Research on security protection of OPC UA PubSub Protocol

Tianyu bu, Xi Li, Jinfeng Huang, Zhigang Sun
College of Computer, National University of Defense Technology, Changsha 410073, China
butianyu14@nudt.edu.cn

Abstract. As a new generation of OPC protocol, OPC UA provides a standardized interoperability solution for industrial automation. In order to accelerate the application of OPC UA in industrial control networks, OPC Foundation published OPC UA PubSub protocol. With the gradual opening of industrial control network, the security risks of deep manufacturing facilities are greatly increased, so it is urgent to study the security protection of PubSub protocol. Based on PubSub protocol, we study the characteristics of its deployment environment and the security threats it faces, and point out the defects and solutions of PubSub protocol's own security protection mechanism. At the same time, we propose a security gateway model OSG, which is established between the field equipment layer and the field control layer, in order to deal with the security risks existing in the PubSub protocol.

1. Introduction
OPC UA is based on next-generation technologies provided by the OPC Foundation to provide secure, reliable, and vendor-independent transmission of raw data and pre-processed information from the manufacturing level to the production planning or ERP level. With OPC UA, all the required information is available to every authorized application, every authorized person, anytime, anywhere. The Server/Client architecture of the OPC UA protocol was applied as an instance standard in some higher-level industrial use cases, but the performance exhibited at the lower level was insufficient to replace the current bus technology. In order to achieve better performance at the industrial control network level, the OPC UA Foundation extends the OPC UA protocol in the new Part 14, defining a new communication pattern based on the Publish/Subscribe communication paradigm to meet the requirements in a many-to-many communication scenario. Based on the characteristics of small flow between the industrial control layer and the industrial equipment layer, this paper effectively protects the industrial control network by setting up a security gateway between the two layers.

This article is based on I2NSF framework proposed a unified security gateway architecture OSG, adopting software defined framework for centralized control, support OPC UA PubSub communication protocol and security protection function, the data plane through the CPU/FPGA implement efficient work with hardware and software, the heterogeneous resources provide a unified programming API user to focus on the core logic development. This paper analyzes the security threats faced by industrial control networks, and then analyzes the security protection function, architecture design and core implementation mechanisms such as NFV and hardware acceleration of OSG.

2. OPC UA PubSub Threats Model
In OPC UA standard version 1.04, the OPC Foundation analyzed the security threats facing OPC UA systems, including the known threats and reconciliation methods in the OPC UA deployment
environment. This paper summarizes the security threats and reconciliation methods of OPC UA PubSub communication mode based on UADP protocol. As shown in Table 1, OPC UA PubSub has a high security attribute, but it still cannot achieve absolute security, and the protection against some attacks is still inadequate. The detailed analysis of security threats is as follows:

1. Denial-of-service attack: Denial-of-service attack includes flood attack and application crash attack. The threat and impact of a flood attack mainly lies in the fact that an attacker can send a large number of data set messages with the goal of breaking down the Subscriber or dependent components (such as CPU, TCP/IP stack, operating system or file system). PubSub message flooding attacks can use either well-formed or ill-formed messages. For well-formed messages, an attacker can be a publisher of a message that is not a member of the SecurityGroup, or a member of it. For malformed messages, an attacker can use a malicious publisher that sends the malformed message to the network and deplete the system's resources. The reconcilable approach to flood attacks is that in PubSub, the subscriber filters the messages it processes based on the header information, allowing it to quickly discard any messages that do not conform to its desired filtering. In addition, the message signature is checked to eliminate any well-formed messages that are not from the required SecurityGroup. The threat and impact of an application crash attack is that an attacker can send special messages that cause an application to crash. This is usually the result of a known problem in the stack or application. These system errors allow the client to issue commands that cause the server to crash. Another possibility is that the server can respond to a valid message by responding to a response that causes the client to crash. An attacker can also be the Publisher whose publication message causes the Subscriber to break. The reconcilable approach to flood attacks is for OPC UA to provide OPC UA's application for authentication. Laboratory testing and authentication involves testing by injecting errors and garbage commands that may detect common failures. OPC base stacks are also fuzzy-tested to ensure that they are resilient to errors. While a certified OPC UA application is not guaranteed to run failure-free, a certified OPC UA application is more likely to be resilient to application crashes resulting from a denial of service attack.

