THE PERFORMANCE OF OPC-UA SECURITY MODEL AT FIELD DEVICE LEVEL

Olli Post, Jari Seppälä
Department of Automation Science, Tampere University of Technology, Tampere, Finland

Hannu Koivisto
Department of Automation Science, Tampere University of Tecnology, Tampere, Finland

Keywords: OPC-UA, IPSec, Field device security.

Abstract: This paper discusses the performance of OPC UA security model at field device level. Process networks have traditionally been isolated networks but today there is interest to integrate process networks to manufacture and office network. Remote management of field devices via Internet is also gaining interest. This requires implementation of TCP/IP in field devices. However, this causes process networks not being isolated anymore and attention must be paid to the security of process networks. OPC UA is a specification for data transfer in automation systems that can be used to integrate information, horizontally and vertically. Security has also been considered in OPC UA but security measures implemented by OPC UA are too heavy to be uses in field devices. Thus, implementing security profile for authentication without encryption in OPC UA or running OPC UA on IPSec without its own security profile is proposed.

1 INTRODUCTION

Today, there is a growing interest towards the integration of TCP/IP to the process networks. In process networks, security has traditionally been based on access control. Traditional fieldbus based process networks have been isolated networks. Security has been based on restricting physical access. Therefore it has been assumed that there are neither passive nor active attacks in process network. Security measures in isolated process networks have been targeted against user errors. However, this isolation is not the case anymore as TCP/IP is merged to field devices. This allows field devices to be managed over Internet using web applications but this also provides a path for an attacker from Internet to process network using attacks that are well trained in the Internet. It seems that the focus on attacks on automation systems is shifting from internal attacks towards external attacks (Treytl et al., 2005). Still, backdoor accesses such as desktop modems, wireless networks, laptop computers and trusted vendor connections are remarkable sources of attacks (Byres & Hoffman, 2003). The shift can be inflicted because of the path to automation systems that TCP/IP produces. It appears that the external attacks aren't targeted specifically to automation systems but they inflict them as well (Treytl et al., 2005). There is also much interest towards wireless techniques in process network. Controlling access to a wireless media is very hard, if not impossible. Considering these changes in process networks it is clear that the assumption of a secure media in process network is no longer valid. Therefore security against intentional misuse must be considered.

2 SECURITY AT THE FIELD DEVICE LEVEL

2.1 Concepts of Security

Security can be divided into sub concepts and examine security using these sub concepts. These sub concepts are confidentiality, integrity and availability. Confidentiality guarantees the data from unauthorized disclosure, integrity guarantees that data is transferred unaltered in the information

Post O., SeppÃďlÃď J. and Koivisto H.
THE PERFORMANCE OF OPC-UA SECURITY MODEL AT FIELD DEVICE LEVEL.
DOI: 10.5220/0002249103370341
In *Proceedings of the 6th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2009)*, page
ISBN: 978-989-674-000-9

channel. Availability is reachability of data for authorized users.

The confidentiality of the data can be assured by encrypting data, the integrity of data can be assured using hash codes to authenticate data. Availability is more complex concept and any single technique can't assure it. It's also usually reverse requirement compared to confidentiality and integrity. Securing availability requires common practices and techniques to ensure that all the field devices and fieldbus in process network are fully functional continuously.

2.2 Device Level Limitations

The International Society of Automation (ISA, 2004) has defined distinctions between process networks and office networks that create differing requirements for security. Specific features for process network, that are important in the sense, of this paper is that field devices have little resources, unwanted incidents can cause serious damage to property, injuries and even death to people, events in the network are time critical, data and services must be available, integrity of data is very important and that data in process network isn't confidential.

It is a well-known fact that encryption causes much more delay in communication than authentication. For example in IPSec, encryption takes multiple times more time than authentication (Elkeelany et al., 2002). Because the events in the process automation are time critical and data has importance for only short period of time confidentiality isn't a requirement for process network. Availability on the other hand is an important requirement for process network, because missing control or measurement data can inflict serious damage to property and people. Another requirement for process network is integrity of data, because modification of messages and unauthorized messages can also inflict serious damage.

