Active and Passive Combined Identification Approaches for Industrial Control Devices

Jiaxun Fan\textsuperscript{1,2}, Jun Bai\textsuperscript{1,2}, Zhiyao Liu\textsuperscript{3}, Yilu Chen\textsuperscript{1,2}, Chenrui Wu\textsuperscript{1,2}, Zibo Wang\textsuperscript{1,2}, and Bailing Wang\textsuperscript{1,2*}

\textsuperscript{1}School of Computer Science and Technology, Harbin Institute of Technology at Weihai, Weihai 264200, China
\textsuperscript{2}Cyberspace Security Institute, Harbin Institute of Technology, Weihai 264200, China
\textsuperscript{3}China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China

Abstract. Obtaining a complete device inventory is important for securing industrial control systems. For that reason, we developed an industrial control device identification method based on the combination of active and passive approaches. The main tasks of identification method consist of device level identification and specific device information acquisition. Device level identification algorithm, particularly with IP-layer data pre-processing, helps to obtain device types in a passive way, distinguishing between PLCs and non-PLC devices in a short time. After that, we use the active method to further obtain the details of different types of devices. Experimental results verify the effectiveness of this method.

1 Introduction

With increasing devices in industrial control systems are exposed on interconnected network, such as the Internet, more vulnerabilities can be exploited to attack them. One of the first steps required when securing such systems is to obtain a complete device inventory [1]. Therefore, device identification for industrial control systems become a popular research interest in recent years [2-4].

More achievements have been made in the field of device identification for IT systems, mainly including active scanning and passive analysis [5-7]. However, most of them cannot be applied in industrial control systems without modification.

Considering the special facts in industrial control systems, a number of device identification methodologies have been presented until now. Among them, utilizing device fingerprinting plays a core role. Caselli et al. provided a reference model for device fingerprinting and verified it in an industrial environment [8]. With the help of signatures such as data response processing times, the static and low-latency nature in the industrial control networks and physical operation times, Formby et al. proposed two device type fingerprinting methods [9]. Leveraging the stable and persistent control flow communications patterns, Peng et al. presented a fingerprinting method that analysed industrial control protocols [10]. On the contrary, Jeon et al. identified the network port in
supervisory control and data acquisition, and then consecutively inferred the field devices without deep packet inspection for the specific protocols [11].

Compared with the similar work in [12], we further improve the programmable logic controller (PLC) information acquisition method, which also include non-PLC devices.

The main contributions of our work:

(1) Owing to the long-term stable level structure in industrial control systems, the device level identification algorithm proposed, combined with IP-layer data pre-processing, helps to obtain device types in a passive way, distinguishing between PLCs and non-PLC devices in a short time.

(2) For different types of devices, we propose suitable method to further acquire the detailed information. As a result of the time-sensitive feature of PLCs, we analyzed the Ethernet/IP protocol in detail, proposing the format of the detection packet and the parsing method of the return packet. On the other hand, for non-PLC devices, the convention active scanning tools can be directly applied.

2 Device level identification

In this stage, we judge the type of device, such as bottom control device PLC, high level industrial control device based on Windows, Linux or other operating systems, enterprise level device. Device level identification is mainly divided into two parts: data preprocessing stage and level identification stage.

2.1 Data pre-processing

Data preprocessing mainly consists of three sub-stages: IP extraction phase, IP screening phase and IP supplement phase. Data processing phase aims to sieve out redundant data by a series of operations and provide input for coming identification algorithm.

**IP Extraction.** The IP pair contains the interaction logic between devices, which is the basis for judging the device level.

**IP Screening.** The main purpose of this phase is to delete Non-local IP ensuring that all interaction logic (<SRC, DST>) processed by subsequent algorithms is from the target network segment. The basis of this method is that under the condition of normal operation of the system, the interaction traffic between the local network segment IP must be higher than that between the external network segment IP and the local network segment IP.

**IP Supplement.** The fundamental purpose of IP supplement is to solve the problem of incomplete interaction due to incomplete packet capture and the application of multicast technology. The means aims on the IP pair (<SRC, DST>). If there is no corresponding back packet, <DST, SRC>, the supplementary IP pair (<DST, SRC>) will be added to the IP pair set.

