# Extendable ICS Honeypot Design with Modbus/TCP

**I-Hsien Liu**
*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University*
*No.1, University Rd., East Dist., Tainan City 701401, Taiwan*

**Jun-Hao Lin**
*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University*
*No.1, University Rd., East Dist., Tainan City 701401, Taiwan*

**Hsin-Yu Lai**
*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University*
*No.1, University Rd., East Dist., Tainan City 701401, Taiwan*

**Jung-Shian Li***
*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University*
*No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
*E-mail: ihliu@cans.ee.ncku.edu.tw, jhlin@cans.ee.ncku.edu.tw, hylai@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw**
*www.ncku.edu.tw*

**Abstract**

In order to protect the Cybersecurity of Industrial control system (ICS), we design a prototype of an ICS honeypot. All honeypots are controlled by a server, and using the description file to define honeypot's characteristics, to achieve our honeypot system with scalability and high interaction. We compare our honeypot system and Conpot. the results show that the responses of our honeypot system have more interaction. Even more, our honeypot obtained a perfect score in the honeypot scoring mechanism of Shodan.

*Keywords*: ICS, Honeypot, Cybersecurity, Shodan.

## 1. Introduction

With the advancement of communication technology and network transmission, the Industrial Control System (ICS) [1]is no longer limited to local control in order to improve convenience. The industrial control system has moved from a traditional closed operation mode to an Internet connection environment, making the boundary between Information Technology (IT) and Operational Technology (OT) gradually blurred. Although it has increased convenience and many application possibilities, it is bound to face the challenge of network security, especially in key infrastructure facilities that control water resources, electricity, transportation systems and other important fields that maintain the basic functions of the city. They are often the target of hacker attacks. It is important to understand the attack method and formulate the defense method.

To avoid internal attacks from industrial control systems, we assume that the attacker can enter the internal network, in this paper we take Modbus/TCP protocol [2] as an example. Design a set of extensible description files using JSON (JavaScript Object Notation) [3] format to define the characteristics of a honeypot which disguise as a programmable logic controller (PLC) or other ICS devices. And our honeypot system will attract the attacker's attention, record the entire process communication with the attacker, gather information about the attack, to help develop defense strategies.

## 2. Background

Industrial control system is often widely used in various automated factories and critical infrastructure.In recent decades, to improve the convenience, many industrial control equipment began to support the use of Ethernet, greatly increasing the remote operation and maintenance, but also added a lot of network security hazards.

To understand the attack patterns of attackers, some scholars [7] suggest deploying honeypots on the ICS network to protect the ICS environment.However, with the development of honeypot technology, the attacker's hiding space is oppressed, and the attacker is also in the attack and defense, constantly improve the ability to identify the honeypot, if the fingerprint of the honeypot is mastered by the attacker, the honeypot will not play a substantial role. The Internet of Things search engine-Shodan is a very common and effective tool for identifying honeypots [5] .

### 2.1. *ICS Honeypot*

ICS honeypot attempts to imitate an ICS device, like a programmable logic controller (PLC). It can deceive or trap attackers, build various baiting hosts, network services or simulation scenarios, capture and analyze the attack actions, and understand the attackers.

Conpot is a low-interactive open-source ICS honeypot developed by The Honeynet Project [4]. It is easy to implement and supports many ICS protocols (like Modbus/TCP, S7comm, EtherNet IP, etc.). However, its disadvantage is that its fingerprint features are obvious and easy to be identified by an anti-honeypot technology such as honeypot detection tools or IoT search engine.

### 2.2. *SHODAN IoT Search Engine*

Shodan is an IoT search engine commonly used by attackers to reconnaissance some device on the internet. Shodan have a big threat to the cybersecurity of ICS. It can also check whether it is a honeypot or a real control system by Shodan honeyscore [6]. For example, if a honeypot like Conpot uses a default configuration, Shodan can easily recognize it as a fake system, making the honeypot system worthless.

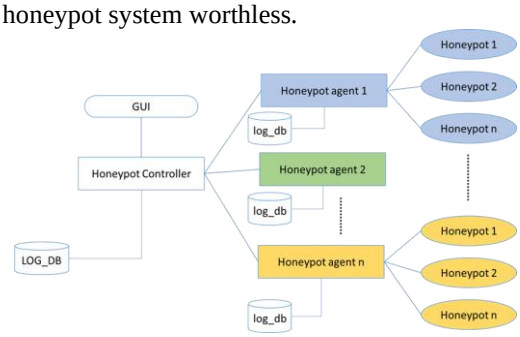


Fig. 1. Honeypot System architecture

## 3. ICS Honeypot System Design

To solve the common problem of lack of interaction in ICS honeypot, this paper tests and observes the network response of real PLC and tries to imitate its response characteristics. The PLC has a register space for storing sensor values or data processing. This numerical information may express the temperature, humidity, and air pressure of the current industrial environment. To increase the degree of reality, the prototype of this honeypot, taking Modbus/TCP as an example, designed a set of description files using JSON lightweight data exchange language as the definition of honeypot characteristics. The description file is the core of the honeypot behavior. It is used to imitate the network response behavior of real industrial control equipment. The description file defines the honeypot IP address, port number, register address and value, response method, etc., for the user can quickly and flexibly configure the honeypot in the industrial control environment.

### 3.1. *System Architecture*

The relationship between the honeypot controller, honeypot agent, and honeypots is shown in Fig. 1., There is a graphical user management interface on the honeypot controller, which can transmit honeypot description file to each honeypot agent, control opening or closing of honeypot in each honeypot agent, and view the honeypot log information, etc.