3 MINIMUM REQUIREMENTS FOR FIELD DEVICE LEVEL SECURITY

3.1 Security Requirements for Process Network

The requirements for security in process control are *availability* of data and data *integrity*. However availability in process network can't be guaranteed with just a single technique. It can be assured with security policies and different techniques. Therefore it's out of scope of this paper. As processing time is scarce resource in field devices, requirements for process network, in the sense of this paper, can be compressed to following sentence. In process network, data integrity has to be assured as little process time as possible without endangering the keys used in authentication.

3.2 Processing Time Consumed by Authentication

Processing time consumed by authentication is dependent on the used algorithm and length of the key. Therefore short keys would be better in field device level than longer keys. European Network of Excellence in Cryptology divides algorithms to secure or not secure (ECRPYT) (2008). Key lengths on the other hand, can only be secure enough, because every key is possible to break using brute force. However, it should be noted that if a key is adequate today it doesn't mean that it's still adequate in future. Automation systems can be used even for decades and same cryptographic keys are probably used in process networks from start-up to shutdown. Therefore, it shouldn't be possible to break algorithms and keys during periods between yearly maintenance for decades to come. It isn't possible to concretize this because future is hard to predict but it's not advisable to use algorithms and key lengths defined as not secure.

4 OPC UA

4.1 Introduction to OPC UA

OPC means open connectivity via open standards in industrial automation and the enterprise systems that support industry. OPC UA is the specification that is supposed to integrate data exchange in automation, horizontally and vertically. There are nine other OPC standards that are in use. These specifications are used in different purposes and they all have their own niche. OPC UA on the other hand is suppose to operate in all those different niches and ultimately replace all the other OPC specifications completely. The motivation to start the standardization of this unification was compatibility issues in integration of different specifications. OPC UA responds this by offering a unified interface to be used in all the networks in automation. OPC UA specification is already released and reference models are soon to be ready.

4.2 OPC UA Security Model

The security model of OPC UA is specified in part 2 of the specification by OPC Foundation (2009). This document describes how security can be assured using OPC UA. First, secure channel is established to guarantee confidentially, integrity and application authentication. Second, secure session is established between server and client to guarantee user authentication and authorization. It should be noted that confidentiality is not a requirement at field device level and it consumes more calculation power than integrity.

Security of data transfer in OPC UA is specified in part 4 of the specification by OPC Foundation (2009). Secure data transfer between clients and servers in OPC UA is based on certificates issued by certificate authority (CA). OPC UA client and server both have application instance certificates, which are sent to the other member of communication channel while establishing secure channel. Both parties validate received certificates from CA. After secure channel have been established client starts to establish a session with server by sending its software certificate to server. While application instance certificates identify instances, software certificates identify particular users. Server responds to this request by sending its own certificates and once again both members validate received certificates from CA. Certificates validated in OPC UA are X.509 certificates. In field device level verifying every received certificate from CA would cause significant delay to data transfer. Therefore, due to X.509 hierarchical nature it would be feasible for automation system provider to act as CA. For example PLC could act as CA for all the field devices connected to it.

The security profiles of OPC UA are specified in part 7 of the specification by OPC Foundation (2009). There are three security profiles available in OPC UA: Basic128Rsa15, Basic256 and none. Basic128Rsa15 is a suite of security algorithms that include aes128 for encryption, sha1 for authentication and rsa15 for key wrap. Similarly basic256 includes aes256 for encryption, sha1 for authentication and RsaOaep for key wrap. Security policy none doesn't include any security algorithms. There are also asymmetric equivalents for symmetric algorithms but they are probably too calculation expensive to be used in field device level to guarantee security.

OPC UA Stack is specified in part 6 of the specification by OPC Foundation (2009). OPC UA is located at the application layer in OSI model. In figure 1 is depicted OPC UA stack compared to OSI model. From figure 1 can be seen that OPC UA stack and OSI model overlap. For example transport layer is done again in OPC UA stack. UA Transport Layer establishes session between two entities as does transport layer in OSI model.

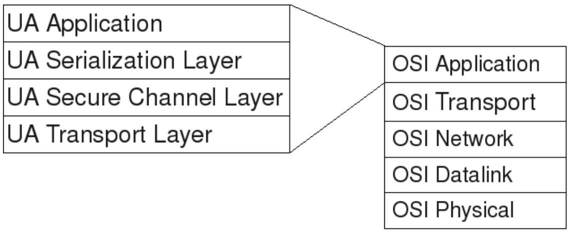

Figure 1: OPC UA stack in OSI model.

