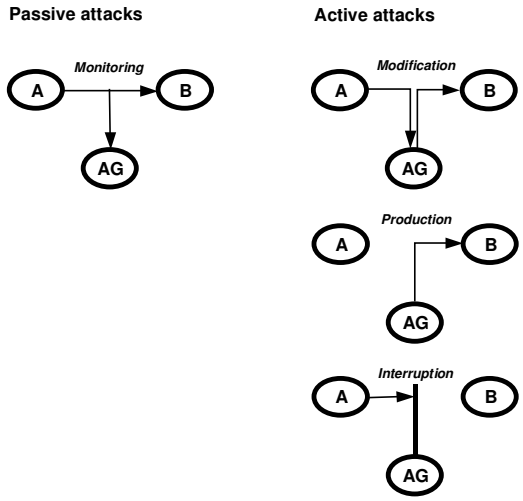

Figure 1: Possible attacks against information systems

As figure 1 shows it is possible to differentiate between passive and active attacks. The passive attack (monitoring), a very important issue in the area of confidential documents, is usually not classified as critical in automation although legal situation might change this. Knowledge about the lighting status of a home for instance will not cause direct damage but might violate a person's privacy. Modification, production and interruption of transmitted data is on the contrary critical, because an aggressor might be able to block the system or to change its behavior.

For a FAN, which is connected to the Internet, four locations of possible attacks must be taken into consideration: the Internet, the connection point (this abstract expression is chosen since it can be a server, firewall, proxy, gateway, etc.), the FAN itself and all the connected machines and devices (see figure 2).

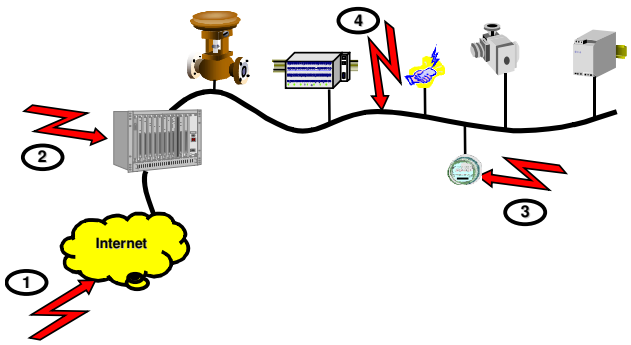

Figure 2: Locations of possible attacks

The problems of the Internet are well known. The established methods of encryption and authentication of data are on a high level ([2],[3]). It is not necessary to elaborate this aspect here. Where as for the Internet part standard solutions exists the protection of the connection point and the FAN heavily depends on the application.
Today's connection points often use no firewall mechanisms at all and limit access to the system by simple username password mechanisms, which are often transmitted in plaintext, too. Newer methods use network traffic security rules of classical firewalls, however, these rules are only based on network addresses (MAC addresses or IP address for instance), and do not consider any "users" or "roles". So-called proxies - another way of connecting two networks - go one step further. They sometimes have the ability to parse ("understand") the used protocols, to authenticate the communication peers as users or roles and to define complex access rules. Proxies separate the two networks and only make public nodes available to the Internet. Any attacks therefore only hit (and probably destroy) the proxy but not the protected node. Furthermore, even if the connection point uses a high security proxy that protects the system from attacks from "outside", attacks from "inside" might still be a threat. The devices themselves should incorporate some security measures as well.

From this point of view the critical points are at least the connection unit and the FAN devices. For this article we want to focus on technical problems. The problem of an insider attack, e. g. done by a fired system administrator, can only be solved by organizational means and will not be tackled directly in this paper, although some security measurement will also help against such attacks. Logging activities might be an approach to prevent and record such insider activities.
The next sections will give an overview of the security means for FANs to protect against attacks from the Internet and attacks from inside of the network, e. g. by malicious nodes ("Trojan horses") or manipulated management messages Such protection becomes more important with extended remote control of FANs. Just imagine manipulated FAN controllers of an HVAC (heating, ventilation and air condition) system or reprogrammed vents that cause extreme damage by transporting the smoke of a small fire somewhere in a bank into security relevant parts of the building. Many other scenarios are imaginable and it is only a question of time, if security aspects will be shunned in the future in the same way.