The honeypot agent parses the description files sent from the honeypot controller, generates the corresponding honeypots according to the feature of the description files and records the visitor information (such as IP address, port number, time, behavior, etc.) in the local database, and finally sends it back to the honeypot controller one by one.

The honeypots are application layer programs in OSI model created by a honeypot agent to open protocol services, which is used to interact with the attacker server honeypot.

### 3.2. *Honeypot Description File Design*

The description file is the core of the honeypot and is the place to define the characteristics of the honeypot. The original idea is that the communication behavior of the equipment in the industrial control environment is simple, and it is often only used to transfer the data between the devices. The communication process is nothing more than HMI reading the sensor value through PLC, or the sensor sending the signal to PLC. Under normal circumstances, the industrial control system flow law, data type is not complex, so it is not difficult to imitate the network communication behavior of industrial control equipment.

After the study of the real industrial control equipment, this paper takes Modbus/TCP, a common protocol in the current industrial control system, as an example, and imitates the surface observed by PLC in the network as the starting point. The simulated items, include PLC equipment model, IP address, port number, address and value of each register, implement of common standard function codes (read or write single or multiple registers), request the implementation of the exception code when an error occurs, and so on.

Finally, the description file is organized into four blocks to simulate the network state of industrial control equipment: Device Info, Pot Type, Default Config, Behavior, and reserve space for expansion fields in each block, can be used to make up for other special undefined conditions.

### 3.3. *Modbus/TCP Implementation Method*

Different from other ICS honeypots, our ICS honeypot not only provides industrial protocol services, but also focuses on improving the authenticity of its responses. According to the specifications of Modbus official document [2], we use Socket to reproduce the honeypot system that supports Modbus/TCP protocol.First, the content of the description file is parsed according to the response mode set by the user, and the honeypot service is opened at multiple sites. The second step is to determine whether it is a Modbus/TCP request. The third step is to determine whether the data is abnormal and whether the data exceeds the interval. These processes Afterwards, it will reply to the attacker based on the response content specified in the description file. If it does not meet the above, it will reply to the attacker's corresponding exception code, and store the log in the database.

## 4. Experiment and Result

We compare the network response differences between the MASTek environmental control model, Conpot, and the prototype of our industrial honeypot system, and using Shodan’s scoring mechanism for honeypots-honeyscore, can Shodan recognize the two honeypots as ICS or honeypot devices?

Then, the results of exploring our honeypot by Shodan can be seen that our honeypot is an equipment of industrial control system in the view of Shodan, and our honeypot can adjust the exposed equipment information on port 502. Using the Honeyscore scoring mechanism of Shodan, and the evaluation result indicated that the honeypot system might be real, and the Honeyscore was 0.3(honeypot would be determined if the Honeyscore was above 0.5).

Similarly, Shodan is used to actively scan Conpot’s IP. The features of Conpot have been completely mastered by Shodan and label it as a honeypot on the industrial control system. In the Honeyscore evaluation, the score even came to 1.0, that is, Shodan is fully confident that it is a honeypot device. In other words, this kind of trap has been difficult to lure an attacker.

## 5. Conclusion

In this paper, a honeypot description file framework was designed to imitate the characteristics of industrial control system’s equipment and implemented by taking Modbus/TCP protocol as an example. Our honeypot system has the characteristics of high expansion. The honeypot agents in different industrial environments can be centrally controlled by one honeypot controller, and more than one honeypot device can be deployed on each agent, which makes it a complete honeynet system.

Our honeypot system compared to Conpot is also very interactive in the network response. The response content is based on the characteristic response defined by description file, which makes it equivalent to the response of real industrial control equipment.
The authenticity of our honeypot system was verified on the Shodan Internet of Things search engine. The results show that our honeypot system can avoid the inspection mechanism of Shodan for ICS honeypot, Shodan label our honeypot system as ICS device. In terms of authenticity, our honeypot system can also perform well.

## Acknowledgements

This work was supported by the Delta Electronics, Inc.' Industry and Academic cooperation project - Design and Prototype of Hybrid Industrial Control System Honeypot and the Ministry of Science and Technology (MOST) in Taiwan.

## References

1. Kevin E. Hemsley, Dr. Ronald E. Fisher, History of Industrial Control System Cyber Incidents, Idaho Falls: Idaho National Laboratory, 2018.
2. ModbusOrganization, "Modbus_Application_Protocol_V1_1b3," 2021. [Online]. Available: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf
3. Wikipedia, "JSON," [Online]. Available: JSON - Wikipedia. [Accessed 26 05 2021].
4. A. Jicha, M. Patton and H. Chen, "SCADA honeypots: An in-depth analysis of Conpot," 016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016.
5. 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, vol. 7, no. 2, pp. 114 - 123, 2014.
6. SHODAN, "Honeypot Or Not?," 2021. [Online]. Available: https://honeyscore.shodan.io/. [Accessed 27 05 2021].
7. Venkat Pothamsetty, Matthew Franz, "SCADA HoneyNet Project: Building Honeypots for Industrial Networks," 2004. [Online]. Available: http://scadahoneynet.sourceforge.net/ [Accessed 27 05 2021].

## Authors Introduction

Dr. I-Hsien Liu

He is a research 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 Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

Mr. Jun-Hao Lin

He received his B.S. degree from the Department of Electrical Engineering, National Taipei University of Technology, Taiwan in 2019. He got the M.S. degree in National Cheng Kung University in Taiwan. His research focuses on network communication and cyber security.

Mr. Hsin-Yu Lai

He received his B.S. degree from the Department of Electrical Engineering, National Chung Cheng University, Taiwan in 2019. He is acquiring the master's degree in Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan.

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 the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.