International Journal of Ambient Computing and Intelligence
Volume 15 • Issue 1

Threat Attribution and Reasoning for Industrial Control System Asset

Shuqin Zhang, Zhongyuan University of Technology, China
Peiyu Shi, School of Computer Science, Zhongyuan University of Technology, China*
Tianhui Du, Zhongyuan University of Technology, China
Xinyu Su, Zhongyuan University of Technology, China
Yunfei Han, Zhongyuan University of Technology, China

ABSTRACT

Due to the widespread use of the industrial internet of things, the industrial control system has steadily transformed into an intelligent and informational one. To increase the industrial control system's security, based on industrial control system assets, this paper provides a method of threat modeling, attributing, and reasoning. First, this method characterizes the asset threat of an industrial control system by constructing an asset security ontology based on the asset structure. Second, this approach makes use of machine learning to identify assets and attribute the attacker's attack path. Subsequently, inference rules are devised to replicate the attacker's attack path, thereby reducing the response time of security personnel to threats and strengthening the semantic relationship between asset security within industrial control systems. Finally, the process is used in the simulation environment and real case scenario based on the power grid, where the assets and attacks are mapped. The actual attack path is deduced, and it demonstrates the approach's effectiveness.

KEYWORDS

Assets, Attribution, Industrial Control System, Reasoning, Threat Modeling

1. INTRODUCTION

With the popularization of industrial Internet of Things and the development of industrial network intelligence (Tsuchiya et al., 2018), the operation and production mode of traditional industries—such as key manufacturing (Chen, 2020), chemical industry, electric power etc. (Alaba et al., 2017)—is gradually updating itself to be more intelligent and informational (Sasaki et al., 2022). Industrial Control System (ICS) is an asset control system used in industrial manufacturing that integrates computer equipment and industrial process control components. The ICS breaks down the notion of isolation inherent in traditional industry and external access (Kumar et al., 2022). The traditional industry did not take security, especially system security, as part of the main design criterion at the beginning (Mi et al., 2021). As the development of ICS networking and information technology (Cruz et al., 2016) are developing, many security protection measures created by network isolation

DOI: 10.4018/IJACI.333853 *Corresponding Author

are increasingly being connected to the network, which may create the risk of exposing ICS security vulnerabilities to hackers (Babu et al., 2017), causing severe economic losses and negative social impact. Threats to asset security in ICS increase along with the level of asset complexity. ICS is involved in almost all aspects of industrial production (AlMedires et al., 2021), and any asset issue could affect the manufacturing and production businesses' ability to continue operations (Zhang et al., 2021), thus causing risks that are out of control. Therefore, how to deal with the behavior of hackers and how to attribute the source of the hacker attacks are the difficulties of today's research. Because of the natural inequality between attack and defense (Su et al., 2022), we must comprehend the asset type and its functions in ICS and take into account all potential threats and attacks in combination with security, so as to judge the impact of the attack on ICS, speculate the attack path of hackers, and ultimately anticipate and respond to hacks in a proactive manner.

Related researchers mainly use three ways to determine ICS security: intrusion detection, security assessment, and system configuration. Intrusion detection is mainly used to achieve prevention by detecting network attacks to avoid being attacked. Bhamare et al. (2020) investigates the applicability of machine learning for anomaly and intrusion detection in ICS but does not take into account the impact on the entire ICS when it is attacked. Security assessment focuses on evaluating system vulnerability prioritization and thus satisfying system security. Qassim et al. (2019) examines the entire network system to ensure system security by identifying a vulnerability assessment methodology in ICS that ensures system security only in terms of vulnerabilities. System configuration focuses on configuring the system for security. AlgoSec (2018) focuses on evaluating cybersecurity policies related to cloud access and implementing them where necessary. This approach focuses more on local security policies. None of the above three approaches consider the impact of a cyberattack on the ICS, and do not consider the diversity of system impacts after being attacked.

In the ICS, the ever-changing ecological environment (Zhang et al., 2019) makes attackers feel in their element. For example, manufacturers often update their software systems for the convenience purpose of users and human-computer interaction ability, but these operations may lead to new vulnerabilities (Knapp et al., 2014), especially those that lack security considerations when considering the initial design (Kriaa et al., 2015). Moreover, the attacker's method and routes are constantly updated, while the defender cannot keep abreast of the latest attack technology and vulnerability information. Therefore, simple intrusion detection, attack attribution and attack prediction cannot perfectly analyze the attack behavior. We need to design a new method to detect and analyze the complex ecological environment of the ICS in time to enhance our knowledge of the threat attack.

Considering the above issues, this paper suggests an ICS threat attribution and reasoning method. Because of the importance of assets in the ICS (Li et al., 2017), this method uses the Purdue model, MITER ATT&CK etc., to describe the asset, and divides the assets into several asset types according to the actual situation of the ICS, thus constructing the ICS's asset type. Then, we use machine learning to analyze the power system attack data set (Koay et al., 2022), which can attribute the source of related attack threats and achieve good results. In this way, it can be learned which part of the ICS has been attacked. Finally, this paper simulates the scenario of the power system attack data set and the real scenario of the attacks on the Ukrainian power grid case (Sullivan et al., 2017). It automatically adds the impact of the ICS or the impact that will be caused after the attack by the attacker through reasoning rules, and finally maps it, which can show the attack path of the attacker.

This paper mainly makes the following contributions:

1. According to the actual situation of ICS, a threat model is constructed, which takes detection, threat, asset, and reality into consideration. And it describes the ICS from the perspective of assets, combines the Purdue model and the actual situation of ICS, puts forward a new concept of asset architecture, constructs an ontology model applicable to the security, and designs six kinds of common inference rules so that it can automatically reason about the system state.