Secure SCADA Network Technology and Methods

FARKHOD ALSIHEROV, TAIHOON KIM
Dept. Multimedia Engineering
Hannam University
Daejeon, South Korea
sntdvl@yahoo.com, taihoonn@paran.com

Abstract: The overall security concern facing the designers and operators of SCADA and, more generally, of industrial control systems typically originates either from malicious threat agents attempting to disrupt the control system operation, e.g. to create a power outage, or it originates from inadvertent actions, equipment failure, or similar. Electric utilities require secure network and control system. This paper illustrates solutions for control networks and equipment, SCADA data and communications.

Key-Words: SCADA security, Secure SCADA networks

1 Introduction

To address security vulnerabilities, organizations primarily install security retrofits or upgrades to their existing SCADA systems. The corresponding standardization bodies and regulatory agencies also deal with the design of new secure systems. For example, security enhancements to IEC control protocols are available and being further developed in IEC 62351 standards. SCADA communications include a diverse set of layered protocols and physical media. A large class of SCADA protocols is implemented using TCP/IP protocols. Utilities' communications network of choice, dedicated for control applications is typically a private IP (Internet Protocol) network (referred to as intranet) and/or an Ethernet. Corresponding open data communications security methods that may be used include firewalling, VPN (Virtual Private Network), tunneling, authentication, cryptography, and IDS (Intrusion Detection System). These methods are standardized by organizations like NIST (National Institute of Standards and Technology), IETF (Internet Engineering Task Force) and ISO (International Standards Organization) in the framework of IP communications and information security standardization.

Typically there are two major analysis methods in regard to security:

1. Enterprise based analysis
2. Technology/threat based analysis.

Both approaches have disadvantages. There are vendors who can offer integrated solutions that meet important technical requirements of secure control networks, SCADA data and protocol communications that are conformant to the regulatory security requirements and industry standards for control network operation, like NERC CIP [1], IEC [2] and NIST [3]. They are the reference standards for diverse implementations, without being the only possible solutions. The requirement of a high level of network security is related to other critical requirements of SCADA communication networks, including [5]:

- Electrical and environmental requirements for communications equipment in substations addressing harsh environmental conditions
- Bounded response times for real-time SCADA applications
- Network resilience, or the ability to heal around failures

In each particular control system and network, the security risk must be assessed and security measures determined accordingly. One should be aware that there is often a trade-off between security, cost, and performance when choosing one method over another. In general, multiple levels of security mechanisms and measures are needed to ensure robust control system communication.

2. Secure SCADA Network Technology and Methods

Network resource, routing and management information exchange should be secured in a communications network used for control purposes. Multiple levels of security measures may be implemented. The level of security protection strongly depends on risk assessment and performance requirements.

2.1 Topology, Routing and Protocols

Network reliability should be ensured by making use of redundant topology and functionality. This includes layer 2 mesh topologies with RSTP (Rapid Spanning Tree Protocol) on the substation LAN (Local Area Network) [5], [6], [7], OSPF (Open Shortest Path First) on the intranet and VRRP (Virtual Router Redundancy Protocol) for redundant access to the IP network and backup links between the routers.
In addition, traffic may be segregated using VLANs to further increase security. Some protocols, such as IPv6, OSPFv3 (RFC 2740) and SNMPv3 (RFC 3826), provide their own mechanisms for authentication and data encryption. MAC address filtering should be used on Ethernet switches and IP address filtering, i.e. IP access lists, should be used on firewalls to define the end devices that are permitted to connect to network devices. QoS (Quality of Service) mechanisms should be used to ensure bounded latencies for real-time SCADA applications and to ensure network resource availability. Messages should be prioritized and PQ (Priority Queuing), CBWFQ (Class-Based Weighted Fair Queuing) or similar queuing mechanisms should be used on routers and switches. IEEE 802.1p prioritization should be used on LAN switches and IP based prioritization should be used on routers.