3 Security in automation networking

We have to keep in mind that an automation system does not only consist of the FAN devices. The source of data (a sensor for instance) is connected to the sink of data (a human) via a number of protocols, interfaces like OPC (object linking and embedding for process control), networks and devices. All of these things must be taken into account do evaluate and to improve the security of a automation system.
.

Traditional systems like the industrial FANs Profibus, Interbus, P-Net and ASI don't have real security mechanisms. Important representatives in building automation are BACnet with a relatively good security approach, and KNX and LonWorks with very limited and low-level security features (details are worked out in [4]). The history of Ethernet-based LANs (Local Area Networks) shows that it usually takes a long time until efficient, secure channels are available. However, we can't see Ethernet alone, as it only covers the lower two layers corresponding to the ISO/OSI seven layer model.
New LAN media like Wireless LANs (WLAN, a.k.a. IEEE 802.11) incorporate security measures like authentication and encryption already in Layer 2, in order to even prevent address spoofing and packet sniffing. Usually, security is implemented in some higher layer (e. g. IPSec, SSL and PGP). However, all parts of the system have to be taken into account.

The focus of this paper is security in home and building automation. Therefore some detailed review of the three main field area networks in this area should be done.

The security part of KNX is based on an APDU rejection mechanism (APDU: Application Protocol Data Unit) in layer 7 with a 4 Byte password. However, the APDUs and the keys are transmitted in plaintext and can be easily recorded by a protocol analyzer. There is no authentication and no encryption service. For small isolated systems the KNX solution can be a good base, if a proxy (see figure 5) will be installed as a link to the Internet, but for big buildings it is definitely not enough.

In LonWorks, authentication services are implemented in layer 4 and 5 and are handled by PDUs. The results are given over to the application layer, which is responsible for rejecting or accepting PDUs and therefore commands. There are various weak spots in the implementation like a secret algorithm for generating the random number, support only for a few communication services and performance issues. In general the LonWorks authentication service is more designed to prevent simple record and playback of commands, rather than to implement a (strong) authentication of sending nodes.

BACnet offers the most advanced security structure of the three investigated systems. It offers various mechanisms and service to provide peer entity, data origin and operator authentication, as well as data confidentiality and integrity that utilize the DES algorithm. The security services usually affect the Application PDUs contents and leave the lower protocol layers unencrypted. In opposite to the above peer orientated systems BACnet introduce a central trusted keyserver that handles the exchange of keys between nodes. The advantage of this approach is that nodes that do not know each other can communicate and that security means can be concentrated on the keyserver. However, the keyserver must be protected against failure and denial of service and will be a primely goal of an attack. The main advantages of BACnet security architecture are that the

concepts are standardized and published and that all commonly needed services are available. Nevertheless, still some problematic areas exists. The BACnet standard leaves the realization of any security measure totally up to the implementer. Therefore especially the generation of keys and random numbers as well as the wrong usage of (session) keys might introduce weak security.

Once such a FAN is connected to the Internet, the connection point is a further location of possible attacks (Figure 3). In literature this unit is described by various terms, e. g. gateway, server or firewall. The respective communication peers (computers, controllers or embedded systems) are interconnected via such connection points or connection units.

