Journal of Robotics, Networking and Artificial Life
Vol. **6**(**3**); December (2019), *pp.* 157–161
DOI: https://doi.org/10.2991/jrnal.k.191202.008; ISSN 2405-9021; eISSN 2352-6386
https://www.atlantis-press.com/journals/jrnal

Research Article

Evaluation and Build to honeypot System about SCADA Security for Large-Scale IoT Devices

Kuan-Chu Lu[1], I-Hsien Liu[1], Jia-Wei Liao[1], Shao-Chun Wu[1], Zong-Chao Liu[1], Jung-Shian Li[1,*], Chu-Fen Li[2]

[1]*Department of Electrical Engineering, Institute of Computer and Communication Engineering, National Cheng Kung University, Tainan City 70101, Taiwan*
[2]*Department of Finance, National Formosa University, Yunlin County 632, Taiwan*

ARTICLE INFO

Article History
Received 26 April 2019
Accepted 22 May 2019

Keywords
Industrial control systems
honeymap
honeypot

ABSTRACT

Under the trend of intelligent industrial control systems, it is very important to prevent network hackers from invading the system to attack devices. In particular, today's hackers have multiple attacks and the number of attacks has increased year-by-year. How to stop hackers from attacking the system has become the main goal of this research. In this study, we explore how to build and evaluate Arduino and Raspberry Pi were used as real-world programmable logic controllers and camouflaged honeypots to simulate the honeymap of the industrial control system. And simulate the common sensors of industrial control systems, such as temperature, humidity, pressure sensors, to send the same type of signal as the real sensors to deceive the hacker, so the hacker will attack the simulated sensor with a high probability. After receiving the hacker's attack signal, returns the spoofed attack result, which makes the hacker mistakenly think that the attack is successful, and no longer causes further damage to the system, and achieves the purpose of protecting the system. At the same time, record the attack means by honeypot to prevention other similar attacks.

1. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) system [1] is now widely used in many critical infrastructures. With the development of technology, SCADA system has becoming highly intelligent, many devices and instruments can be controlled by machine. For the security of the system, it is particularly important to guard against external network attacks [2]. Nowadays, many preventive mechanisms have been developed [3–5]. However, these methods are usually only effective for external attackers, but they cannot be effectively used for internal attacks, so this study is to propose effective methods to prevent internal attacks. Most of the industrial control systems in the world isolate the internal network from outside. It is for the purpose to prevent attacks from external hackers. However, the internal defense is still very weak. If the hacker invades the internal network through the internal computer, the system could be attacked [6,7], such as Modifying the sensor data will cause the device to be judged to be normal under overload conditions, causing the device to continue to operate abnormally, resulting in damage to the device. In this case, if there is no effective defense mechanism, it will cause great losses.

In order to prevent internal attacks and reduce the chance of equipment being attacked, a honeynet system is built in the internal network, and a large number of honeypots are disguised as Programmable Logic Controllers (hereinafter referred to as PLCs), and a large number of modifications can be made in the installation. Numerically simulate the sensor and use the web page to monitor the condition of all sensors. When attacked by an attacker, the honeypot records the attack information and sends it to the monitoring page, allowing the user to immediately discover it and use the analog sensor to modify the value to trick the attacker. If the attacker attacks the real PLC and modifies the sensor data, there is a certain probability that the analog sensor will be attacked. The user can find out from the monitoring page that the value of the analog sensor is different from the preset analog sensor. It is possible to judge the attack and immediately respond.

2. LITERATURE REVIEW

2.1. Honeypot Introduction

Honeypot is a system that, like honey captures insects to induce an attacker to detect and attack. The purpose is to deploy a fake system that allows attackers to capture, and record and observe while being invaded, so that the attack behavior can be tracked or a new attack mode can be discovered [8]. From a defensive perspective, when we deploy the honeypot to the real host, it increases the time cost of the attacker's detection system host, which in turn increases the buffer space for administrators to react. In addition, before the attacker conducts an attack, it usually performs a scanning action to find the weak point host as the starting point of the attack, and the trapping system can also record the scan [9], so that the manager can find out early and respond to the effectiveness of early warning.

*Corresponding author. Email: ihliu@cans.ee.ncku.edu.tw

2.2. Industrial Control Honeypot

Conpot is a low-interaction honeypot built on the server side, designed for use in industrial control systems. It features easy deployment, modification, and the ability to simulate complex programmable logic controllers such as the SIMATIC S7 series. It also provides a custom human interface service and a complete communication terminal to improve the ability to spoof. Compared with the highly interactive honeypot, although Conpot can achieve less complete information on the attack, compared with the highly interactive honeypot, the actual system simulation is required. Conpot is simulated by the program, and its deployment risk is very low. In this experiment, Conpot was used to deploy honeypots for industrial control [10].