| Threats            | Impacts                  | Reconciliation                  | Weakness                        |
|--------------------|--------------------------|---------------------------------|---------------------------------|
| Denial of Service  | Availability             | Header Filter, Signature        | DoS Attacks with legal packets  |
| Eavesdropping      | Confidentiality,         | Encryption                      | None                            |
|                    | Authentication,          |                                 |                                 |
|                    | Authorization            |                                 |                                 |
| Message spoofing   | Integrity, Authorization | Signature, Check UADP Header    | Legal packets with malicious payload |
| Message alteration | Integrity, Authorization | Signature                       | None                            |
|                    |                          |                                 |                                 |
| Message replay     | Authorization,           | Check UADP Header               | None                            |
|                    | Authentication           |                                 |                                 |
| Malformed Messages | Integrity, Availability | Check UADP Header               | Consume too much resource of the network and device |
| Rogue Publisher    | All except Integrity,    | Signature                       |                                 |
|                    | Non-Repudiation          |                                 |                                 |

2. Eavesdropping attack: The threat and impact of eavesdropping attack mainly lies in the unauthorized disclosure of sensitive information, which may directly lead to serious security holes or be used for subsequent attacks.

The reconciliatory approach to eavesdropping attacks is OPC UA PubSub, which addresses message spoofing threats by providing the ability to sign messages.
Messages can also contain a valid PublisherId, DataSetClassId, timestamp information, network message number, and serial number, which further limits message spoofing.

3. Message substitution attack: The threat and impact caused by message substitution attack mainly lies in that the attacker may capture or modify the network traffic and application layer messages and forward them to the OPC UA Subscriber, and the message change may allow the attacker to access the system illegally. The reconciling approach to message substitution attacks is that OPC UA USES the message signature to counter message changes.

4. Message replay attack: The threat and impact caused by message replay attack mainly lies in that network traffic and effective application layer messages can be captured and re-sent to the OPC UA Subscriber at a later stage without modification. An attacker may cause damage or property damage by incorrectly notifying the user at inappropriate times or by sending a valid command such as opening a valve. The reconciliation approach to message replay attacks is that OPC UA PubSub USES PublishId, DataSetId, and can use the time stamp, network message number, and serial number of the published message. Messages can be signed and cannot be changed without detection, making it difficult to replay messages with all fields enabled. It's worth noting that PubSub allows you to disable fields in messages. Disabling timestamps, network message Numbers, and serial Numbers will allow replay attacks. If you need to consider replay attacks in CSMS, these fields should be enabled.

5. Malformed message attack: The threat and impact of malformed message attack mainly lies in that the attacker can create various messages using invalid message structures (ill-formed XML, SOAP, UA binaries, etc.) or data values and send them to the OPC UA Subscriber. The OPC UA Subscriber may incorrectly handle some of the ill-formed messages by performing unauthorized operations or processing unnecessary information. It can lead to denial or degradation of services, including application termination, or, in the case of an embedded device, a complete crash. In the worst case, an attacker can use malformed messages as a preparatory step to a multilevel attack to access the underlying system of an OPC UA application. The solution to malformed message attacks is to implement the OPC UA application to counter the threat of malformed messages by checking whether the message has the correct form and whether the message parameters are within their legal range. Invalid messages are discarded.

6. Malicious publisher attack: The attacker built a malicious OPC UA publisher or installed an unauthorized instance of a real OPC UA publisher in the system. Rogue Publisher may attempt to masquerade as a legitimate OPC UA Publisher or it may simply appear in the system as a new OPC UA Publisher. The conciliatory approach to the malicious Publisher attack is for the OPC UA Subscriber subscribe application to counter the effect of the Rogue Publisher by validating the signature on the published message.

3. OTG Model
Figure 1 describes the workflow of gateway security protection for OPC UA PubSub system in industrial control network. As shown in the figure, the industrial control network is composed of the field control layer and the field equipment layer, and the communication between the field control layer and the field control layer only adopts OPC UA PubSub mode. Due to the gradual opening of the industrial control network, the risk of invasion on the field control layer equipment is greatly increased. Attackers may attack the fragile field equipment layer with the help of the field control layer equipment, thus causing a great impact on the industrial production. In order to prevent the field equipment layer from being attacked by the field control layer, we set up the gateway between the field control layer and the field equipment layer, and achieve the purpose of security protection of the field equipment layer by conducting security detection and filtering of OPC UA Publish flow from the field control layer.

