Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip

Radio-frequency-based anomaly detection for programmable logic controllers in the critical infrastructure

*Samuel Stone, Michael Temple**

Department of Electrical and Computer Engineering, Air Force Institute of Technology, 2950 Hobson Way, Wright-Patterson Air Force Base, Ohio 45433, USA

ARTICLE INFO

Article history:
Received 16 January 2012
Accepted 11 May 2012
Published online 29 May 2012

Keywords:
SCADA systems
Programmable logic controllers
Radio frequency emissions
Anomaly detection

ABSTRACT

Advances in the processing power and efficiency of computers have led to the proliferation of information technology (IT) systems in nearly every aspect of our daily lives. The pervasiveness and reliance on IT systems, however, have increased the susceptibility to cyber attacks. This is of particular concern with regard to supervisory control and data acquisition (SCADA) systems in the critical infrastructure. Compromises of SCADA systems – in particular, the programmable logic controllers (PLCs) used as field devices to control and monitor remote processes – could have devastating consequences. However, because of their limited onboard computing resources (e.g., processing power and memory), conventional bit-level IT security mechanisms are not well suited to safeguarding PLCs.

This paper describes a methodology for detecting anomalous operations of PLCs. The methodology uses information extracted from radio frequency (RF) features to identify changes in operating characteristics due to malicious actions or system failure. The experimental results demonstrate the utility of the RF-based anomaly detection methodology for PLC verification.

1. Introduction

Modern society is critically dependant on computers and information technology (IT) systems. However, this dependence brings about heightened threats to critical systems as malicious actors become better equipped to conduct cyber attacks. As stated in the USA PATRIOT ACT of 2001 [1]: "Private business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors". The Homeland Security Presidential Directive 7 of 2003 [2] calls for the prioritization of critical infrastructure assets for the purpose of protecting them from terrorist attacks.

The reliance on computing and IT resources extends to the critical infrastructure as demonstrated by the automation and networking capabilities of supervisory control and data acquisition (SCADA) systems that monitor and control operations in every critical infrastructure sector. A SCADA system is a highly distributed industrial control system that centrally monitors and controls operations at remote field sites. Remote field sites incorporate automated devices, such as programmable logic controllers (PLCs), that control actuators and monitor sensors associated with physical operations.

Stuxnet has demonstrated that PLCs are highly vulnerable to malicious manipulation [3]. However, the limited processing power and memory of PLCs precludes the adoption of typical bit-level security mechanisms that are commonly

* *Corresponding author.*
E-mail address: michael.temple@afit.edu (M. Temple).

1874-5482/$ - see front matter © 2012 Published by Elsevier B.V.
doi:10.1016/j.ijcip.2012.05.001

employed in IT systems. These mechanisms generally detect unauthorized or anomalous activity by analyzing data in the higher layers of the Open Systems Interconnect (OSI) model [4].

Recent research has exploited attributes at the lowest OSI physical layer to augment bit-level security [5–7]. This is accomplished using radio frequency (RF) fingerprints that are sufficiently unique to enable human-like discrimination of device emissions. These emissions are nearly impossible to replicate, and they can protect against security credential counterfeiting schemes. This paper describes an RF-based methodology, which uses information extracted from RF features to detect anomalous operations of PLCs in SCADA systems. The anomalous behavior may be incidental (e.g., induced by degraded or failed components) or intentional (e.g., induced by cyber attacks).

2. Background

Data access and trust relationships in cellular communications and wireless networking systems are commonly verified via authentication methods operating in the upper, bit-level OSI model layers. Common authentication credentials include media access control (MAC) addresses, electronic serial numbers (ESNs), and international mobile equipment identity (IMEI) numbers. At the network level, additional protection mechanisms include firewalls and intrusion detection systems (IDSs) to detect and block cyber attacks. At the client level, virus detection and host-based IDSs are employed for protection. Unfortunately, these common IT protection mechanisms are generally not implementable in PLC-based SCADA systems.

SCADA systems comprise special purpose machines that generally lack the computing resources (e.g., processing power and memory) of most IT network servers and client desktop computers. Additionally, it is not uncommon for many industrial control system components (including PLCs) to remain operational for decades. Simply stated, the functionality of a PLC is insufficient for running the majority of virus detection and IDS programs. Thus, PLC-based systems suffer increased exposure to threats, including those with the potential to inflict substantial physical losses as in the case of Stuxnet [8,3]. Given the inability to implement bit-level protection for SCADA systems, this research focuses on detecting anomalous activity by exploiting physical attributes of RF emissions during system operation.

RF attributes have been previously used for device classification, identification, authentication, and operational status assessment [5,9–11,6,12]. Based on this body of research, it is reasonable to expect that such attributes are present in RF emissions from SCADA devices such as PLCs. However, it remains to be determined if these attributes can be used to detect anomalous operation. This research attempts to leverage physical layer characteristics to detect anomalous and/or malicious activity in SCADA components. Specifically, it seeks to assess the uniqueness of RF emission attributes for the purpose of classifying PLC operation as normal or anomalous.

At the core of PLC-based SCADA systems are semiconductor integrated circuit (IC) devices. Variations in materials, processes, and environmental factors during semiconductor manufacture impart operational (i.e., electrical) variations in IC devices even if they are designed to be equivalent. Post-manufacture testing examines the operational variations to ensure that the functional characteristics of devices are within the defined tolerances before they are made available to consumers. Indeed, the unique RF fingerprints produced by the inherent variations existing between tolerance-compliant devices have been successfully exploited for IC classification and verification [5].

2.1. Emission collection

Research in the area of physical contact assessment has exploited differences in the electrical responses measured from IC pins to verify physical design authenticity [13,14]. Of particular relevance is the research related to non-contact electromagnetic assessment where RF emissions from ICs are collected for the purpose of classification and verification [5]. For a given device under test, the average RF signal power, which is significantly lower than a "by design" signal response, is collected using a near-field RF probe placed in close proximity of the test device. The collection configuration and details (e.g., bandwidth and frequency range) are largely determined by the clock frequency of the test device and are empirically developed based on observation of the collected signals. The near-field probe output is digitally sampled and stored by an advanced oscilloscope. This digital signal is used to develop the RF fingerprint using post-collection processing. The resultant RF fingerprint can then be used to either classify the test device (i.e., a 1-to-*M* comparison to determine the best match) or to authenticate the test device (i.e., a 1-to-1 comparison to determine the degree of the match).

2.2. Authentication-based anomaly detection

The biometric classification and authentication methodology of Jain et al. [15] forms the basis for our efforts to detect anomalous PLC operation. As a proof-of-concept demonstration, authentication is implemented as a one-to-one comparison of an RF fingerprint representing the current operation and a stored reference fingerprint representing a "claimed" condition of normal operation.

RF fingerprints have been used in a similar manner to authenticate the operation of PIC microcontrollers with better than 99.5% accuracy [5]. The assessment is based on the analysis of the receiver operating characteristic (ROC) curve as commonly used to address binary classification problems such as biometric authentication. In a binary classification, the claim is either authenticated (i.e., positive result) or not authenticated (i.e., negative result).

In the case of PLC anomaly detection, the device under test operates under one of two possible conditions: "normal" or "anomalous". The goal is to accurately determine if the test device is operating normally. This is accomplished by claiming normal operation regardless of the actual unknown operation and making a final declaration of normal or