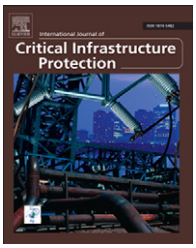
Available online at www.sciencedirect.com
SciVerse ScienceDirect
www.elsevier.com/locate/ijcip



A security-hardened appliance for implementing authentication and access control in SCADA infrastructures with legacy field devices

Jeffrey L. Hieb, Jacob Schreiver, James H. Graham*

Intelligent Systems Research Laboratory, J.B. Speed School of Engineering, University of Louisville, Louisville, KY 40292, USA

ARTICLE INFO

Article history:
Received 25 April 2012
Accepted 20 December 2012
Available online 11 January 2013

Keywords:
SCADA systems
Field devices
Authentication
Access control
Bloom filters

ABSTRACT

Considerable progress has been made with regard to securing industrial control systems. However, security challenges remain for field devices, and these challenges are compounded by the presence of legacy field devices. This paper describes the design, implementation and performance of a security-hardened, bolt-on, security appliance for legacy field devices. The approach uses a microkernel-based architecture and employs Bloom filters to implement challenge-response authentication and role-based access control for in an in-line field device security pre-processor. The microkernel-based architecture isolates network-interacting software from security-enforcing components, reducing the size of the trusted computing base of the device. Bloom filters provide a fast and constant access time solution for authentication and authorization checks. An analysis of the impact of Bloom filter false positive rates is provided, and it is shown that the false positive rates can be made arbitrarily low. Experimental results are also presented for a prototype device. Security-related computations on the pre-processor take less than one millisecond to perform, indicating that the prototype and the underlying approach are well-suited to a variety of industrial control system environments. Penetration tests demonstrate that the device is robust to attack, except for certain denial-of-service attacks.

1. Introduction

Supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs), collectively referred to as industrial control systems (ICSs), are networks of computer-based systems that provide remote telemetry and real-time control of physical systems and processes. Industrial control systems play a central role in operating many critical infrastructures assets such as electric power, water treatment, and oil and gas distribution systems. A typical industrial control system consists of a master, one or more field devices, and a communications infrastructure. The master or master terminal unit (MTU) in combination with a separate or integrated human machine interface (HMI) processes messages received from field devices, presents the information to operators and engineers, and sends control directives back to field devices. Fig. 1 shows the components of a typical industrial control system. The field devices and the master are connected by a communications network, which may involve serial lines, the public switched telephone network, cellular networks, and various types of UHF/VHF radio links. Field devices and operators may be in different

*Corresponding author.
E-mail address: jeff.hieb@louisville.edu (J.L. Hieb).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.01.001

Fig. 1 – Industrial control system.

parts of the same building, in nearby buildings, or across the country. The communication protocols used by field devices and master units are referred to as SCADA protocols.

When industrial control systems were initially developed, little attention was paid to cyber security because the systems were physically isolated and used proprietary hardware, software, and communication protocols [1–5]. However, due to network connectivity and convergence, industrial control systems are now exposed to cyber attacks [1,4]. The security problems are exacerbated by the lack of sender authentication and message integrity in SCADA protocols, the use of default passwords or no passwords for system-level access to devices, and the increasing use of commodity operating systems. Most efforts at securing industrial control systems employ established information technology security controls such as firewalls and network intrusion detection systems; these controls are typically applied to the control network and the connections between the control network and the enterprise network. This is an appropriate and much needed first response. However, Stuxnet [6] and other recent incidents demonstrate that improved cyber security at the field device level is urgently needed.

Field devices are embedded systems that typically comprise an embedded operating system, control system software, and analog and digital inputs/outputs. These devices present unique security challenges. They have long deployment lifetimes, sometimes as much as 30 years. Moreover, infrastructure assets incorporate numerous legacy field devices, most of which lack security features and do not support the integration of new security features. The replacement of field devices, which often incorporate specialized hardware, is usually not an option because of the expense involved. Additionally, security solutions for field devices must be sensitive to the performance requirements of industrial control systems and the systems and processes they control.

This paper describes the design, implementation and performance of a field device security pre-processor (FD-SPP) that provides message integrity, sender authentication, and role-based access control of field devices. The FD-SPP is secured using an architecture that was originally developed to provide robust, verifiable security for next-generation field devices; the architecture is, nevertheless, appropriate for creating security-hardened, bolt-on security appliances for field devices such as the FD-SPP. The architecture isolates software that interacts with the control network from security-enforcing software and the software that operates connected field equipment. To achieve robust and predictable performance, the FD-SPP uses Bloom filters to determine if a SCADA message needs to be authenticated and if the user has the privileges to carry out the requested operation. Bloom filters are susceptible to false positive errors, but the false positive rates can be reduced to levels that are acceptable for field devices used in industrial control applications.

2. Background

The lack of security features in most SCADA protocols is recognized as a major problem. Wright et al. [7] have designed a low-latency encryption scheme for serial SCADA communications, which is intended to address the lack of integrity and authentication checks on communications to and from field equipment. Several commercial products have been released that provide some level of security for field equipment; these include SEL 3620 [8] and SEL 3021 [9] from Schweitzer Engineering Laboratories, and the Tofino Security Appliance [10]. The SEL 3620 is a secure Ethernet gateway that handles Ethernet and serial communications, but is intended primarily for Ethernet connections. The SEL 3620 provides link level encryption (using IPsec) of all traffic to and from a field site; it also provides firewall capabilities at the field level, event logging, and user-based access control. The SEL 3021 is a serial encrypting transceiver that provides link level encryption for serial communications. The Tofino Security Appliance supports only Ethernet networks and provides link level encryption using IPsec, a SCADA-protocol-based firewall, and event logging.

This paper describes a microkernel-based, security-hardened architecture for field devices and remote terminal units (RTUs) [11,12]. The architecture supports a suite of field device security services and isolates network interface software, including drivers, network stacks and application layer processing, from security-enforcing code, cryptographic keys and field equipment software (analog and digital input/output) interfaces.

2.1. *Security-hardened architecture for field devices*

The operating system plays a key role in securing any computer system, since its primary purpose is to provide access to physical resources and to control shared access to the resources through well-defined abstractions. The kernel is the portion of the operating system that executes under the privileged mode of the processor and provides the lowest level of abstraction between the physical components and the rest of the system. It is typically the kernel, or some part of the kernel, that accesses the physical resources of a field device, and it must run with full privileges to do so. The kernel also provides protection mechanisms that keep application processes separate and determines the specific