Control Level
The field control layer usually includes HMI, SCADA, industrial PC, and so on, and there are both OPC UA Publisher and OPC UA Subscriber. For example, HMI sends control instructions to the field device layer as Publisher, and SCADA receives the acquisition information from the field device layer as Subscriber. When the field control layer device ACTS as the Subscriber identity, it is impossible to
develop an attack on the field device layer, but only as the Publisher identity. Therefore, in the figure, all devices that can be used as Publisher identity are abstracted as A host A, and messages are periodically published to the field device layer as Publisher in the whole system. A maintains A Pub_table, which records the Subscriber information Sub (including IP, MAC, subscribed content, etc.), the multicast address M_Cast, and the agreed minimum release period ITV. A is divided into two working states: Safe Scenario in case of no invasion and Attack Scenario in case of invasion. According to the UADP type mapping described in the OPC UA PubSub specification, the message sent by A is divided into three parts. The first part is the header P_H, the second part is the UADP header U_H, and the third part is the UADP Payload U_P payload. Under the Safe Scenario, the message A sends to the field equipment layer is in the Normal state. Under the Attack Scenario, an attacker may launch multiple attacks with the help of A, which are classified into three types of messages sent by the Attack: Illegal, Malicious and DoS. The characteristic of a message of Illegal type is that P_H or U_H is Illegal, that is, there is no published-subscribe relationship in the current PubSub system that satisfies the parameters in P_H or U_H. The packet characteristic of the card type is that U_P is Malicious and that the operations involved in the UADP load exceed the permissions of the corresponding U_H. The DoS type of message features P_H, U_H, and U_P are all legal, almost the same as Normal packets in the security scenario, but with a significant increase in the frequency of publication.

Fig.1 the work process of OTG

Field Level
Field equipment layer usually includes PLC, DCS, sensors, and so on, and there are both OPC UA Publisher and OPC UA Subscriber. For example, PLC uploads the collected information to the field control layer as Publisher, or receives the control parameters from the field control layer as Subscriber. When the field device layer is the Subscriber, it may suffer from the attack from the field control layer Publisher. Therefore, all the devices that can be used as Subscriber identity are abstracted into 2 PLCs in the figure, which are RESPECTIVELY PLC B and PLC C and are connected to the field control layer through the router. B and C, as the Subscriber throughout the system, receive the messages issued by A from the field control layer. B and C maintain a Sub_table table each, and the table records Publisher information Pub (including IP, MAC, PublisherId, etc.), DataSetWriterId data set write module ID DSWId, and the agreed minimum release cycle ITV.

Gateway
As shown in the figure, the gateway is located between the field control layer and the field equipment layer. All messages sent from the field control layer to the field equipment layer need to be processed by the gateway. The figure mainly describes the message detection process of the software layer. The
gateway adopts the architecture of software and hardware co-processing, and the hardware layer is relatively simple, which is mainly responsible for timestamp and message filtering, which is not shown in the figure. The software layer is mainly responsible for attack detection, including message detection and DoS detection. The message detection module detects the message contents, including ACL function and DPI function. The ACL function detects headers, including Header P_H and UADP Header U_H. The ACL function internally maintains ACL tables, whose entries are processing rules that determine the processing action of the message based on the information in the header P_H (quintuple) and the information in the UADP header U_H (PublisherID, DataSetWriterId, etc.). The processing action is divided into three types: D is to drop the action without forwarding and send it to ACL management module; N is to DPI function; P is to DoS detection module. The DPI function detects the load and detects whether the UADP load U_P is malicious according to the parameters in U_H of the UADP header. The DPI function internally maintains the DPI table, and the table entry is the processing rule, which determines the processing action of the message according to the information in the UADP header U_H (PublisherID, DataSetWriterId, etc.) and the information in UADP load U_P (DataSetMessage, etc.). The processing action is divided into two types: D is to drop the action and not forward it, and send it to ACL management module; P is to DoS detection module. DoS detection module USES the DoS detection algorithm proposed in this paper to detect DoS attacks based on OPC UA Publish stream, including delay statistics function and DoS detection function. The delay statistics function is responsible for the statistics of Publish stream delay, collecting and storing the delay of each message, and finally estimating the network delay by using the linear regression method. The delay statistics function is also responsible for issuing the corresponding algorithm parameter configuration to the DoS detection function. DoS detection function is responsible for detecting whether the message published by Publisher will trigger DoS attack due to overfrequency release. If DoS attack is detected, the message will be sent to ACL management module as the attack response mechanism.

