A Novel IDS Securing Industrial Control System of Critical Infrastructure Using Deception Technology

Shaobo Zhang, Beijing Institute of Technology, China

Yuhang Liu, Peking University, China

Dequan Yang, Beijing Institute of Technology, China*

https://orcid.org/0000-0002-2551-1945

ABSTRACT

The industrial control system (ICS) has become the key concept in the modern industrial world, enabling process monitoring and system control for general industrial systems and critical infrastructures. High-skilled hackers can invade an imperfect ICS by existing vulnerabilities without much effort. Conventional defenses (such as encryption and firewall) to keep invaders away are getting less effective when an attack is carried out by exploiting an array of particular vulnerabilities. Under this circumstance, a new-type intrusion detection system (IDS) based on deception strategy using honeypot technique is proposed, which is of dramatic effectiveness in protecting ICSs of critical infrastructures. In this honeypot-based model, the authors capture malicious internet flows and system operations. They analyze the collected data before alerting and preventing the intrusion alike when it affects the system in the future. This paper deals with the model's concept, architecture, deployment, and what else can be achieved in the field of critical infrastructure cybersecurity (CIC).

KEYWORDS

Critical Infrastructure, Honeypot, Industrial Control System, Intrusion Detection System

INTRODUCTION

Over the past decade, various modern technologies such as the Internet of Things (IoT), Big Data, and Cloud Computing have been terrifically advanced. These significant improvements bring abundant opportunities for industry development and become essential drivers of innovation in industry. As a result, a new industry concept has emerged, the Fourth Industrial Revolution (Industry 4.0) (Schwab, 2017).

As the so-called "Fourth Industrial Revolution" evolving further, industry today has become more intellectual and connective than any other era in history. As a result, Industrial Control Systems (ICSs), designed to focus on system functions rather than the Internet connection and remote distribution, are now migrating from their original isolated networks (usually LANs) to some public environment, such as the Internet. By utilizing the powerful ability of interconnection, ICSs, including Supervisory Control and Data Acquisition Systems (SCADAs) (Gaushell & Darlington, 1987), Distributed Control System (DCS), and other control system configurations like Programmable Logic Controllers (PLC)

*Corresponding Author

(Stouffer et al., 2011), can conduct remote control and instant supervision of the target industrial systems nowadays.

Unfortunately, a variety of cybersecurity challenges has been emerging due to exposing of vital services of ICSs. (Ani et al., 2017) Tight connection of devices and components of ICSs results in high risk in security. Communication of devices perennially exchange vast quantity of safety-critical data through the open air and constantly attract various types of attack. Attackers may manipulate the whole industrial Internet by exploiting vulnerabilities in front-end equipment and sensors, communication networks, and back-end of IT systems (Kumar & Patel, 2014). Once attackers gain the whole or partial access control privileges of the system, there is no doubt that informational and economic loss will be immeasurable. Even people's life security will be in great jeopardy in some severe cases. On December 23, 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company in Ukraine, reported customer service outages. The outages were due to a third party's illegal entry into the company's computer and SCADA systems: some crucial substations were disconnected for three hours. Later statements indicated that the cyberattack impacted additional portions of the distribution grid and forced operators to switch to manual mode. It is said that a foreign attacker remotely controlled the SCADA distribution management system. The outages were initially thought to have affected approximately 80,000 customers. However, later it was revealed that three different distribution companies were attacked, resulting in several outages that caused approximately 225,000 customers to lose power across various areas. (Case, 2016) A typical domino effect of attacks on ICSs has been seen in the event. (Arief et al., 2020)

Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems. As cybersecurity issues have become the primary concern of ICSs, IDSs have become a necessary addition to the security infrastructure of most organizations (Bace & Mell, 2001). Intrusion detection methodologies are classified into three major categories: Signature-based Detection (SD), Anomaly-based Detection (AD), and Stateful Protocol Analysis (SPA). Every one of these types is utilized in different situations. Using the IDSs, the authors can make monitoring the whole security system a much more relaxing work with higher efficiency. In the industrial Internet field, the use of IDSs is commonplace owing to their high quality and low cost.

Along with IDS, the honeypot is another helpful method to perceive unknown attacks and intrusions. As the honeypot is commonly defined as "an information system resource whose value lies in unauthorized or illicit use of that resource", the honeypot is the security resource deception frame up to act like a decoy whose importance resides in getting probed, attacked, or compromised. It contains no sensitive data; however, it pretends to be a valuable portion of the network (Oza et al., 2019). With the help of the deception function of the honeypot, IDSs can be used to collect valuable data from zero-day attacks and other unknown malicious actions in SCADA systems or DCSs. Thus, the authors may be about to stop attacks alike outside our critical infrastructures next time.

To avoid ICS being intruded and make it have confidentiality, availability, non-repudiation, identification, integrity, and logging specifications, necessary actions must be done. As ICS and other industrial Internet is a resource-constrained communication network which largely relies on low-bandwidth channels for communication among lightweight devices regarding CPU, memory, and energy consumption (Heer et al., 2011), traditional security mechanisms such as secure protocols (Gubbi et al., 2013), lightweight cryptography (Cole & Ranasinghe, 2008) and privacy assurance (Pöhls et al., 2014) are no longer suitable to protect the complicated industrial Internet.

In this study, a novel IDS using deception technology solution for ICS and critical infrastructures is proposed to solve the difficulties listed before. The authors deploy a self-developed honeypot system onto several Industrial Control Computers to simulate an actual ICS environment and expose the experiment system to the external Internet. With this well-designed honeypot, the authors successfully collect a large quantity of malicious data generated by different attackers. The system retains the collected data safely and then analyzes it. For our system administrators, they can easily view the

Related Content

The UID Project: Lessons Learned from the West and Challenges Identified for India

Rajarshi Chakraborthy, Haricharan Rengamani, Ponnurangam Kumaraguruand Raghav Rao (2011). *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives (pp. 1-23).*

www.irma-international.org/chapter/uid-project-lessons-learned-west/50710

Benchmarking Steganalysis

Andrew D. Ker (2009). *Multimedia Forensics and Security (pp. 266-290).*

www.irma-international.org/chapter/benchmarking-steganalysis/26997

An Image Region Description Method Based on Step Sector Statistics and its Application in Image Copy-Rotate/Flip-Move Forgery Detection

Likai Chen, Wei Luand Jiangqun Ni (2012). *International Journal of Digital Crime and Forensics (pp. 49-62).*

www.irma-international.org/article/image-region-description-method-based/65736

A Hybrid Intrusion Detection System for IoT Applications with Constrained Resources

Chao Wu, Yuan'an Liu, Fan Wu, Feng Liu, Hui Lu, Wenhao Fanand Bihua Tang (2020). *International Journal of Digital Crime and Forensics (pp. 109-130).*

www.irma-international.org/article/a-hybrid-intrusion-detection-system-for-iot-applications-with-constrained-resources/240653

Copy-Move Forgery Localization Using Convolutional Neural Networks and CFA Features

Lu Liu, Yao Zhao, Rongrong Niand Qi Tian (2018). *International Journal of Digital Crime and Forensics (pp. 140-155).*

www.irma-international.org/article/copy-move-forgery-localization-using-convolutional-neural-networks-and-cfa-features/210142