ACE Working Group
Internet Draft
Intended status: Standards Track
Expires: July 20, 2017

M. Wei
QQ. Huang
SY. Li
P. Wang
SD. Zhang
Chongqing University of
Posts and Telecommunications

January 16, 2017

The consideration of OPC UA security in constrained environments
draft-wei-ace-opc-ua-security-00

Abstract

OPC Unified Architecture (OPC UA) is a communication protocol for industrial automation developed by the OPC Foundation. Compared with OPC, OPC UA provides a complete set of security mechanisms to ensure data confidentiality, data integrity and data availability. With the development of industrial internet of things, more and more nodes are expected to be implemented OPC UA, which are resource constrained. This draft discusses OPC UA security mechanisms and the applicability in a constrained environment. An outline of a lightweight security mechanism for OPC UA using in constrained device is proposed.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

With the development of industrialization and information technology, the requirement of information sharing is more and more intense in industrial automation system. However, there are generally a number of equipments from different manufacturers and different information exchange standards in the industrial automation system. It is difficult to achieve interconnection of information. The problem of "Information Island" is easy to cause. In order to achieve cross network and platform communication, OPC foundation proposes an OPC communication protocol. OPC Unified Architecture (OPC UA) [IEC62541] is proposed, which provide a path forward from the original OPC communications model (namely, the Microsoft Windows only process exchange COM/DCOM) to a cross-platform service-oriented architecture (SOA) for process control, while enhancing security and providing an information model.

Multi-platform may implement OPC UA, including portable ANSI C, Java and .NET implementations. With the development of industrial internet of things (IIoT), more and more constrained nodes are expected to be implemented OPC UA in IIoT. The application of OPC UA security mechanisms in constrained environment need to be evaluated. OPC UA Security consists of authentication and authorization, encryption and data integrity via signatures. The authentication uses X.509 certificates exclusively. It relies on the application developer to choose which certificate store the UA application. For instance, it is possible to use the public key infrastructure (PKI) of an Active Directory, which is a challenge for the constrained IIoT field device.

This draft analyses and evaluates the overhead of OPC UA security mechanisms. An outline of a lightweight security mechanism for OPC UA using in constrained device is proposed.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Terms Used

Readers are required to be familiar with the terms and concepts defined in [RFC4949], including "authentication", "authorization", "confidentiality", "integrity", "availability" ,"message authentication code", "verify", etc.

Terminology for constrained environments including "constrained network", "constrained node", "class 1", etc. is defined in [RFC7228].

Implicit certificate: It is a variant of digital certificate, such that a public key can be reconstructed from any implicit certificate, and is said then to be implicitly verified, in the sense that the only party who can know the associated private key is the party identified in the implicit certificate.

2. OPC UA security model

OPC UA security model include three layers: application layer, communication layer and transport layer, as shown in Figure 1. These security layers cover essential data security objectives such as integrity, confidentiality, availability, authorization and authentication. OPC UA is the application layer protocol of OSI model, but the mentioned security layers are different from the OSI model layers.

```
         +---------------------------+           +---------------------------+
         |       OPC UA Client       |           |       OPC UA Server       |
         | +-----------------------+ |           | +-----------------------+ |
         | |   Application Layer   | |           | |   Application Layer   | |
         | | +-------------------+ | |           | | +-------------------+ | |
         | | |User Authentication| | <--Session--> | |User Authentication| | |
         | | |User Authorization | | |           | | |User Authorization | | |
         | | +-------------------+ | |           | | +-------------------+ | |
         | +-----------------------+ |           | +-----------------------+ |
         |                           |           |                           |
         | +-----------------------+ |           | +-----------------------+ |
         | |   Communication Layer | |           | |   Communication Layer | |
         | | +-------------------+ | |           | | +-------------------+ | |
         | | | App Authentication| | |   Secure  | | | App Authentication| | |
         | | | App Authorization | | <--Channel--> | | App Authorization | | |
         | | |   Confidentiality | | |           | | |   Confidentiality | | |
         | | |      Integrity    | | |           | | |      Integrity    | | |
         | | +-------------------+ | |           | | +-------------------+ | |
         | +-----------------------+ |           | +-----------------------+ |
         |                           |           |                           |
         | +-----------------------+ |           | +-----------------------+ |
         | |    Transport Layer    | |           | |    Transport Layer    | |
         | | +-------------------+ | |   Socket  | | +-------------------+ | |
         | | |   Availability    | | <-Connection->| |   Availability    | | |
         | | +-------------------+ | |           | | +-------------------+ | |
         | +-----------------------+ |           | +-----------------------+ |
         +---------------------------+           +---------------------------+
```

Figure 1. OPC UA security mode

In Figure 1, in the application layer, the session provides user authentication and authorization by using a logical connection between OPC UA server and OPC UA client. User authentication can be achieved by username/password, digital certificates or WS-Security token. The authorization for authenticated user depends on the implementation of the OPC UA server by each manufacturer.

The communication layer provides confidentiality, integrity and application authentication. The secure channel is built to ensure real-time data exchanged in security between OPC UA client and OPC UA server in a session. In order to obtain application authentication, the communication layer can use encryption, digital signature and security digital certificate.