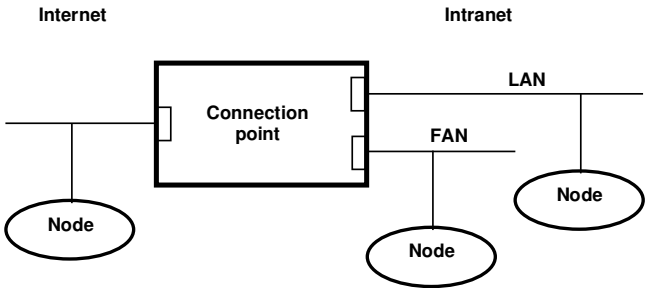

Figure 3: Connection between Internet and intranet

The terms used for the connection unit often describe only a small part of the behavior of the connection unit. Therefore especially the terms gateway, server and firewall must be used carefully:
A gateway on the one hand is defined as device that connects two different networks over all ISO/OSI layers via the application layer or the application. However, the protocol transformation is not the issue here. So, this expression should be avoided in the context of this paper.
A server on the other hand is always to be seen in connection with a client and offers services to the client. Often connection units are between the client and the server, or servers and clients are integrated in the connection unit. So, the server and client describes the communication relationship rather than the device. A firewall at last usually simply filters packets that want to go from one side of the firewall to the other one.
A secure connection unit often includes these aspects in a joint manner. E. g. to inhibit unauthorized access it is not sufficient to filter IP packets (firewall), also the contents of the packets must be authorized (security server) and may be translated (gateway).
Today's connection units can be divided into the following for types:

1. a connection without any firewall service
2. a low level firewall (a router with packet filters)
3. a masquerading firewall and
4. a proxy

A connection without any firewall service allows a path through in any direction at any time and is to be avoided.
The classic firewall is the low-level firewall with a packet filtering router. The base is the implementation of rules, that some connections are allowed, others not. Such a rule could be for example, that it is possible to transmit data from interface A to Interface B to the specified address 192.168.1.3 by http or from interface B to Interface C only for nodes with the Internet addresses 192.168.1.* of the LAN to all addresses of the FAN. The weak point is that intruders can still sniff the network, learn privileged addresses and subsequently spoof them in order to fake their identity.

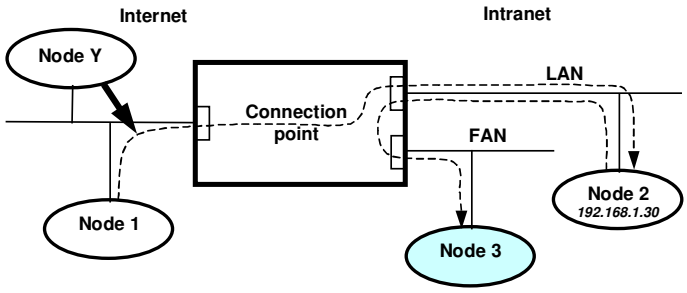

Figure 4: Example of a possible attack

Since such a packet filtering firewall can only grant or deny permissions by analyzing IP address and service number(a.k.a ports, like port 80 for the hypertext transfer protocol http), this concept entirely relies on the correctness of the network addresses, which can be easily manipulated Figure 4 demonstrates such a malicious scenario where node Y spoofs the address of node 1 to introduce malicious code into node 2, which will then start to attack node 3 which was originally protected by the firewall. The above scenario also shows that only packets, that go through the firewall can be filtered. Traffic within the local network cannot be supervised.

A masquerading firewall (a.k.a. Network Address Translation NAT) translates the addresses from one side to the other. No address of the intranet (inside network segment) is visible in the Internet (outside segment). Normally, only the direction from right to left, from intranet to Internet (figure 3) is possible. There is only one possibility for communication from “outside” to “inside”: explicit port forwarding.. It is a pure end-to-end connection, again based on IP addresses that can be faked (only if this open channel is used by a secure protocol like secure shell SSH, one can be assured that port forwarding is not a big security hole). The masquerading firewall perfectly protects internal nodes, but it is very inflexible and insecure when it comes to providing controlled access from outside to inside since in this case it acts like an ordinary packet filtering firewall.

