Chapter 11

GENERATING HONEYPOT TRAFFIC FOR INDUSTRIAL CONTROL SYSTEMS

Htein Lin, Stephen Dunlap, Mason Rice and Barry Mullins

Abstract  Defending critical infrastructure assets is an important, but extremely difficult and expensive task. Historically, decoys have been used very effectively to distract attackers and, in some cases, convince attackers to reveal their attack strategies. Several researchers have proposed the use of honeypots to protect programmable logic controllers, specifically those used in the critical infrastructure. However, most of these honeypots are static systems that wait for would-be attackers. To be effective, honeypot decoys need to be as realistic as possible. This chapter introduces a proof-of-concept honeypot network traffic generator that mimics a genuine control system in operation. Experiments conducted using a Siemens APOGEE building automation system for single and dual subnet instantiations indicate that the proposed traffic generator supports honeypot integration, traffic matching and routing in a decoy building automation network.

Keywords:  Honeypots, network traffic generation, industrial control systems

1. Introduction

The United States Ghost Army conducted deception operations in France, Belgium, Luxembourg and Germany during World War II [1]. The mission was to deceive the enemy and lure German units away from Allied combat units. Engineers set up inflatable armored tanks, aircraft, airfields, tents and motor pools. Other tactics such as looping convoy traffic, deploying military police and posting general and staff officers in public places were used to draw Axis resources (e.g., intelligence assets and combat power) away from the real targets. The Ghost Army also played recordings of actual armor and infantry units over loudspeakers. Deceptive radio transmissions were broadcast on fabricated networks called “Spoof Radio.” The Ghost Army leveraged the comprehensive deployment of decoys and deception techniques to overload enemy sensors and intelligence gathering capabilities.

The rights of this work are transferred to the extent transferable according to title 17 § 105 U.S.C.
Deception techniques and decoy technologies are employed in cyberspace in the form of honeypots. These systems may be simple (e.g., virtual machines) or complex (e.g., full-scale replicas of industrial control systems). Limited-scale industrial control system honeypots do not generate traffic that truly represent control systems. Thus, attackers who passively monitor the honeypots may be able to differentiate them from operational systems. Network traffic generators (NTGs) could increase realism and help deceive potential attackers, but they are geared for traditional information technology network performance testing as opposed to creating industrial control system decoys. This chapter introduces a proof-of-concept honeypot network traffic generator that can mimic genuine industrial control systems.

2. Background

Critical infrastructure systems have long been considered immune to network attacks that have plagued traditional information technology systems. Historically, process control and supervisory control and data acquisition (SCADA) systems have relied on proprietary hardware, software and isolation for security. However, the convergence of information technology and operational technology is pushing towards open standards based on Ethernet, TCP/IP and web-based technologies and protocols. According to Gartner [5], operational technology systems are becoming more like information technology systems, including in terms of their vulnerabilities.

The information technology/operational technology convergence introduces several security challenges. Operational technology systems often run software without updates for 15 to 20 years compared with the three to five year lifecycles of information technology systems [23]. Since the 1960s, SCADA system architecture trends show a drastic decline in the use of proprietary hardware from 60% to 2% and software from 100% to 30% [17]. As a result, security practices (e.g., security through obscurity) used in older-generation operational technology systems are no longer applicable to the newer systems [5].

Information technology systems are capable of handling multiple functions and support the addition of third-party security applications. In contrast, operational technology systems are designed to support specific industrial processes and have resource constraints. Adding resources or features to these systems may not be possible because they often lack the memory and/or computing resources to support the enhancements. Implementing traditional information technology security solutions in industrial control systems may also cause timing disruptions and may negatively impact performance and availability [23].

2.1 Control System Threats

Trend Micro [25] has published a study covering attacks on external-facing industrial control devices and honeypot technologies developed to identify threat actors and their motivations behind attacks. The study highlights five activities conducted by attackers: (i) reconnaissance using free and open-source tools