2.2 Level identification algorithm

The key purpose of the level identification stage is to classify the device IP in the set according to the IP pairs after pre-processing, so as to provide a basis for identifying the detailed device information in the next step. The common industrial control system architecture model is shown in Fig. 1. Layer A is the control layer, layer B is the process layer, layer C is the enterprise layer. The physical process layer and the public network layer are not represented.
Based on the interaction relationship, it is suggested that the target devices of layer A device are layer A and layer B devices, while the target devices of layer B device are layer A and layer C devices, the target device of layer C is only the layer B device.

Therefore, devices in layer B and C can be distinguished according to the intersection result of IP set of device destination. When the destination IP set of two device IPs is empty, it can be determined that the two IPs must be in layer B or C, not layer A. After obtaining all non-control layer IP, the differential set with all IP sets is used to obtain layer A device IP, and then layer B device and layer C device are determined in turn according to the interaction relationship.

3 Device details probing

In this stage, the main purpose is to choose different detection strategies to detect the industrial control device according to the device type. We can obtain the detailed information of the device, including the IP address of the target device, the open port of the device, device manufacturer, device type, device model, device name, device firmware version, device description information, device support protocol, etc.

3.1 PLC probing

The characteristic PLC device of the industrial control system uses the special industrial control protocol, and is more sensitive to detection than the traditional IT device. Therefore, different detection methods are needed for different types of device in the industrial control system. For PLC device, firstly, we need to determine the type of the protocol. Secondly, we construct a specific data packet according to the protocol, then send a small number of detection packets, so as to obtain the detailed information of the device. The number and frequency of data packets sent are far less than those of a normal probe.

A general detection process will be shown to detect the PLC device based on Ethernet/IP protocol. Ethernet/IP is a modern standard protocol based on the Common Industrial Protocol (CIP). It is packaged to use CIP protocol in Ethernet. The CIP frame of Ethernet/IP encapsulates information including command, data point, message and so on. CIP frame includes four layers: CIP device configuration file layer, application layer, presentation layer and session layer. The rest of the packets are Ethernet/IP frames, through which CIP frames are transmitted over the Ethernet. To detect the Ethernet/IP devices, we need to construct the corresponding query command, and then, through the identify object supported by the CIP protocol, we can obtain the information of the query device.
3.2 Non-PLC device probing

Aiming to gather information for non-PLC devices in Industrial control network, recently some professional methods have already been proposed. Support for port scanning techniques in order to acquire open ports and service information. Moreover, the information about operating system of target device could be obtained via the application of the active or passive fingerprint recognition technology of operating system protocol stack. Additionally, the acquisition of specific service version could be achieved through the banner service information. According to above-mentioned analysis, in the detection of industrial control system intranet non-PLC devices could be identified with the help of Nmap, Masscan or Zmap.

4 Experiment

In the experiment, a safety water treatment system is chosen as a case study to prove the applicability of the algorithm to real data. The system that was built by the iTrust [13] laboratory in Singapore is a water treatment test bed with complete functions, consisting of PLCs, HMI, monitor, history server, engineering station and Enterprise information device.

4.1 Experiment of device level identification

The architecture of safety water treatment system shows that this system has a complete Three-tier Architecture. The real node interaction obtained through the analysis of traffic is shown in Fig.2. The types of nodes in the interaction diagram correspond to that in architecture diagram one by one.

We use (7, 12) to represent the intersection of the destination IP sets of node7 and node12. According to the destination IP set of each node, (7, 12), (7, 13), (7, 14), (11, 14), (8, 12), (9, 14) and (10, 12) is an empty set, and consequently the nodes 7, 8, 9, 10, 11, 12, 13, 14 are correctly evaluated as high-layer nodes. However, due to the lack of standard in the real architecture, (1, 12) also is an empty set, and consequently the node 1 is evaluated as a high-layer device node by mistake, which is a problem to be solved in the future. The 0-layer nodes can be inferred via the difference set of the set of high-layer nodes and the set of total nodes, which are nodes 2, 3, 4, 5, 6. After 0 layer nodes are obtained, determine whether the destination IP set of each node in the high-layer node set includes 0-layer devices, if does, the node is 1-layer device. Similarly, if the destination IP set of node does include 1-layer devices, it is 2-layer device.