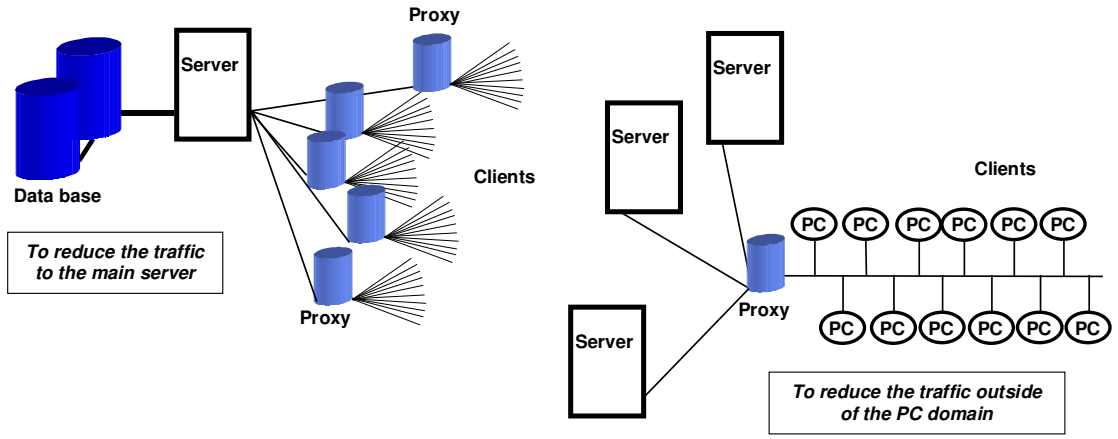

Figure 5: Possible integrations of proxies

Proxies were developed to reduce network traffic between servers and clients. Figure 5 shows common different architectures of proxies. To reduce the load of a server proxies also cache popular requests from clients and the corresponding responses of the server. Such a proxy can easily be used as a very secure firewall. All the data from the intranet is copied as images into the proxy (figure 6), and when a client wants to have some data, it sees the images in the proxy as data of the intranet. So, the clients never have a direct connection to the FAN, which is shielded off by the proxy. Additionally the “internal” nodes do not have direct access to the external network, so malicious code (e. g. viruses) cannot transmit data to the Internet, since any connection to outside demands some user interaction, special permissions and settings and so forth. The most important aspect however, is that modern proxies look “into” the transmitted data packets and are able to parse and understand the contents. Hence the proxy can inhibit communication in the upper layers and allow for instance a group of users access to certain services.

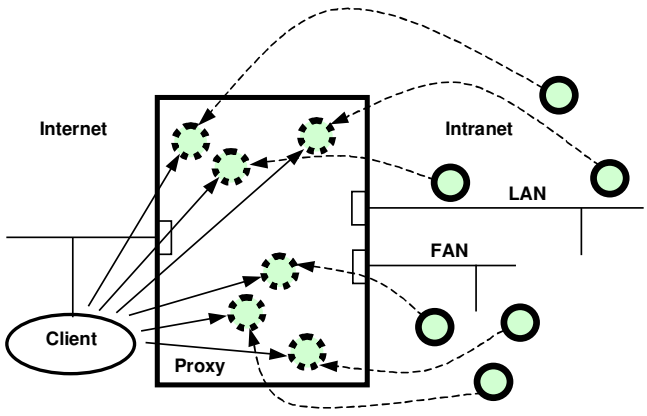

Figure 6: The proxy function

The proxy therefore is a selective mirror for the internal services the nodes offer and the external services from the Internet. The restrictions consist in the fact that

only the explicitly declared services are available, and the therefore the level of security is increased. However, for electronic commerce and other high security domains, a proxy is still not enough: Attacks from inside the FAN are still possible. The example of automated electricity meter reading is therefore vulnerable because the non-trusted user (the customer) is inside.

4 Complex systems

In the former chapters it was explained that the connection to the Internet on the one hand and the FAN itself on the other hand make it necessary to take over security functions. In this sense the question must be faced, if this necessity increase or decrease?