5 IPSEC

IPSec is a network layer protocol that can assure data confidentiality and integrity, origin identification and prevent replay attacks (Douligeris et al., 2007). IPSec consists of three elements. First element is security mechanisms. In IPSec there are two of them: authentication header (AH) for authentication and encapsulating security payload (ESP) for encryption. Security mechanisms can also be united to guarantee both encryption and authentication. Second element is security association. This is an agreement on which security mechanisms are used between two members in data transfer. Third element is the infrastructure for key management. It is used to agree an SA between two members.

There are also two modes for transferring data: transport and tunnel. In transport mode ESP mechanism encrypts and optionally authenticates IP payload. AH on the other hand, authenticates payload and also selected portions of IP header. In tunnel mode IP packet is encapsulated inside another IP packet. This way inner IP packet is examined only by the end-points of the data transfer. Thus, data integrity and confidentiality of the whole inner IP packet can be guaranteed.

Another security solution providing data integrity for TCP/IP based field device could be TLS (Dierks & Allen, 1999). It offers the same security as IPSec and it is implemented in common web browsers, which makes it a good choice for remotely configure field devices (Treytl et al., 2004). However, in process network control and measurement data are one-way traffic. There is no need to acknowledge received packets. Data has value for only a short period of time. If a packet is lost on transfer is doesn't matter because another packet is sent shortly after previous. Therefore, there is no need to establish connection between field devices and connectionless UDP would be better solution than TCP. TLS can't be used over UDP but UDP can be packed to IPSec (Alshamsi & Saito, 2005). Thus, IPSec was chosen to under inspection in this paper.

6 PERFORMANCE ANALYSIS

This paper tries to determine whether the security model of OPC UA is efficient in data transfer or could there be another solution for secure data transfer in process network, still allowing OPC UA services to be used.

All three OPC UA security profiles, none, basic128 and basic256, were measured as well as IPSec AH. Also basic128 and basic256 data authentication without encryption were measured. However it should be noted that authentication without encryption is not an OPC UA security profile. By doing also these measurements IPSec AH and authentication done by OPC UA security profiles can be compared. Three packet sizes were used in calculations 1024 bytes, 10 240 bytes and 102 400 bytes to measure delay caused by security measures.

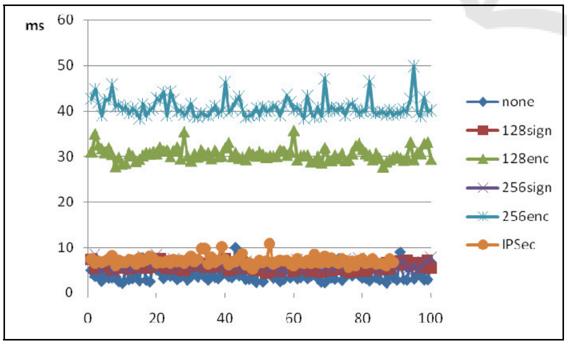

Figure 2: Delay inflicted using 102 400 bytes packet size.

In figure 2 is presented measurements done using packet size 102 400. Although this packet size isn't realistic in field device level it depicts the overall situation well. From figure 2 can be seen that encryption causes much more delay compared to authentication and security profile none. It can be also seen that measurements for all authentication algorithms and security policy none were similar. Therefore it can be said that because confidentiality isn't a requirement in field device level and because encryption adds a lot of overhead to measurement, encryption is not feasible solution to guarantee field device level security.

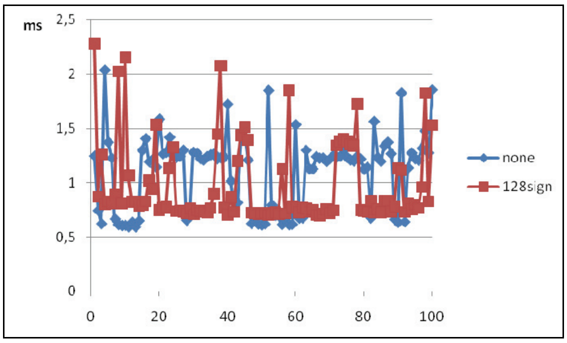

Figure 3: Delay inflicted using packet size 1024 bytes.