3. EVALUATION AND BUILD TO RESULTS

3.1. Temperature and Humidity Module—DHT22

The temperature and humidity sensor contains a calibrated digital signal output. It devoted to digital module acquisition technology and temperature and humidity sensing technology to guarantee high reliability and excellent sustainable stability. Therefore, the product has the advantages of excellent quality, ultra-fast response, strong anti-interference ability and high cost performance. Each sensor is calibrated in an extremely accurate humidity calibration chamber. The calibration coefficients are stored in the One-time Password (OTP) memory as a program, and these calibration coefficients are called internally during the processing of the detection signal. The single-wire serial interface makes system integration quick and easy. Ultra-small size, extremely low power consumption, and signal transmission distances of up to 20 m make it the best choice for even the most demanding applications. The product is available in a four-pin single-row lead package. For example, the DHT22 sensor specifications are shown in Table 1. The specified range is power, temperature, Humidity measurement range, temperature, humidity measurement accuracy and output signal, etc., will have certain specifications [11]. Table 2 shows the requirements of the DHT22 sensor module connector corner, which defines how each different development version of the pin is connected and as a means of transmission.

Table 1 | DHT22 sensor specifications

Power supply (V)	DC 3.3–5.5
Humidity measure range	0–99.9% RH
Temperature measure range (°C)	−40 to 80
Humidity measure accuracy	±1% RH
Temperature measure accuracy (°C)	±0.2

Table 2 | DHT22 sensor module joint angle

Temperature and humidity sensor module	Development board pin	Comment
DAT	Arduino digital Input pin 2	DHT22 data output pin
5 V	Arduino pin 5 V	5 V anode pin
GND	Arduino pin GND	Common ground pin

3.2. Pressure Sensor—FlexiForce

The Flexiforce Sensor is a piezoresistive type of pressure sensor. Its advantages include a highly linear relationship between load and resistance change. The sensor body is very thin (0.127 mm) and flexible, belonging to a thin-film sense. Measuring component. The main sensing area is located in a circular area with a front end diameter of 9.53 mm. The FlexiForce has a very high linearity when paired with the circuit shown below, so FlexiForce is used in this study as a sensor for measuring pressure and for simulation.

3.3. Setting Industrial Control Honeypot

This research used Ubuntu Mate 16.04 LTS operating system as the Linux environment built by Conpot, and referenced github.com/mushorg/conpot [5] for Conpot construction. After the Ubuntu Mate 16.04 LTS operating system is installed, to open the Ubuntu terminal, you first need to add a new multipath to the /etc/apt/sources.list file. After the installation is complete, enter the following command to execute the conpot. If the installation is successful, you can see the Conpot icon, that is, its masquerading device model appears on the terminal. In this study, the Siemens-S7-200 was used as the device for Conpot masquerading, and the following instructions were executed. As shown in Figure 1, the post-execution screen was completed. When the Conpot was successfully executed, the honeypot was deployed.

After Conpot is installed, it is preset that the attack source will not be recorded. Therefore, it is necessary to modify its profile and enable its record function. Therefore, the attack behavior captured during Conpot execution will be recorded in the Conpot.json file. Among them, after completing the modification of the above profile and creating a new log file, you can try to attack the Conpot. In this study, the socket is connected to the S7Comm port opened by Conpot and the string is transmitted. The result is shown in Figure 2.

4. IMITATE SCADA SYSTEM METHODS

In most industrial control systems, the use of internal and external domain segmentation as a mechanism to prevent attackers from intruding, this method can make it difficult for attackers to invade the internal domain from the external domain [12], thus achieving protection. The purpose of the device, but if the attacker has invaded the internal domain, the device in the internal domain does not have any further defense capability to protect itself. Therefore, in the study, the internal network is added with the honey network to protect the internal network. The security of the device under the domain, and because the attacker has the opportunity to directly attack the real device, modify the data of the actual sensor. Therefore, the simulated sensor signal is added to the real device in the experiment to confuse the attacker, to further protect the safety of system equipment.