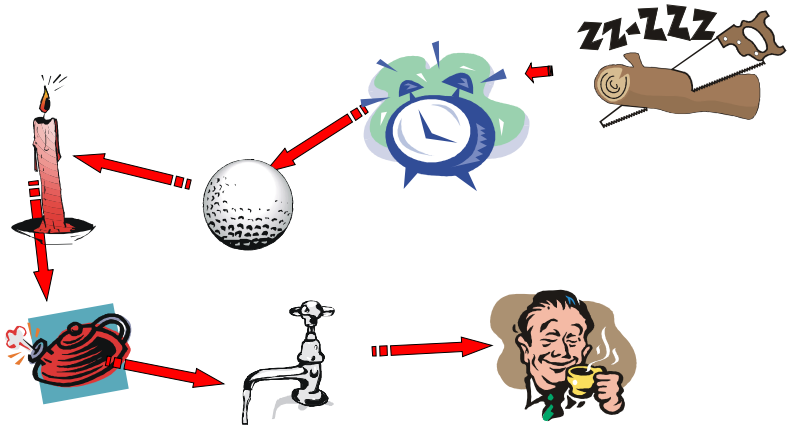

Figure 7: The smart house 30 years ago

About thirty years ago, there was a brilliant film about an intelligent engineer who developed an intelligent house (not called that in those times). One could see him sleeping (figure 7), a mechanical clock rang, a ball fell, which ignited a light, which ignited a stove to heat up the water, and finally the engineer could drink the automatic prepared coffee. What do "automatic systems" mean in this sense? What's behind it? A complete mechanical way of thinking, and that is exactly what we learned in school and university: we learn to linearize, to abstract, to eliminate the right side effects, to separate the different processes, to be able to describe the processes, which we want to control.
Today's approaches exactly tend to do the opposite. We should try to find all dependencies in the process, and to describe them as mathematical algorithms, but it is not necessary to look for closed solutions because we can simulate the whole process, if we have enough sensor data. In this way the two decisive aspects are to look for a lot of different data from many various sensors, and to build up sets of equations and algorithms, with which we feed the computer. In other words: the problems are moved into the computer. In this way the system can be manipulated easier and much more precisely.

That was the idea with fly-by-wire, when the Airbus industry overtook Boeing in the technical sense. And from that time on, one has found similar ideas in all the

different applications, like the controlling of elevators, garage doors and construction cranes. Drive-by-wire, where one will replace the steering column and partly axis for the wheels of a car, is the next step. The result: The necessity for sensors and also for FANs increases dramatically.

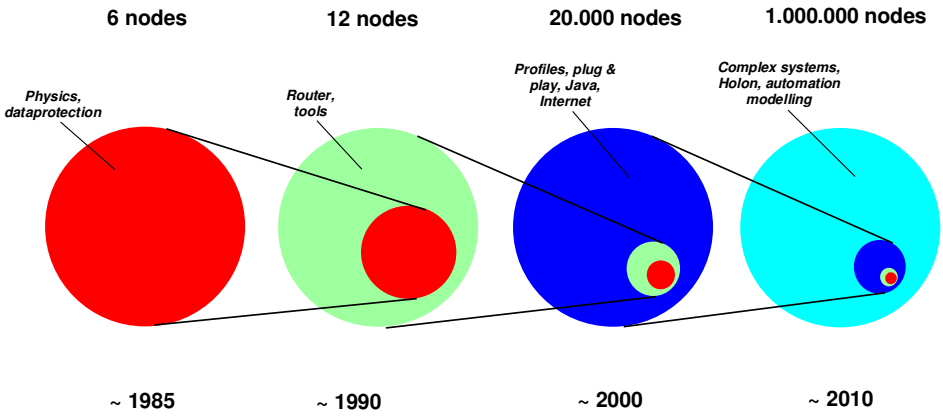

Figure 8: The increasing number of nodes within one system

This is a fact that can also be seen in [10] as figure 8 presents. It is the result of an unrepresentative but interesting analysis: the number of nodes within one system increases dramatically from 6 in 1985 to millions of nodes within the not so distant future and all the different networks will be networked by IP. A huge network with a lot of services will be built up. It will become a complex multilayer system. To handle such a huge network, assembled by a high number of small networks, also new approaches as shown in the next section will be needed.

5 Modern solutions and examples

The discussion shows, that a normal firewall is not enough, because in the Internet (and almost all other networks) it is easy for an intruder to fake IP packets. Traditional masquerading firewalls even have further problems. Connection-less protocols like UDP (user datagram protocol) are typically not supported. Unfortunately UDP is very popular for new IP-based automation protocols like the various flavors of Industrial Ethernet [8]. A better solution is to consider the higher layer protocols instead of trying to make lower layer IP secure. Figure 9 shows a proxy that parses the protocols and separates and protects the internal nodes from the Internet.

