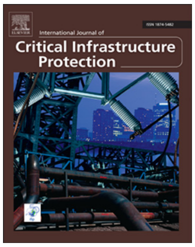
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Detecting anomalous programmable logic controller behavior using RF-based Hilbert transform features and a correlation-based verification process

Samuel J. Stone[a,*], *Michael A. Temple*[a], *Rusty O. Baldwin*[b]

[a]*Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, USA*
[b]*Riverside Research, 2640 Hibiscus Way, Beavercreek, Ohio 45431, USA*

ARTICLE INFO

Article history:
Received 1 April 2013
Received in revised form
8 April 2014
Accepted 12 February 2015
Available online 20 February 2015

Keywords:
Industrial control systems
Programmable logic controllers
RF emissions
Anomaly detection
Hilbert transforms

ABSTRACT

Industrial control systems are used to operate critical infrastructure assets in the civilian and military sectors. Current industrial control system architectures are predominantly based on networked digital computers that enable reliable monitoring and control of critical functions via localized and distributed operations. Many industrial control systems, in particular, supervisory control and data acquisition (SCADA) systems, implement monitoring and control using programmable logic controllers, which have served as gateways through which cyber attacks have been orchestrated against high-profile industrial control system targets.

This paper focuses on securing the programmable logic controller gateway against unauthorized entry and mitigating attack risks by (i) adopting a previously demonstrated capability that provides hardware device discrimination using information extracted from intentional radio frequency (RF) emissions; and (ii) adapting the RF-based verification methodology to exploit information in unintentional programmable logic controller emissions to detect anomalous operations and enhance industrial control system security. Operational status verification (normal operation versus anomalous operation) is demonstrated using emissions from 10 like-model programmable logic controllers. The correlation-based verification approach with Hilbert transform features demonstrates superior performance than with untransformed time domain features. Experimental results demonstrate that an arbitrary equal error rate (EER) benchmark ($\text{EER} \leq 10\%$) is achieved for all programmable logic controllers with a signal-to-noise ratio (SNR) of 5.0 dB when Hilbert-transformed features are used for complete programmable logic controller program scans or SNR=0.0 dB when each programmable logic controller program operation is compared independently. This benchmark was not achieved for any programmable logic controllers when untransformed time domain features were employed.

Published by Elsevier B.V.

[*] Corresponding author.
E-mail address: samuel.stone@afit.edu (S.J. Stone).

http://dx.doi.org/10.1016/j.ijcip.2015.02.001
1874-5482/Published by Elsevier B.V.

1. Introduction

Modern digital computing technology provides industrial control systems with unprecedented levels of monitoring, automation and control of infrastructures ranging from waste water treatment facilities to nuclear power plants in the civilian and military sectors. Industrial control systems use networked computers to monitor and control systems in local facilities as well as assets in facilities located around the world. A key component of industrial control systems are supervisory control and data acquisition (SCADA) systems that provide centralized control and monitoring of large-scale, distributed assets. However, the functionality and efficiency provided by networking technologies come with an increase in system vulnerabilities that can be exploited by cyber attacks.

Security experts at McAfee [20] suggest that SCADA system defenses can be enhanced by removing potentially vulnerable SCADA assets from production networks and placing them in dedicated SCADA networks. The motivation for isolating SCADA systems is due in part to the number of critical infrastructure assets that use SCADA systems. The U.S. Air Force Civil Engineering Center (AFCEC) has stated that Air Force assets as well as industry assets are “at best insufficiently protected from cyber threats” [31]. This is particularly alarming given the priority placed on critical infrastructure assets by the USA PATRIOT Act [30], Homeland Security Presidential Directive (HSPD) 7 [5] and President Obama's Executive Order 13636 [21]. Indeed, protecting vital industrial control systems in the critical infrastructure is essential to mitigate the risk of attacks and minimize the potential of catastrophic consequences.

SCADA systems typically perform their monitoring and control tasks using field devices that implement the desired functionality. One such field device is the programmable logic controller (PLC), a special-purpose computer that performs low-level functions such as collecting sensor data and operating physical valves or switches. While programmable logic controller operating systems and communications protocols are typically proprietary, most programmable logic controllers have the ability to operate in standard computer networks. Consequently, they are vulnerable to cyber attacks such as those executed by Stuxnet [34] and Duqu [28], which targeted SCADA functionality by exploiting vulnerable programmable logic controller modules and compromised the reliable operation of physical assets.

The vast majority of information technology systems, including personal computers and network devices, are protected to some degree from cyber attacks through a variety of intrusion detection and anti-virus programs. This is in sharp contrast to programmable logic controller implementations that have very limited protection options – their proprietary design and limited processing power and memory resources preclude the direct use of standard computer and network defense mechanisms. Additionally, many programmable logic controllers remain in service for decades due to the prohibitive cost of re-engineering industrial control systems. Thus, programmable logic controllers become obsolete (unsupportable) relative to information technology standards and capabilities that rapidly evolve to satisfy consumer demands; this prevents the implementation of typical “bit-level” information technology protective measures in programmable logic controllers.

Traditional bit-level intrusion detection and anti-virus programs monitor activity and assess system status using information in the higher layers of the Open Systems Interconnect (OSI) model [35]. Recent research has successfully exploited device attributes in the lowest OSI layer (physical layer) to augment traditional bit-level security measures in the upper layers (network layer through application layer) [7,8,11,24,32]. These security augmentations use information extracted from radio frequency (RF) emissions (unintentional emissions as in [2,3,7,17] and intentional emissions as in [1,8,11,14,18,24,25,32,33]) to provide a means for discriminating between hardware devices much like DNA is used to uniquely discriminate between humans.

Research efforts focused on using physical layer information to secure devices against malicious code and monitor them for energy efficiency have analyzed the power consumed by the operating devices [2,3,6,12,19,29]. Other research has examined RF emissions from semiconductor devices to verify hardware or software integrity [7,17]. The approach described in this paper differs from previous unintentional emission (physical layer) efforts in three respects: (i) it focuses on device RF emissions, not power consumption; (ii) it uses RF emissions to verify software operations, not hardware identities; and (ii) it provides visibility at the operation level instead of at the program level (where a program comprises multiple operations).

In previous research related to programmable logic controllers [26,27], the unintentional RF emission process described in [7] for integrated circuit hardware discrimination was adopted and successfully integrated with a correlation-based anomaly detection (CBAD) process to demonstrate a new capability for identifying software anomalies or potential malicious programmable logic controller operation. The CBAD process described in [26,27] is adopted in this paper to implement an improved anomaly detection capability using Hilbert transformed sequences of unintentional programmable logic controller time domain emissions. However, the methodology is refined to establish a more robust normal condition reference sequence that better reflects operational implementation and to incorporate an operation-by-operation anomaly detection process. Excellent results are obtained using 10 like-model programmable logic controllers, including the device tested in [26,27]. The use of RF emissions facilitates the deployment of a monitoring network of individual low-cost RF probes placed on programmable logic controllers that relies on an analysis system. Because this analysis system would rely only on physical layer information from programmable logic controllers, it can be isolated from network-based cyber attacks by implementing it as a standalone system.

2. Technical background

Extensive research has focused on securing information technology systems and networks by controlling access and detecting malicious programs in the higher level OSI layers (data link layer through application layer). Bit-level credentials, such as media access control (MAC) addresses and international mobile equipment identity (IMEI) numbers, control network access while anti-virus and intrusion detection software protect information technology systems from malware. Had the information technology protection methods been available for programmable