DATA SECURITY CONSIDERATIONS IN MODERN AUTOMATION NETWORKS

Mikko Salmenperä
Tampere University of Technology, Institute of Automation and Control
P.O. Box 692, FIN-33101 Tampere, Finland

Jari Seppälä
Tampere University of Technology, Institute of Automation and Control
P.O. Box 692, FIN-33101 Tampere, Finland

Keywords: Data security, increasing complexity, automation services support systems, automation networks, security, telecommunication networks.

Abstract: The automation manufacturing business has reached its turning point and manufacturers are forced to create new business areas. Their expertise about field devices will be the source for future growth of automation industry. This includes monitoring, maintenance, data analysis and process tuning which all require good remoting capabilities in order to be successfully and cost efficiently applied as a service for production plants. This trend builds new challenges for automation services support systems. They are forced to adapt into global business model where customers utilise network connections from old modem lines into modern mobile communication networks. ”Information is power” therefore securing production and other process related information systems in modern automation networks is becoming a necessity. The resent headlines have proven that automation systems are becoming more vulnerable with the inclusion of standard office and Internet technologies into the automation networks. The only way to meet the security challenges in a global scale is to build the the connectivity using secure-by-desing methodology.

1 INTRODUCTION

The current trend for modern automation systems is increased use of networking on all levels of plant. Fieldbusses provide plant floor level networking reaching to individual field devices. Industrial ethernet solutions integrate each fieldbus island into distributed and at the same time centrally controlled automation system. Emerging solutions for automated monitoring and optimisation of field devices, process state and higher level functions such as enterprise resource management require more information to be extracted directly and continuously from the automation system. There is also increasing need to be able to access all of this newly available information remotely by for instance subcontractor providing maintenance for field devices or process optimisation.

The increasing complexity of the automation networks requires a new thinking in security related issues. The mixed usage of intranet, extranet and internet without the full understanding of the required security considerations often results in achieving headlines in local and more often global news. Data security is requirement for prevention of information loss, spying or improper use of automation system. The saying ”Information is power” is clearly applicable to automation related businesses.

The main security threat comes from the same fact as the biggest benefits, integration of different services and systems via protocols common in todays Internet. This means that the security problems common to Internet are also present in the automation networks. It means that most of the methods used to provide data security in Internet are applicable to automation environment. However, the End-to-End security from field device to automation services support systems or end user cannot be found in any available study although standardisation organisations have done considerable work on the area (Webb and et. al., 2004).

This paper presents architecture of a modern automation network and studies possibilities to implement reasonable level of security in it. Common threats to data security in Internet that can also be applied to modern automation environment are also briefly discussed.

Salmenperä M. and Seppälä J. (2004).
DATA SECURITY CONSIDERATIONS IN MODERN AUTOMATION NETWORKS.
In *Proceedings of the First International Conference on Informatics in Control, Automation and Robotics*, pages 279-282
DOI: 10.5220/0001141602790282

2 MODERN AUTOMATION NETWORK STRUCTURE

Automation networks inside a plant are rapidly evolving. The increased data throughput capabilities of fieldbusses and the added intelligence in the field devices themselves provide a foundation on which a new business model can be build. In this model the plant outsources certain routine tasks that support production e.g. plant maintenance or process optimization. The new service providers who take on a responsibility of particular task in several plants, even on a global scale, base their business heavily on telecommunication. By remotely monitoring of automation systems state and various other information systems present at plants, they can optimize usage of materials and personnel and consentrate know-how into service centers.

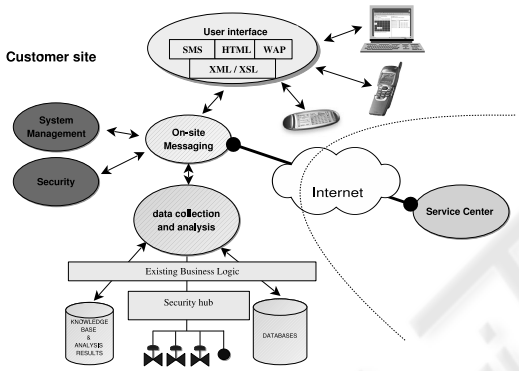

Figure 1: Automation services support system.

Modern automation network has three feature requirements which are connectability, message transfer reliability and loose connectivity. Connectability means interfaces to the various systems. This can be achieved by using messaging and messages within the system that are based on open standards such as XML and SOAP (Haavisto, 2001). The Second requirement is message transfer reliability. All message chains inside, as well as to and from, the system must be reliable and traceable. There are message types that must not be lost under any circumstances. The basis of messaging reliability comes in the form of Message Oriented Middleware (MOM) (Kero, 2004) or products that offer similar functionality. The last but not least requirement is loose connectivity. In modern distributed automation environments customer sites and service providers must not have permanent connection dependencies. Also dynamic binding of services must not occur i.e. you cannot use static IP addresses in any referencing to services as the address spaces tend to change every now and then.