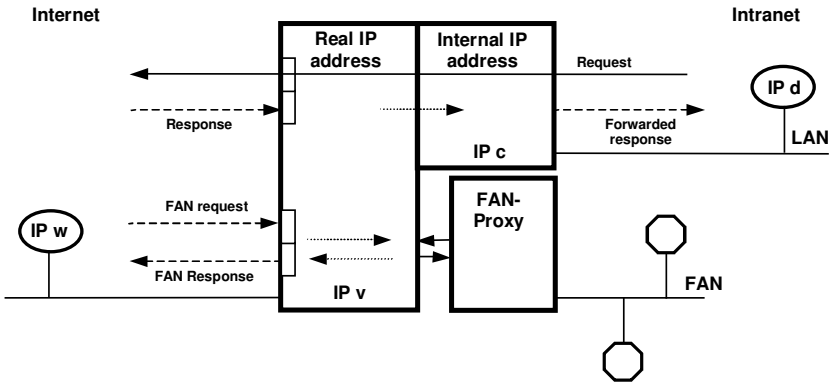

Figure 9: Proposed firewall-proxy solution

Besides the “internal attack” problem, another disadvantage of such systems is that they must to be permanently administered. A system administrator for every home is unthinkable. New concepts are necessary, concepts that offer secure end-to-end connections, where the channel in between can be insecure (Figure 10).

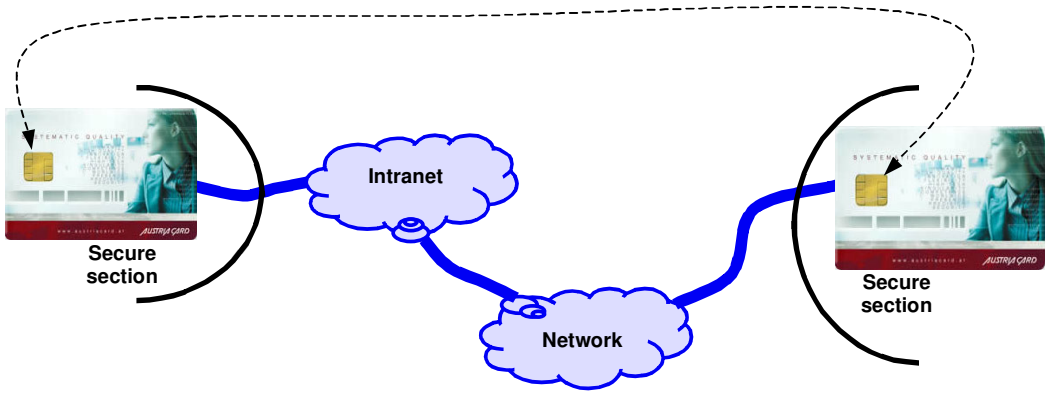

Figure 10: Secure end-to-end-connection

Secure end-to-end connections offer a security level that satisfies the needs of electronic commerce and electronic banking. Neither “the Internet” nor the server, nor the proxy nor the FAN itself can read or manipulate the transmitted data. The remaining risk of this approach is the security of the end system. In payment systems or the GSM system this problem is solved by introducing a security token (smart card), which securely stores secrets (e. g. keys) and execute security procedures (e. g. cryptographic algorithms) tamperproof. Although smart cards are a proven security token, depending on the risk other means like dedicated ASICs (application specific integrated circuit) or especially secured microcontroller could be used. A utility company that wants to read out their energy meters via insecure channels (like the Internet) would need to equip the meters and the meter reading server with such smart cards [9]. The data can be signed and authenticated or even encrypted by the metering smart card and only

be decrypted by the smart card at the company. Such a system would be state of the art for high security applications. The same can be done to secure remote maintenance as shown in Figure 11. The washing machine company should only be able to log into the washing machine and not into other private units in a private home.