In figures 3 and 4 are presented delay inflicted using 1024 bytes packet size. In figure 3 are presented security profile basic128 and none. In figure 4 are presented security profile basic256 and IPSec AH. From figure 3 and 4 can be seen that delay caused by all of these security profiles is alike. It can't be said whether one is better than the other. More measurements are needed for to draw conclusions. However measurements clearly show that in small packet sizes authentication doesn't cause significant delay compared to security profile none.

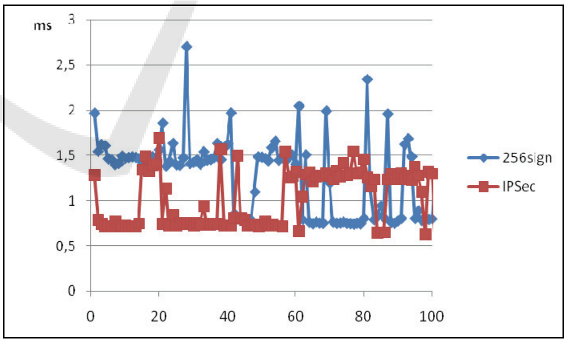

Figure 4: Delay inflicted using 1024 bytes packet size.

7 CONCLUSIONS AND FUTURE WORK

Preliminary results show support the hypothesis that OPC UA security models are not efficient enough to be used in field device level data transfer because there isn't plain authentication supported. Therefore it's suggested that either new security profile for authentication is included or that IPSec is used along OPC UA to guarantee integrity at automation field device level. This way field devices can be remotely managed over TCP/IP and still assure integrity of data efficiently at field device level. Data transfer in OPC UA rests on x.509 certificates. In future it should be considered whether there would be better solution for field device level. For example by PLC acting as CA.

REFERENCES

Alshamsi, A., Saito, T., 2005. A technical comparison of IPSec and SSL. In: IEEE (Institute of Electrical and Electronics Engineers), The 19th International Conference on Advanced Information Networking and Applications. Tamkang, Taiwan 28-30 March 2005.

Byres, E. & Hoffman D., 2003. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. In: ISA (International Society of Automation), Process Control Conference 2003.

Dierks, T. & Allen, C, 1999. The TLS Protocol Version 1.0, Request for Comments: 2246.

Douligeris, C. et al., 2007. *Network Security Current Status and Future Directions*. Hoboken, NJ: Wiley-IEEE Press.

Elkeelany, O,; Matalgah, M.M., Sheikh, K.P., Thaker, M., Chaudhry, G., Medhi, D. & Qaddour, J., 2002. Performance Analysis of IPSec Protocol: Encryption and Authentication. In: IEEE (Institute of Electrical and Electronics Engineers), International Conference on Communications 2002.New York, United States of America 28 April - 2 May 2002.

European Network of Excellence in Cryptology, 2008. Yearly Report on Algorithms and Keysizes (2007-2008) [Online] Available at: http://www.ecrypt.eu.org/ecrypt1/documents/D.SPA.28-1.1.pdf [Accessed 25 March 2009].

International Society of Automation, 2004. ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment

OPC Foundation, 2009. OPC Unified Architecture

Specification, Part: 2 Security Model, Release 1.01

OPC Foundation, 2009. OPC Unified Architecture Specification, Part: 4 Services, Release 1.01

OPC Foundation, 2009. OPC Unified Architecture Specification, Part: 6 Mappings, Release 1.00.

OPC Foundation, 2009. OPC Unified Architecture Specification, Part: 7 Profiles, Release 1.00.

Treytl, A., Sauter, T. & Schwaiger, C., 2004. Security measures for industrial fieldbus systems - state of the art and solutions for IP-based approaches. In: IEEE (Institute of Electrical and Electronics Engineers), IEEE International Workshop on Factory Communication Systems. Vienna, Austria 22-24 September 2004.

Treytl, A., Sauter, T. & Schwaiger, C., 2005. Security measures in automation systems-a practice-oriented approach. In: IEEE (Institute of Electrical and Electronics Engineers), 10th IEEE Conference on Emerging Technologies and Factory Automation. Catania, Italy 19-22 September 2005.