Figure 1 depicts a rough design of how monitoring could be done. In 1 the service center is loosely connected to the customer sites and MOM is used as a backbone of all monitoring operations on the factory and global scale. This kind of a common framework is the essential part of the future automation network.

Security is not a feature requirement - it must be a integrated part of the system (Nikunen et al., 2001). The security is can be divided into three areas: internal, external and devices and services. The last on is actually a subset of the internal security area but is mentioned as separate because of the different nature of the devices and services. The main purpose of the implementation of security is to prevent any unauthorised or improper access to services and to provide a trace both authorised and unauthorised accesses or access attempts.

2.1 TRENDS IN NETWORKED AUTOMATION

The evolving plant automation has resulted in multiprotocol solutions. The Industrial Ethernet is spreading although it has a major problem - it is not a standard rather a collection of incompatible solutions. This seems to be the trend in the fieldbus area. However, there is also a trend to use an IP based monitoring in automation. Some manufacturers have already built switches which operate simultaneously as a traditional fieldbus device and as an IP enabled device. Since automation field is much slower in adapting new technologies it can be safely stated that multiprotocol environments will be the solution for today and for the next five to ten years.

The IP protocol is the source for the most of security problems. The traditional automation protocols are usually not routable and there is a lot less ready made tools for making hacking programs. Without any doubt the biggest problem come from the fact that IP is the protocol for Internet. Anyone can easily find simple and effective tools for hacking into IP based networks. However, since the IP is everywhere and its importance is ever growing, a safe assumption is that automation protocols - most of them anyway - will be routed on top of the IP in the future.

Most of the automation specific protocols are also such that there is no security at all. This is understandable since they were designed for use in closed systems. This means that the security issues must be dealt with on the IP level of the automation network. The actual security problem is not running traditional protocols on the top off the IP. The problem is bringing the IP to the factories.

Business in manufacturing of the automation equipment is not growing so the growth must be found somewhere else. Since the common nominator of many business areas is outsourcing the obvious new

area for automation manufacturers is to sell their automation systems expertise. This consists of maintenance, diagnostics, analysis and tuning (Helanterä et al., 2004). There are usually a few experts on certain area and they are more and more mobile in global scale. Also the customers with their subsidiaries operate globally and are required to interconnect the offices and plants to enable more accurate business tuning. This brings new challenges also to the automation services support systems (ASSS).

Automation services support system have to cope with many different type of network connections. The most challenging part are the mobile connections due to their unreliable and nondeterministic nature. Although the connection to plant is rarely implemented with mobile technologies the devices or device grids are becoming more and more mobile. The ability to take the mobile equipment into remote diagnostics services will be strong asset in the future. The mobility however will bring a totally different problem area to normally local area network (LAN) based automation.

3 SECURITY THREATS

There are several different types of security treats that must be taken into account when considering the data security of the automation network. Valid users themselves are the most common threat any computer system has. Intentional or unintentional misuse of computer systems occurs commonly in every day operation. The system must also be fortified against unauthorised or improper use. This means that each user has strictly defined role in the automation system, and is only allowed to execute operation that correspond to this role. Outside access, meaning access from Internet, is also necessary to implement flexible operating environment for subcontractors and service providers participating in plants production and upkeep. However this access must be very carefully evaluated and controlled as any unauthorised use could lead into catastrophic consequences e.g. loss or theft of valuable information, process malfunction or worse. Computer viruses create a whole new type of data security threat. They can compromise even the best of security, by executing code that allows unauthorised access by some third party. The complete security analysis in networked automation is beyond this paper. More complete study of the are can be found in (Nikunen, 2001).

4 FEASIBLE SOLUTIONS – PERVASIVE-UBIQUITOUS SECURITY

Security design in automation network requires above all careful thinking. The challenges come from various, mostly quite old, field devices. Users and modern intelligent devices are usually not a problem since they have the necessary computing power and interfaces.

Layered security architecture is the obvious choice. This causes some overlapping security in some parts but ensures that also the least capable devices are provided reasonable security. This also provides extra security, if one layer is breached the second layer will hold at least long enough that no important information is lost. In practice this means securing data in message level (OSI model: application layer) as well as in TCP/UDP and IP levels (OSI model: transport and network layers). Message level security with traditional field devices requires deployment of security hubs. The main function of these hubs is, in addition to converting oldish protocols to IP based routable protocols, is to include the security into the communication by securing the messages. This implementation will bring in extra costs but reduces the total cost compared to renewing all field devices into more capable ones.