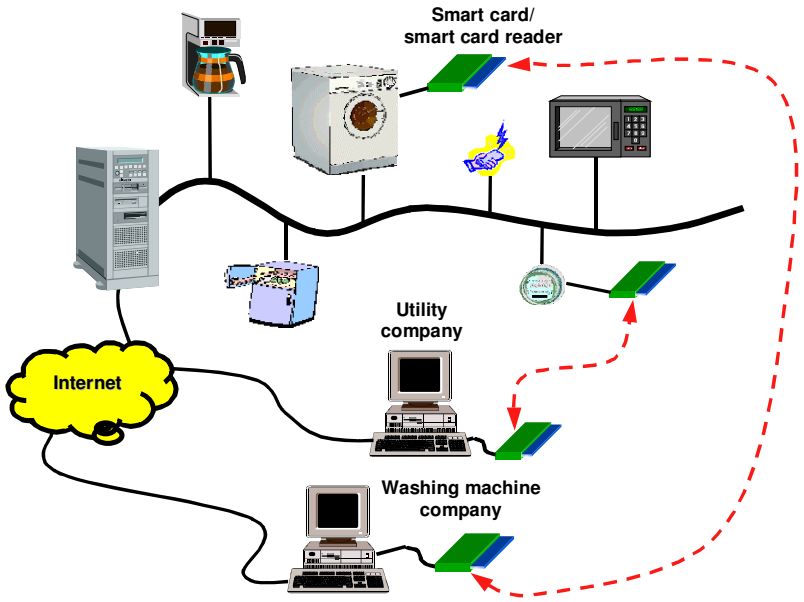

Figure 11: Secure automatic metering and maintenance of a washing machine at homes

Obviously the above system is very cost intensive and might not be necessary for the simple metering problem. Depending on the threats and the security policy different sections of the communication path can be secured in the same way Possible scenarios are to use smart cards only to secure the connection between proxy and the client in the Internet or to secure the connection between proxy an the intranet nodes with smart cards. The first scenario is applicable to normal factory plants where the intranet is physical secure within the plant. The second scenario will more likely apply to systems where the FAN/intranet can be accessed physically by attackers. Last but not least a combination of this methods might be used due to performance issues such as insufficient resources in nodes and organizational reasons.