In the system architecture, an Arduino is used to simulate a real programmable logic controller, receive the signal from the sensor, and build a Conpot on the Raspberry Pi to deploy the honeypot to disguise the common programmable logic on the market. Controller to capture malicious sources. And use another Arduino to simulate the actual sensor signal such as temperature and pressure, and transmit the plausible data to the programmable logic controller, so that the

```
2018-11-13 23:31:49,046 Fetched ·            as external ip.
2018-11-13 23:31:49,061 Conpot modbus initialized
2018-11-13 23:31:49,062 Found and enabled ('modbus', <conpot.protocols.modbus.modbus_server.ModbusServer object at 0x71ff94b0>) protocol.
2018-11-13 23:31:49,072 Conpot S7Comm initialized
2018-11-13 23:31:49,073 Found and enabled ('s7comm', <conpot.protocols.s7comm.s7_server.S7Server object at 0x721023b0>) protocol.
2018-11-13 23:31:49,080 Found and enabled ('http', <conpot.protocols.http.web_server.HTTPServer object at 0x72102630>) protocol.
2018-11-13 23:31:49,085 Found and enabled ('snmp', <conpot.protocols.snmp.snmp_server.SNMPServer object at 0x721023f0>) protocol.
2018-11-13 23:31:49,092 Conpot Bacnet initialized using the /home/subject/.local/lib/python3.5/site-packages/conpot/templates/default/bacn
2018-11-13 23:31:49,093 Found and enabled ('bacnet', <conpot.protocols.bacnet.bacnet_server.BacnetServer object at 0x72102270>) protocol.
2018-11-13 23:31:49,099 IPMI BMC initialized.
2018-11-13 23:31:49,100 Conpot IPMI initialized using /home/subject/.local/lib/python3.5/site-packages/conpot/templates/default/ipmi/ipmi.
2018-11-13 23:31:49,101 Found and enabled ('ipmi', <conpot.protocols.ipmi.ipmi_server.IpmiServer object at 0x72006730>) protocol.
2018-11-13 23:31:49,110 Class    22/0x0016, Instance   1, Attribute     1 <== [{'class': 22}, {'instance': 1}, {'attribute': 1}]
2018-11-13 23:31:49,112 Class    22/0x0016, Instance   1, Attribute     2 <== [{'class': 22}, {'instance': 1}, {'attribute': 2}]
2018-11-13 23:31:49,113 Class    22/0x0016, Instance   1, Attribute     1 <== [{'class': 22}, {'instance': 1}, {'attribute': 1}]
2018-11-13 23:31:49,116 Class    22/0x0016, Instance   1, Attribute     3 <== [{'class': 22}, {'instance': 1}, {'attribute': 3}]
2018-11-13 23:31:49,117 Class    22/0x0016, Instance   1, Attribute     2 <== [{'class': 22}, {'instance': 1}, {'attribute': 2}]
2018-11-13 23:31:49,118 Class    22/0x0016, Instance   1, Attribute     1 <== [{'class': 22}, {'instance': 1}, {'attribute': 1}]
2018-11-13 23:31:49,119 Found and enabled ('enip', <conpot.protocols.enip.enip_server.EnipServer object at 0x720069b0>) protocol.
```

Figure 1 | Conpot execution screen.

```
[common]
sensorid = default

[virtual_file_system]
data_fs_url = default
fs_url = default

[session]
timeout = 10

[daemon]
;user = conpot
;group = conpot
```

Figure 2 | Conpot's profile.

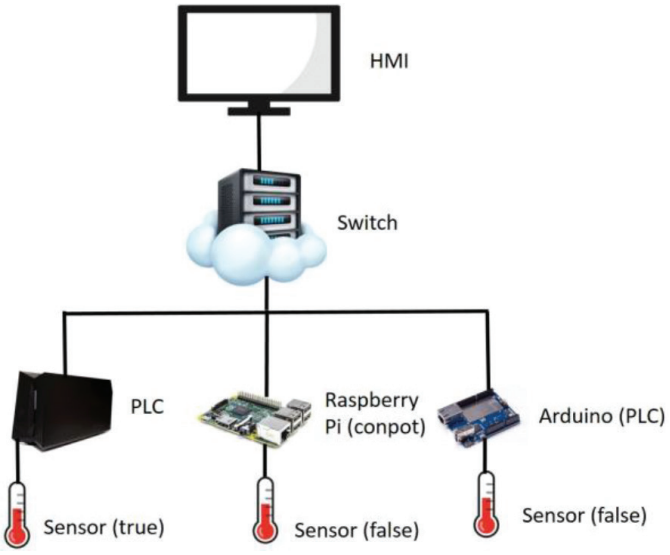

Figure 3 | Basic Conpot structure.

hacker can hardly distinguish the signal generated by the real device, which will cause harm to the system, as shown in Figure 3.

5. CONCLUSION

The number of attacks per year is gradually increasing. However, how to stop hackers from attacking industrial control systems becomes the main goal of this research. This research will explore how to build and evaluate Arduino and Raspberry Pi as real-world programmable logic controllers and camouflaged honeypots to simulate the common sensing devices of industrial control systems, such as temperature, humidity, pressure sensors, to deceive the attacker through the analog mode and the model of the real sensing device, so that the attacker mistakenly thinks that the attack is successful when attacking the device. To achieve the purpose of protecting the system, use the honeypot to record the attacker, and predict that future attackers may use those attack methods to achieve the effect of preventing the attack.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest.