The transport layer uses socket connection, here, error recovery techniques are used to maintain the availability of services in transport layer. Therefore, system accessibility is enhanced.

3. The security requirements of OPC UA in constrained environments

The security requirements of OPC UA will be analyzed from the following three aspects.

Firstly, the implementation of OPC UA security is based on traditional public key infrastructure (PKI) technology. However, PKI requires high computation and storage overhead, furthermore, digital certificates management is complex. For constrained node, the storage of certificates and certificate revocation lists increase the storage cost, and the application and revocation of certificates increase the communication cost. When opening a secure channel, the certificate is verified by local or remote certification authorities (CAs). In e-commerce environment, it is very common that a waiting time of 5-10s until the Web server hosting a Web shop has validated the certificate of the customer. However, the waiting time 5-10s is a very long interval for industrial devices located at the field level of the automation pyramid. Industrial applications are featured by many applications, which must be connected to a server for short period of time; furthermore, these applications must access to the server when needed without any delays.

Secondly, the security policies in the OPC UA specification (such as Basic128Rsa15 and Basic256Sha256) are based on RSA public key algorithm. The algorithm is realized by the large prime decomposition problem, which involves a large number of exponential power operations and modulo operations. It has a large number of complex operations, which will seriously affect the real-time requirements of IIoT. Furthermore, the security strength of RSA public key algorithm is guaranteed by the key length. The current technology has been able to decipher 512 bits RSA key in the effective time. Considering the security of the system, the RSA key length must be increased. However, with the increase of RSA key length, the computation will be more and more complex, which will seriously affect the efficiency of the RSA algorithm and the performance of IIoT.

Thirdly, the following scenarios have been considered during performance evaluation of the OPC UA security:

(1) Data exchange with no security mechanisms.

(2) Use of the Secure Channel with no use of certificate.

(3) Use of the Secure Channel with local verification of the certificates.

(4) Use of the Secure Channel with remote validation of the certificates.

According to [CaCh2013], the time overhead required to establish a secure connection is shown below:

For scenarios (1), the time overhead is the least 0.054s, however, scenario (1) has no security functions; For scenarios (2), the time overhead is 0.16s, however, because IT technology is applied to IIoT, scenario (2) can easily be compromised; For scenarios (3), the time overhead is 0.31s, however, scenario (3) is only suitable for small scale; For scenarios (4), the time overhead is 14s, therefore, the scenario (4) has no value for IIoT.

In summary, the implementation of current OPC UA security mechanism in constrained environments is a big challenge.

4. A lightweight security mechanism for OPC UA

In order to deal with OPC UA security requirements in constrained environments, a lightweight security mechanism is proposed as shown in Figure 2. The lightweight security mechanism mainly use implicit certificates and elliptical curve cryptography (ECC), the main reasons are as follows:

Digital certificates can represent a substantial investment, both in infrastructure, memory (to store and manipulate the certificate), and bandwidth (in repeatedly transferring the certificate to various entities). Implicit certificates are smaller and faster than digital certificates. Implicit certificates can enable a low-resource trust model for resource-constrained settings.

ECC is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. Compared with RSA, ECC can obtain the same security performance by using shorter key. Therefore, ECC can establish equivalent security for constrained nodes.

```
               +--------+                              +--------+
               | OPC UA |   --- Implicit Certificate--->    | OPC UA |
               | Client |   <--- Implicit Certificate---    | Server |
               +--------+                              +--------+
                  |                                       |
                  |                                       |
                  v                                       v
          +-----------------+                    +-----------------+
          | Server's public |                    | Client's public |
          |       key       |                    |       key       |
          +-----------------+                    +-----------------+
                  |                                       |
                 ECC                                     ECC
                  |                                       |
                  v                                       v
         +------------------+                    +-----------------+
         |   Symmetric keys |                    |  Symmetric keys |
         +------------------+                    +-----------------+
                  \                                       /
                   \                                     /
                    \Used for signing and encrypting messages/
```

Figure 2. The proposed security mechanism of OPC UA

5. Security Considerations

TBD.

6. IANA Considerations

This memo includes no request to IANA.

7. References

7.1. Normative References

7.2. Informative References

[IEC62541] IEC, "OPC UA, OPC unified architecture, IEC 62541", 2015, <https://webstore.iec.ch/searchform&q=IEC%2062541>.

[RFC2119] Bradner, S.,” Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC2119, March 1997.

[RFC7228] Bormann, C.,” Terminology for Constrained-Node Networks”, ISSN: 2070-1721, RFC7228, May 2014.

[RFC4949] Shirey, R.,” Internet Security Glossary, Version 2”, RFC4949, August 2007.

[CaCh2013] Cavalieri S, Chiacchio F.,” Analysis of OPC UA performances”, Computer Standards & Interfaces, June 2013.

Authors' Addresses

Min Wei
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: weimin@cqupt.edu.cn

QingQing Huang
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: huangqq@cqupt.edu.cn

ShuaiYong Li
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: lishuaiyong@cqupt.edu.cn

Ping Wang
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Phone: (86)-23-6246-1061
Email: wangping@cqupt.edu.cn

ShuaiDong Zhang
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: 18983976906@163.com