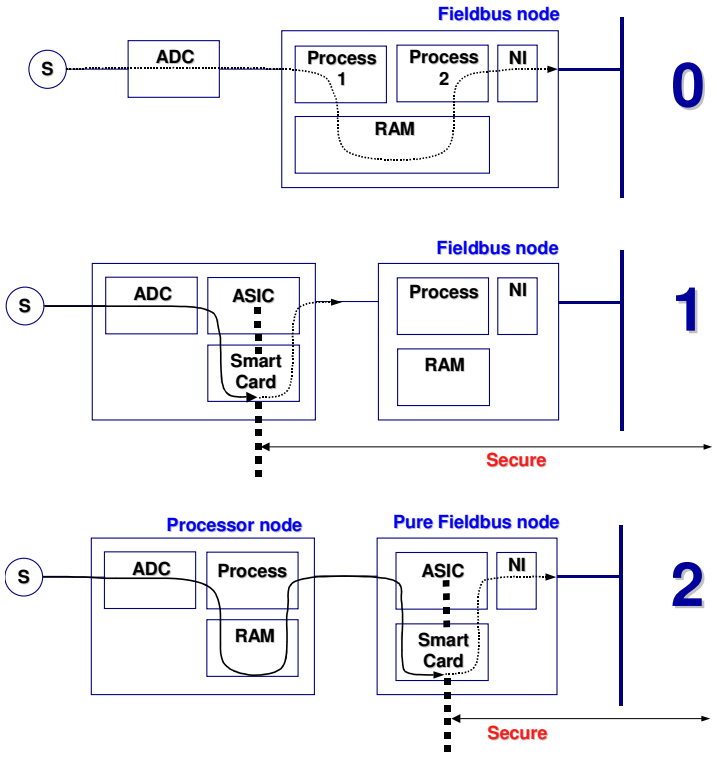

Figure 12: Unsecured (1) and secure (2 + 3) FAN nodes

Securing the information at the FAN node needs special design at the node. In an usual sensor node without encryption and authentication services the information flows through the ADC (analog digital converter) inputs, through the pre-processing stage to the communication process (figure 12, type 1). By using management services of the network all the nodes' memory can be browsed through and even downloaded. In such a way, the node cannot be made secure at all, because every information from input data to secret keys can be read from the nodes memory by a standard network management tool. A security token (smart card) has to be integrated and the node must be securely divided into two units: the sensor-application part and the network part (figure 12, type 2). An ASIC has to be designed in such a way that only encrypted/authenticated data be read from outside.
In this solution the FAN node behaves like a "normal" node relating for example to the network management system. The approach in version type 3 offers more flexibility in the sensor part and offers a more general purpose node, but causes problems with interoperability in standard FAN nodes. It has to be considered that security and interoperability are antagonistic things. To solve this, new concepts have to be introduced to FANs. Problems to be solved are representation of data points, access schemes, key distribution, etc..

6 Conclusion

The paper stated, that the number of nodes (embedded systems) as well as the number of networked networks will increase dramatically. Additionally the

complexity of systems will increase too. The control functions will become increasingly responsible for critical decisions where even human lives could depend on. In this sense, there is no doubt: security will become (and in some areas already is) an important issue in future.
As the paradigm of physical access protection and isolated system changes to networked and remote controlled systems new security means and security policies have to be developed and introduced for all the various applications. In the past, the main advantage of FANs compared to other networks was their sophisticated interoperability, which allows for a technically easy and commercially effective composition of complex systems. Currently, in terms of security, FANs lag behind their competitors, and it is high time to keep up. The combination of interoperability and security will be the next great challenge for field area networks. Besides the main purpose of network security measures - protecting the transmission of data – a further part of security plays an important role for automation networks (and especially building automation networks): access control. Once, a user is authenticated, someone somewhere has to decide what network resources this user is granted access to. Whether these access lists are kept central at one server in the network or whether they are kept in a decentralized manner, the need for such lists is clear. The main goal for such access control systems must be to keep management as simple and efficient as possible. Further research must clarify the requirements and possible solutions to this problem.

[1] Palensky, P. ; Sauter, T. ; Schwaiger, C.: Security und Feldbusse – ein Widerspruch? it&ti, 42 (2000), 4; pp. 31 - 37, 2000.
[2] Stallings, W.: Cryptography and Network Security: Principles and Practice, 3rd edition, Prentice Hall, 2003.
[3] Menezes A., van Oorshot P., Vanstone S.: Handbook of Applied Cryptography, 5th printing, CRC Press, 2001.
[4] Schwaiger, C.; Treytl, A.: Smart Card Based Security for Fieldbus Systems. 9th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA accepted paper, 2003.
[5] Schwaiger C.; Sauter, T.: A secure architecture for fieldbus/ Internet gateways. Proceedings of 8th IEEE International Conference on Emerging Technologies and Factory Automation, pp. 279-285, 2001.
[6] Schwaiger, C.; Sauter, T.: Security strategies for field area networks. Industrial Electronics Society, IEEE 2002 28th Annual Conference of the IEEE, pp. 2915-2920, 2002.
[7] Palensky, P., Sauter,T.: Security Considerations for FAN-Internet connections. Proceedings of the IEEE International Workshop on Factory Communication Systems, Porto 2000, pp. 27-35, 2000.
[8] *Bertoluzzo, M.; Buja, G.; Vitturi, S.:* Ethernet networks for factory automation.

Proceedings of the 2002 IEEE International Symposium on Industrial Electronics, 2002. ISIE 2002., Volume: 1 , 8-11, pp. 175-180, 2002.
[9] Palensky, P., Pratl, G.: Secure and scalable automated meter reading. Proceedings of Domestic Use of Energy Conference, DUE 2003; pp. 233 – 236, 2003.
[10] Dietrich, D.: Evolution potentials for fieldbus systems, IEEE International Workshop on Factory Communication Systems, WFCS 2000 Porto, pp. 145-146, 2000.