ACKNOWLEDGMENTS

This work was supported by the Ministry of Science and Technology (MOST), Taiwan under contracts numbers MOST 108-2218-E-006-035- and MOST 108-2221-E-006-110-MY3.

REFERENCES

[1] S.A. Boyer, SCADA: supervisory control and data acquisition, 4th edition, International Society of Automation, USA, 2009.

[2] A. Tesfahun, D.L. Bhaskari, A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures, Autom. Control Comput. Sci. 50 (2016), 54–62.

[3] T.C. Pramod, K.G. Boroojeni, M. Hadi Amini, N.R. Sunitha, S.S. Iyengar, Key pre-distribution scheme with join leave support for SCADA systems, Int. J. Crit. Infrastruct. Protect. 24 (2019), 111–125.

[4] D.J. Kang, J.J. Lee, B.H. Kim, D. Hur, Proposal strategies of key management for data encryption in SCADA network of electric power systems, Int. J. Electr. Power Energy Syst. 33 (2011), 1521–1526.

[5] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA security in the light of Cyber-Warfare, Comput. Secur. 31 (2012), 418–436.

[6] B. Miller, D.C. Rowe, A survey SCADA of and critical infrastructure incidents, Proceedings of the first annual conference on research in information technology (RIIT), ACM, Calgary, Alberta, Canada, 2012, pp. 51–56.

[7] R. Masood, Um-e-Ghazia, Z. Anwar, SWAM: Stuxnet Worm Analysis in Metasploit, 2011 Frontiers of Information Technology, IEEE, Islamabad, Pakistan, 2011, pp. 142–147.
[8] D.S.K. Tiruvakadu, V. Pallapa, Confirmation of wormhole attack in MANETs using honeypot, Comput. Secur. 76 (2018), 32–49.
[9] S. Campbell, Supporting digital signatures in mobile environments, WET ICE 2003. Proceedings of the twelfth IEEE international workshops on enabling technologies: infrastructure for collaborative enterprises, IEEE, Linz, Austria, 2003, pp. 238–242.
[10] A. Jicha, M. Patton, H. Chen, SCADA honeypots: an in-depth analysis of Conpot, IEEE conference on intelligence and security informatics (ISI), IEEE, Tucson, AZ, USA, 2016, pp. 196–198.
[11] M. Afzal, Temperature Monitoring With DHT22 & Arduino, 2016, https://create.arduino.cc/projecthub/mafzal/temperature-monitoring-with-dht22-arduino-15b013 (accessed April 18, 2019).
[12] A. Di Pietro, C. Foglietta, S. Palmieri, S. Panzieri, Assessing the impact of cyber attacks on interdependent physical systems, in: J. Butts, S. Shenoi, (Eds.), Critical infrastructure protection VII. ICCIP 2013. IFIP Advances in information and communication technology, Springer, Berlin, Heidelberg, 2013, pp. 215–227.

Authors Introduction

Mr. Kuan-chu Lu

He received his M.S. degree in the Department of Information Management from National Yunlin University of Science & Technology, Taiwan, in 2015. He is working toward the PhD degree in the Department of Electrical Engineering, Institute of Computer and Communication Engineering, National Cheng Kung University. His current research interests are in the areas of Industrial Control System (ICS) and network security.

Dr. I-Hsien Liu

He is a reacher fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and department of electrical engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests are Cloud security, Wireless Network, Group Communication and Reliable Transmission in Mobile ad hoc networks.

Mr. Jia-Wei Liao

He is a B.S. student in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He was born in Taichung, Taiwan, in 1997. He received the B.S. degree in Electrical Engineering from National Cheng Kung University (NCKU), Tainan, Taiwan, in 2019.

Mr. Shao-Chun Wu

He is a B.S. student in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He was born in New Taipei City, Taiwan, in 1997. He received the B.S. degree in Electrical Engineering from National Cheng Kung University, Taiwan in 2019.

Mr. Zong-Chao Liu

He was born in Taoyuan City, Taiwan, in 1994. He received the B.S. degree in Communication Engineering from National Center University (NCU), Taoyuan, Taiwan in 2016, and is studying for the M.S. degree in Computer and Communication Engineering from National Cheng Kung University (NCKU), Tainan, Taiwan, now.

Prof. Jung-Shian Li

He is a full professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in computer science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include wired and wireless network protocol design, network security, and network management. He is currently involved in funded research projects dealing with optical network, VANET, Cloud security and resource allocation, and IP QoS architectures. He is the deputy director general of National Center for High-performance Computing (NCHC), National Applied Research Laboratories. He serves on the editorial boards of the International Journal of Communication Systems.

Prof. Chu-Fen Li

She is an Associate Professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in information management, finance and banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European Journal of Operational Research, Journal of System and Software, International Journal of Information and Management Sciences, Asia Journal of Management and Humanity Sciences, and others.