Critical Infrastructure Protection and Security Benchmarks

Guillermo A. Francia III
Jacksonville State University, USA

Xavier P. Francia
Jacksonville State University, USA

INTRODUCTION

In 1997, the President's Commission on Critical Infrastructure Protection published a report, *Critical Foundation*, that studies the critical infrastructure of the United States. The commission defined critical infrastructure as "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and service" (Marsh, 1997). This infrastructure includes the nation's transportation, oil and gas production and storage, water supply, emergency services, government services, banking and finance, electric power, and telecommunications.

Recently, cyber security has become a concern for these systems. The reliance of these systems has progressively evolved from operations that were not formerly computerized to computer based supervisory and control functions such as SCADA (Kroll, 2006). Compromising these computer based supervisory systems may lead to significant damage to these systems which we depend on and even loss of human life (Krutz, 2006).

Experience in securing traditional IT systems cannot simply be applied to industrial control systems (ICS) due to their differing requirements and development; a special set of security metrics is needed for industrial control systems. In this article, we present a literature review of various metrics used to analyze the security posture of an industrial control system. We also cover other concerns on the operations of industrial control systems, including threats and vulnerabilities. We aggregate the information learned from the literature and propose our own set of metrics for measuring security in industrial control systems. This set of metrics is distributed among a proposed set of operational stages for industrial control systems. Finally, we propose an automated system to gather and perform real-time monitoring and visualization for secure operational intelligence applicable to ICS .

BACKGROUND

The increasing network connectivity witnessed in Supervisory Control and Data Acquisition (SCADA) systems raises cyber security concerns for Industrial Control Systems (ICS) facilities. Further, the various and numerous instrumentation and control systems, mingled with external offices and corporate business systems around it, creates a heterogeneous environment that is difficult to monitor and maintain against cyber attack.

General ICS Threats and Vulnerabilities

Threats to industrial control systems (ICS) include "adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders, and natural sources such as from system complexities, human errors and accidents, equipment failures and natural disasters," (Stouffer, 2008). These threats to ICS are described in Table 1.

Policy and Procedure Vulnerabilities

As mentioned by Stouffer (2008), security documentation, such as policies and procedures as shown in Table 2, with management support can reduce vulnerabilities

DOI: 10.4018/978-1-4666-5888-2.ch419

Table 1. Threats to ICS (Stouffer, 2008)

Threat Agent	Description
Insiders	Insiders include disgruntled persons who have unrestricted access to cause damage or steal data.
Phishers	Phishers use spam and spyware to execute phishing schemes in an attempt to steal identities or information for monetary gain.
Spammers	Spammers distribute unsolicited email with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations through denial-of-service attacks.
Spyware/Malware Authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware to generate funds or gather sensitive information.
Industrial Spies	Industrial espionage seeks to acquire intellectual property.
Attackers	Attackers may break into networks for thrill of challenge or bragging rights. Conducting attacks have become easier to use through attack tools and attack scripts and protocols readily available to download from the Internet.
Bot-network Operators	Bot-network operators take over multiple systems to coordinate and distribute attacks, phishing schemes, spam, and malware.
Criminal Groups	Criminal groups use spam, phishing, and spyware/malware to commit identity theft and online fraud for monetary gain.
Foreign Intelligence Services	Several nations are aggressively working to develop information warfare doctrines, programs, and capabilities for espionage activities and disruption of the supply, communications, and economic infrastructures of others.

by mandating the conduct of the organization. If documentation for security is incomplete, inappropriate, or nonexistent, vulnerabilities can be introduced to ICS.

SCADA Vulnerabilities

In *Securing SCADA Systems* (Krutz, 2006), the author outlines the following as major risk elements to SCADA systems:

- Connections to vulnerable networks
- Use of standard hardware platforms or software with known vulnerabilities
- Vulnerable, remote connections
- Real-time deterministic requirements which are used over information security controls that cause communication delays

In the same work, the author also provides valuable steps for risk assessment of SCADA systems.

SPECIFIC ICS PROTOCOL VULNERABILITIES

Vulnerabilities in DNP3

In Patel and Yu (2007), two models are proposed to enhance the security of DNP3. The first model proposes authentication via digital signatures. This model can protect against modification and spoofing attacks. The Master Terminal Unit (MTU) calculates a hash digest using the input stream and encrypts this digest using its private key. Both the key and the encrypted digest are sent to the Remote Terminal Unit (RTU). The RTU then decrypts the digest using the MTU's key and calculates and compares the value of the hash. The second model verifies the identities of the MTU and RTU through the use of a shared secret key.

Vulnerabilities in Modbus

Byres, Franz, and Miller (2004) list vulnerabilities inherent in Modbus. The Modbus protocol lacks confidentiality as the protocol transmits messages in clear text. Furthermore, the protocol lacks integrity because