**OTG Control Layer**

The control layer maintains a Publish-sub relationship master table PubSub_control_table with entries for information about the Publish-sub relationship via the gateway. PubSub information is divided into five parts, namely, write module Id DSWId for Publisher information Pub, Subscriber information Sub, Multicast information M_Cast, DataSetWriterId data set and the agreed minimum release cycle ITV.

The control layer is responsible for the configuration such as issuing security policy to the gateway of the data layer, including ACL table, DPI table item rules and DoS detection module related parameters (PublisherId, ITV, etc.). At the same time, I was responsible for the configuration of the router in the data layer, and realized the PubSub communication mechanism based on UADP by configuring the routing multicast table.

**OTG Data Layer**

A in the field control layer is in the attack scenario or security scenario, and publishes packets to B and C periodically as Publisher according to Pub_table. The multicast address of the issued message is BC, the destination MAC address is B and C, and the minimum agreed release cycle is 100ms. After entering the gateway, the published message is processed by hardware and enters the software layer. The message first enters the message detection module. The ACL function can detect the illegal type of attack message and the execution action is D. Although it is not possible to detect whether the UADP load is malicious, it is possible to determine whether the load is vulnerable based on the DataSetWriterId in U_H. Generally speaking, if the malicious payload is a data type, it is difficult to have a significant impact on the industrial equipment, because it is difficult for the attacker to grasp the operation logic of the equipment, so it is difficult to launch attacks based on the malicious data. However, if the malicious load is the operation instruction type, it is equivalent to mastering the control authority of industrial equipment, it is easy to launch attacks on industrial equipment, and the impact is more significant. If the DataSetWriterId is an Op type and represents the load as an action instruction type, then the action is N and sent to the DPI function for further processing. If the DataSetWriterId is of type Reg and represents the load as data type, then the action is P, skipping the DPI function and sending it to the DoS detection module for further processing. Next, the message enters the DoS detection module. First, the path
selection module determines whether the message should be sent delay statistics function or DoS detection function. The delay statistics module needs to be trained in advance to configure parameters for DoS detection function in advance. The detection algorithm in DoS detection module is realized by an automaton, which is divided into safe state, critical state and attack state. In the security state, the message needs to enter the delay statistics function, and then enter the DoS detection function. If it is in a critical state, the message goes directly into the DoS detection module. If it is in an attack state, the DoS detection module will link the ACL management module, and the corresponding Publisher will be shielded in the hardware ACL module. There is no case that the message will enter the software again.

After the message comes out from the gateway, it goes to the router, which copies and forwards the message according to the multicast address. In the figure, the router multicast address is BC, the corresponding destination MAC is B and C, and the router copies the message and forwards it to PLC B and PLC C of the field equipment layer respectively.

4. Conclusion
Based on the characteristics of the flow in the field control layer, this paper establishes a security gateway between the field control layer and the field equipment layer to effectively protect the industrial control network. In this paper, a unified security gateway architecture, OTG, is proposed to provide a comprehensive solution that supports multiple protocols and timely protection for the security gateway design of industrial control networks. OTG adopts software-defined architecture for centralized management and control, and realizes efficient co-processing of software and hardware through CPU/FPGA heterogeneous resources on the data plane, and provides unified programming API for users to focus on the development of core logic.

References
[1] German Federal Office for Information Security (BSI). 2017. OPC UA Security Analysis. [Online].https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2.
[2] Polge J, Robert J, Le Traon Y. Assessing the impact of attacks on OPC-UA applications in the Industry 4.0 era[C]/2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2019: 1-6.
[3] Mourtzis D, Angelopoulos K, Zogopoulos V. Mapping Vulnerabilities in the Industrial Internet of Things Landscape[J]. Procedia CIRP, 2019, 84: 265-270.
[4] Neu C V, Schiering I, Zorzo A. Simulating and Detecting Attacks of Untrusted Clients in OPC UA Networks[C]/Proceedings of the Third Central European Cybersecurity Conference. 2019: 1-6.
[5] Srivatsa M, Liu L. Securing publish-subscribe overlay services with eventguard[C]/Proceedings of the 12th ACM conference on Computer and communications security. 2005: 289-298.
[6] Tsien Y L, Gai R L. User Activity Based Application-Layer DoS/DDoS Attack Defense Algorithm[C]/Applied Mechanics and Materials. Trans Tech Publications Ltd, 2015, 742: 693-697.