available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Security issues in SCADA networks

Vinay M. Igure, Sean A. Laughter, Ronald D. Williams*

Charles L. Brown Department of Electrical and Computer Engineering, University of Virginia, Charlottesville, VA 22904, USA

ARTICLE INFO

Article history:
Received 27 June 2005
Revised 1 February 2006
Accepted 6 March 2006

Keywords:
SCADA network security
Critical infrastructure security
SCADA protocol analysis
Firewalls
Intrusion detection systems
SCADA cryptography

ABSTRACT

The increasing interconnectivity of SCADA (Supervisory Control and Data Acquisition) networks has exposed them to a wide range of network security problems. This paper provides an overview of all the crucial research issues that are involved in strengthening the cyber security of SCADA networks. The paper describes the general architecture of SCADA networks and the properties of some of the commonly used SCADA communication protocols. The general security threats and vulnerabilities in these networks are discussed followed by a survey of the research challenges facing SCADA networks. The paper discusses the ongoing work in several SCADA security areas such as improving access control, firewalls and intrusion detection systems, SCADA protocol analyses, cryptography and key management, device and operating system security. Many trade and research organizations are involved in trying to standardize SCADA security technologies. The paper concludes with an overview of these standardization efforts.

Modern industrial facilities, such as oil refineries, chemical factories, electric power generation plants, and manufacturing facilities are large, distributed complexes. Plant operators must continuously monitor and control many different sections of the plant to ensure its proper operation. The development of networking technology has made this remote command and control feasible. The earliest control networks were simple point-to-point networks connecting a monitoring or command device to a remote sensor or actuator. These have since evolved into complex networks that support communication between a central control unit and multiple remote units on a common communication bus. The nodes on these networks are usually special purpose embedded computing devices such as sensors, actuators, and PLCs. These industrial command and control networks are commonly called SCADA (Supervisory Control and Data Acquisition) networks.

In today's competitive markets, it is essential for industries to modernize their digital SCADA networks to reduce costs and increase efficiency. Many of the current SCADA networks are also connected to the company's corporate network and to the Internet. This improved connectivity can help to optimize manufacturing and distribution processes, but it also exposes the safety-critical industrial network to the myriad security problems of the Internet. If processes are monitored and controlled by devices connected over the SCADA network then a malicious attack over the SCADA network has the potential to cause significant damage to the plant. Apart from causing physical and economic loss to the company, an attack against a SCADA network might also adversely affect the environment and endanger public safety. Therefore, security of SCADA networks has become a prime concern.

1. SCADA network architecture

A SCADA network provides an interconnection for field devices on the plant floor. These field devices, such as sensors and actuators, are monitored and controlled over the SCADA network by either a PC or a Programmable Logic Controller

* *Corresponding author.*
E-mail addresses: vmi5e@virginia.edu (V.M. Igure), sal4t@virginia.edu (S.A. Laughter), rdw@virginia.edu (R.D. Williams).
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.03.001

(PLC). In many cases, the plants also have a dedicated control center to screen the entire plant. The control center is usually located in a separate physical part of the factory and typically has advanced computation and communication facilities. Modern control centers have data servers, Human–Machine Interface (HMI) stations and other servers to aid the operators in the overall management of the factory network. This SCADA network is usually connected to the outside corporate network and/or the Internet through specialized gateways (Sauter and Schwaiger, 2002; Schwaiger and Treytl, 2003). The gateways provide the interface between IP-based networks on the outside and the fieldbus protocol-based SCADA networks on the factory floor. The gateway provides the protocol conversion mechanisms to enable communication between the two different networks. It also provides cache mechanisms for data objects that are exchanged between the networks in order to improve the gateway performance (Sauter and Schwaiger, 2002). A typical example of SCADA network is shown in Fig. 1.

Apart from performance considerations, the design requirements for a SCADA network are also shaped by the operating conditions of the network (Decotignie, 1996). These conditions influence the topology of the network and the network protocol. The resulting SCADA networks have certain unique characteristics. For example, most of the terminal devices in fieldbus networks are special purpose embedded computing systems with limited computing capability and functionality. Unlike highly populated corporate office networks, many utility industry applications of SCADA networks, such as electric power distribution, are usually sparse, yet geographically extensive. Similarly, the physical conditions of a factory floor are vastly different from that of a corporate office environment. Both the large utility and factory floor networks are often subjected to wide variations in temperature, electro-magnetic radiation, and even simple accumulation of large quantities of dust. All of these conditions increase the noise on the network and also reduce the lifetime of the wires. The specifications for the physical layer of the network must be able to withstand such harsh conditions and manage the noise on the network.

Typical communications on a SCADA network include control messages exchanged between master and slave devices. A master device is one which can control the operation of another device. A PC or a PLC is an example of a master device. A slave device is usually a simple sensor or actuator which can send messages to the command device and carry out actions at the command of a master device. However, the network protocol should also provide features for communication between fieldbus devices that want to communicate as peers. To accommodate these requirements, protocols such as PROFIBUS have a hybrid communication model, which includes a peer-to-peer communication model between master devices and a client–server communication model between masters and slaves. The communication between devices can also be asymmetric (Carlson, 2002; Risley et al., 2003). For example, messages sent from the slave to the master are typically much larger than the messages sent from the master to the slave. Some devices may also communicate only through alarms and status messages. Since many devices share a common bus, the protocol must have features for assigning priorities to messages. This helps distinguish between critical and non-critical messages. For example, an alarm message about a possible safety violation should take precedence over a regular data update message. SCADA network protocols must also provide some degree of delivery assurance and stability. Many factory processes require real-time communication between field devices. The network protocol should have features that not only ensure that the

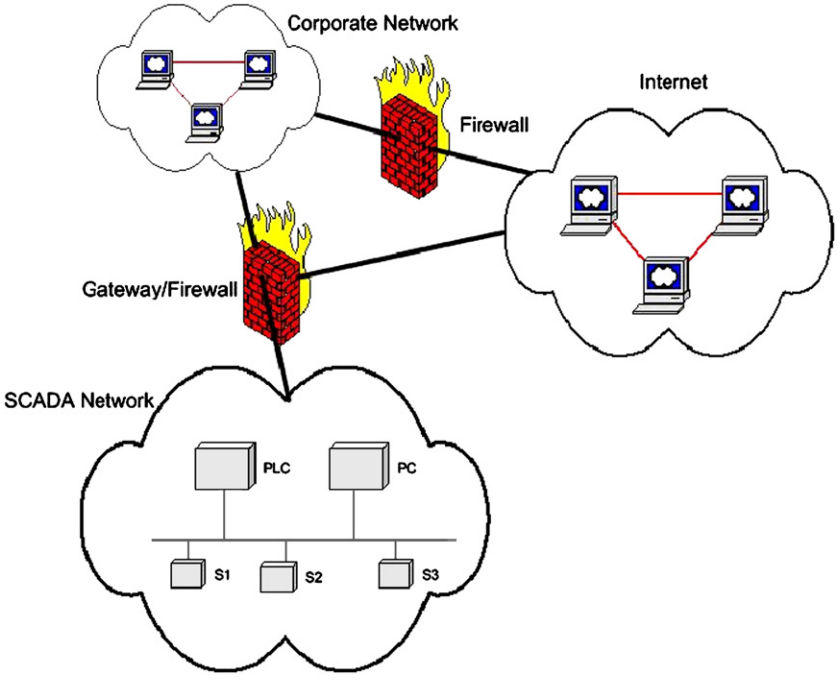

Fig. 1 – Typical SCADA network architecture.