Chapter 14

GENERATING ABNORMAL INDUSTRIAL CONTROL NETWORK TRAFFIC FOR INTRUSION DETECTION SYSTEM TESTING

Joo-Yeop Song, Woomyo Lee, Jeong-Han Yun, Hyunjae Park, Sin-Kyu Kim and Young-June Choi

Abstract  Industrial control systems are widely used across the critical infrastructure sectors. Anomaly-based intrusion detection is an attractive approach for identifying potential attacks that leverage industrial control systems to target critical infrastructure assets. In order to analyze the performance of an anomaly-based intrusion detection system, extensive testing should be performed by considering variations of specific cyber threat scenarios, including victims, attack timing, traffic volume and transmitted contents. However, due to security concerns and the potential impact on operations, it is very difficult, if not impossible, to collect abnormal network traffic from real-world industrial control systems. This chapter addresses the problem by proposing a method for automatically generating a variety of anomalous test traffic based on cyber threat scenarios related to industrial control systems.

Keywords:  Industrial control systems, anomaly detection, traffic generation

1. Introduction

Industrial control systems are used in a variety of critical infrastructure assets such as power plants, waterworks, railways and transportation systems. The security of industrial control systems in the critical infrastructure is a grave concern due to the increased risk of external attacks and the potentially serious impact on operations [7, 23]. Therefore, it is important to develop sophisticated systems that can rapidly and accurately detect anomalous industrial control network behavior due to potential attacks.
Intrusion detection systems, which have been used for decades to detect and respond to abnormal operations in information technology systems and networks, are increasingly used in operational technology infrastructures such as industrial control networks. Intrusion detection systems are classified as misuse detection systems and anomaly detection systems [5]. Misuse detection relies on attack signatures – patterns and characteristics – to identify attacks. Therefore, misuse detection is ineffective against zero-day attacks and clever variants of known attacks. In addition, the massive network flows, diversity of attacks and increasing numbers of new attacks make it difficult for modern misuse detection systems to keep up with the threats.

Anomaly detection relies on deviations from normal usage patterns that are specified or learned. The approach is attractive for use in industrial control networks because of their stable structure, predictable traffic and relatively low traffic volumes [1, 20]. An anomaly-based intrusion detection system learns a statistical model of normal activities, which it compares against data pertaining to current activities in order to detect behavioral abnormalities, including those caused by undetected or zero-day attacks.

The same cyber attack can be executed on different targets at different times and with variations in its content. Depending on the environment, an anomaly-based intrusion detection system may or may not detect the same attack. Therefore, to evaluate the performance of an anomaly-based intrusion detection system, extensive testing has to be conducted using variations of each cyber threat scenario, including the targets, attack timing, traffic characteristics and transmitted content. Unfortunately, due to security concerns and the potential operational impact, it is very difficult, if not impossible, to evaluate cyber threat scenarios on real-world industrial control systems.

A solution to this problem is to use a testbed that models a real industrial control network and the physical infrastructure. The testbed can then be employed to collect normal and abnormal traffic. However, a high-fidelity testbed is expensive to implement and operate; in any case, it would never completely model the actual assets. Additionally, it is infeasible to create and analyze a large number of cyber attack scenarios, especially when each scenario can have numerous variations.

Efforts have been made to collect real-world traffic using honeypots [19], but such traffic does not adequately model real industrial control environments. A possible solution is to generate abnormal industrial control network traffic by modifying normal traffic to model cyber threat scenarios while maintaining the characteristics of the normal traffic to the extent possible. For each cyber threat scenario, the nature of anomalous network traffic varies. Therefore, the characteristics of abnormal traffic could be modified based on the specific points of time, target sessions and characteristics of the cyber threat scenarios, and a number of cases could be generated to perform accurate performance analysis. However, depending on the specific scenario, it may be difficult to manually modify normal traffic based on variants of the cyber threat scenario.