According to the above evaluation logic, the target IP of nodes 7, 8, 9, 10, 11 contains 0-layer devices so that they are concluded as 1-layer devices, and the remained nodes 12, 13, 14 are 2-layer devices.
In order to understand the influence of the amount of data on the accuracy of the algorithm, two hours of data were tested in the experiment, and the accuracy of the algorithm was measured via each hour's data is incremented by 10mins in Fig.3. The calculation formula of data accuracy: accuracy = the IP amount of correct evaluation/ the total amount of IP. The test results in Fig. 4. show that with the amount of data increasing, the accuracy stabilizes at around 92% when the data is in more than 30mins, but the accuracy would not improve when the amount of data continues increasing.

**Figure 3.** The accuracy of the algorithm measured by the data in every 10 mins.

**Figure 4.** The accuracy of the algorithm in the situation where the data is incremented by 10mins.

### 4.2 Experiment of device details probing

In order to get the details of the Ethernet/IP device, the List identify device information query request should be firstly sent to the device. The packet was captured between an HMI device and a PLC device. The probing results are shown in Table 1.

**Table 1.** Device information.

| Field           | Value                                      |
|-----------------|--------------------------------------------|
| IP              | 192.168.1.60                               |
| Device Type     | PLC                                        |
| Vendor ID       | Rockwell Automation/Allen-Bradley          |
| Name            | 1756-L71/B LOGIX5571                       |
| Serial Number   | 0x00ac995c                                 |
| Code            | 92                                         |
5 Conclusion and outlook

In this paper, we proposed an industrial control device identification method based on the combination of active and passive approaches. By IP-layer data pre-processing from industrial control traffic, the device level identification algorithm can accurately distinguish between PLCs and non-PLC devices in 30 minutes. Then, we construct probe packets with the proprietary protocol such as Ethernet/Ip for PLCs. The experiment showed that we can further acquire device information with less disturbance for the industrial control network.

This work was supported by the National Key Research and Development Program of China (2018YFB2004200)

References

1. A. Wedgbury & K. Jones, Automated asset discovery in industrial control systems-exploring the problem. ICS-CSR.3, 73-83. (2015)
2. R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices, International Journal of Critical Infrastructure Protection, 7, 114-123. (2014)
3. X. Feng, Q. Li, H. Wang, and L. Sun, Characterizing industrial control system devices on the internet. ICNP, 1-10. (2016)
4. A. Hansson, M. Khodari, and A. Gurtov, Analyzing Internet-connected industrial equipment. ICSigSys, 29-35. (2018)
5. P. Auffret, SinFP, unification of active and passive operating system fingerprinting, Journal in computer virology, 6, 197-205. (2010)
6. E. Bou-Harb, M. Debbabi, and C. Assi, Cyber scanning: a comprehensive survey, IEEE communications surveys & tutorials, 16, 1496-1519. (2013)
7. S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, Gtid: A technique for physical device and device type fingerprinting, IEEE Transactions on Dependable and Secure Computing, 12, 519-532. (2014)
8. M. Caselli, D. Hadžiosmanović, E. Zambon, and F. Kargl, On the feasibility of device fingerprinting in industrial control systems, in International Workshop on Critical Information Infrastructures Security, 155-166. (2013)
9. D. Formby, P. Srinivasan, A. Leonard, J. Rogers, and R. A. Beyah, Who’s in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems. NDSS. (2016)
10. Y. Peng, C. Xiang, H. Gao, D. Chen, and W. Ren, Industrial control system fingerprinting and anomaly detection, International Conference on Critical Infrastructure Protection,73-85. (2015)
11. S. Jeon, J.-H. Yun, S. Choi, and W.-N. Kim, Passive fingerprinting of scada in critical infrastructure network without deep packet inspection, arXiv preprint arXiv:1608.07679. (2016)
12. A. T. Al Ghazo and R. Kumar, ICS/SCADA Device Recognition: A Hybrid Communication-Patterns and Passive-Fingerprinting Approach, IM, 19-24. (2019)
13. iTrust [Online] Available: https://itrust.sutd.edu.sg/.