Solution to reasonable security can be achieved by existing technologies. It is tools and ready made solutions that lacking at the moment. Basis of almost any security mechanism is identity. Without identifying all entities participating in operation of a system, we cannot enforce security. In its simplest this means that we must know who the user, service or device is in order to be able to make proper authorisation decisions, encryption key selection and proper logging of events occurring in the system.

Logging of security events is necessary because of several reasons. It can be used to detect improper use of the system by authorised personnel before security or system operation is compromised. Logging can also be used to track unauthorised use. The system can then be reinforced against this particularattack if necessary. This enables evolving security as new threat are detected. In case of security is ever breached, security logs can be used to determine criticality of the breach. In fact without logging it may well be impossible to ever detect some of the most severe security breaches.

Encryption and signing of data is basic tool for data security. Encryption protects data against unauthorised access and eavesdropping. Signing on the other hand guarantees that the sender is who he claims to be. Both of these methods rely on encryptions keys to achieve their purpose. However they require a feasi-

ble solution to distribution of these keys. Public key infrastructure PKI (Diffie and Hellman, 1976) is an example of such a key distribution method.

PKI in itself is just an architecture, not an implementation. X509 is probably the most notorious and widely used implementation of PKI principles. However it has rather complex and several times extended specification containing a lot of unnecessary features for modern automation network. There is an other PKI based specification, namely Simple Public Key Infrastructure SPKI (Ellison and et al., 1999). SPKI provides an effective and flexible way to implement access control. Example implementation of SPKI in automation network is introduced in (Salmenperä, 2000). When compared to X.509 based certificates SPKI is more light weight and simpler authentication and authorisation mechanisms.

XML has made easier to transfer information from one system to another. Still, as in may cases before, security issues were not included in design from the start. XML in the beginning was just a base on which to build applications. W3.org with help of many other organisations and companies has improved the security by introducing XML Security (W3.org, 2001a) and XML Signature (W3.org, 2001b) frameworks. These has enabled building of open secure remote procedure calls and messaging. Good example of combination of these is Secure Web Services (IBM, 2002). However, these do not solve the problem of key management which still remains mostly a proprietary implementation.

5 CONCLUSION

Despite of security threats and unsolved problem with feasible solution for AAA problem networked automation by support services can be achieved even with current technology. The requirements in short are 1) common sense and 2) inclusion of secure thinking in automation network design.

Mobility will bring new challenges to automation services support systems. The unreliable nature of mobile link in both access and security areas must be taken into account in the design of communication. Only secure-by-design is sufficient enough for mobile environments. Enforcement of best practices and policies are requirement for minimising the unreliable human factor.

Successful implementation of security is always based on standards. Standards define common terminology and enables change of tools if nessessary. Use of open formats are the key to inclusion of all field devices into the automation service support system. XML based messages and Message Orienter Middleware are building blocks for modern automation system and they form a framework that can be applied inside factories and scale well to global analysis and maintenance service applications.

REFERENCES

Diffie, W. and Hellman, M. (1976). New directions of cryptography. In *IEEE Transactions of Information Theory*, pages 644– 654.

Ellison, C. and et al. (1999). SPKI requirements, rfc2692 and rfc2693. http://search.ietf.org/rfc/rfc269[2—3].txt; accessed February 27, 2004.

Haavisto, H. (2001). .NET messaging techniques in condition monitoring network. Master's thesis, Tampere University of Techonology, Automation Department. In Finnish.

Helanterä, H., Salmenperä, M., and Koivisto, H. (2004). Implementing MATLAB® based analysis services in global condition monitoring system. Submitted for ICINCO 2004.

IBM (2002). Web services security (WS-Security). http://www-106.ibm.com/developerworks/webservices/library/ws-secure/; accessed February 27, 2004.

Kero, J. (2004). Advanced messaging in enterprise scale maintenance system. Master's thesis, Tampere University of Techonology, Automation Department.

Nikunen, J. (2001). Security considerations on wide area networking industrial solutions. Master's thesis, Tampere University of Techonology, Automation Department.

Nikunen, J., Salmenperä, M., and Koivisto, H. (2001). Global condition monitoring network. *Automation2001*.

Salmenperä, M. (2000). E-speak in enterprise scale condition monitoring network. Master's thesis, Tampere University of Techonology, Automation Department.

W3.org (2001a). XML Encryption. http://www.w3.org/Encryption/;accessed February 27, 2004.

W3.org (2001b). XML Signature. http://www.w3.org/Signature/;accessed February 27, 2004.

Webb, B. and et. al. (2004). Integrating electronic security into the manufacturing and control systems environment. Technical Report ISA-TR99.00.02-2004, The Instrumentation, Systems, and Automation Society.