2.2 User and Device Authentication

The most often used AAA (Authentication, Authorization and Accounting) server is the Remote Authentication Dial-In User Service (RADIUS) (RFC 2865 and 2866) using IEEE 802.1x with the Extensible Authentication Protocol (EAP). It plays a key role in user authentication at all levels in the network. For example, firewalls and access routers can act as authenticating agents, intermediaries for client devices or entities connecting to them, such as wireless devices and end user equipment. The authenticating agent challenges the entity, which authenticates itself, e.g. using a username and password, which are forwarded to and processed by the authentication server, e.g. RADIUS, that gives authorization and access rights to the client. Passwords should be encrypted when sent across a network. Some form of cryptographic hash should be used that is specifically designed to prevent replay attacks e.g. approved by FIPS (Federal Information Processing Standards) [6]. One may supplement password authentication with other forms of authentication such as challenge/response or by using biometric or physical tokens. Physical tokens are suitable in physically secure area. Role Based Access Control (RBAC) should be used to restrict user privileges to only those that are required to perform a task. Currently, IEC TC57 WG15 has initiatives to develop standards to define RBAC for SCADA communications. All system administrator communication must be authenticated, confidential and its integrity protected. The following methods provide such security: SSHv2 (Secure Shell), rather than Telnet and HTTPS (Hyper Text Terminal Protocol over Transport Layer Security), RFC 2818, rather than HTTP

2.3 Firewalls

Network firewalls control data flow between networks employing differing security postures.
NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, provides general guidance for selection of firewalls and firewall policies [8]. In a SCADA environment, a firewall must be deployed between the SCADA control network and the business network. Firewalls should include the following features: extensive logging of events, IDS, DMZ (DeMilitarized Zone) based policy routing, access lists, etc.
Firewall use depends strongly on network topology.

2.4 IPsec VPN

An IPsec-based VPN can provide tunneling between physical security perimeters. It typically runs between the corresponding firewalls, or as needed, between routers. A remote user can also gain access to a secure perimeter by connecting via an IPsec VPN. IPsec can ensure integrity, authenticity and confidentiality of data, [11] and [9].
The technique involves establishing an IPsec tunnel over an arbitrary, possibly insecure, IP network, and transmitting data through the tunnel. Each IP packet is encrypted and encapsulated within an additional IP packet at the IPsec tunnel ingress. Routers use the new IP header information to forward the packet between the tunnel endpoints. The original frame is extracted and decrypted at the tunnel egress. IPsec uses one or both of the Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols. AH provides data integrity and packet origin authentication. ESP encrypts the IP packet. IPsec including both AH and ESP is a mandatory part of IPv6 implementation. Its use is optional both with IPv4 and IPv6. IPsec devices use Internet Key Exchange (IKE) to authenticate the peer, negotiate and distribute symmetric encryption keys, and establish IPsec security associations. IPsec often uses preshared key and signature for device authentication. IPsec can use shared secret keys only, or it can make use of PKI. Efficient IPsec VPN management in a smaller network may imply that the administrator can easily configure secret keys. An IPsec-based VPN should be implemented only if necessary to augment the end-to-end security methods already in use by a SCADA

application. IPsec authentication may be used without SCADA performance degradation. IPsec encryption should not be implemented if SCADA runs over TLS as in IEC 62351-3 and -4. Reencrypting data traffic is generally redundant, costs additional processing resources, and causes the traffic to incur additional latency in transit.

2.5 Intrusion Detection System

An Intrusion Detection System (IDS) issues alerts when a system is being probed or attacked [8]. It generally collects information from different sources at strategic points in the network, analyzes the content of individual packets for malicious traffic, and then issues alarms, drops data, logs events and activities, and initiates other responses as necessary. IDS vendors also develop and incorporate attack signatures for various application protocols such 8as DNP (Distributed Network Protocol) and ICCP (Inter-Control Center Communications Protocol), in addition to the usual signatures [3].

Network based IDS are deployed on control network equipment. Host based IDS are deployed on SCADA servers, systems that use general purpose operating systems, and those running SCADA protocols, etc. Integrated IDS control of agents in network equipment and in SCADA devices is the most efficient implementation of IDS, since they include hostbased and network based IDS. Note that the addition of IDS agents has the potential to adversely affect system performance.

2.6 Wireless and Modem Links

Modems are often used to provide backup links. Callback systems can be used to ensure that a dialer is legitimate by using the callback number stored in a trusted database. Remote control software should use unique user names and passwords, encryption, and audit logs. Link layer neighbor authentication should be done e.g. using CHAP (Challenge Handshake Authentication Protocol) of RFC 1994.

Wireless user access and links between network equipment may be implemented in several ways.

Users or nodes may act as wireless clients of an IEEE 802.11b/g network access point, or two or more nodes may form a point-to-point or multipoint fixed installation using 802.11 Ad-Hoc mode. All wireless communication should be protected by the available security features such as strong data encryption protocols e.g. IEEE 802.11i with AES support. Wireless access should use IEEE 802.1x authentication which authenticates clients either via user certificates or via a RADIUS server. Hardware accelerators may be needed to perform cryptographic functions to reduce encryption latency.

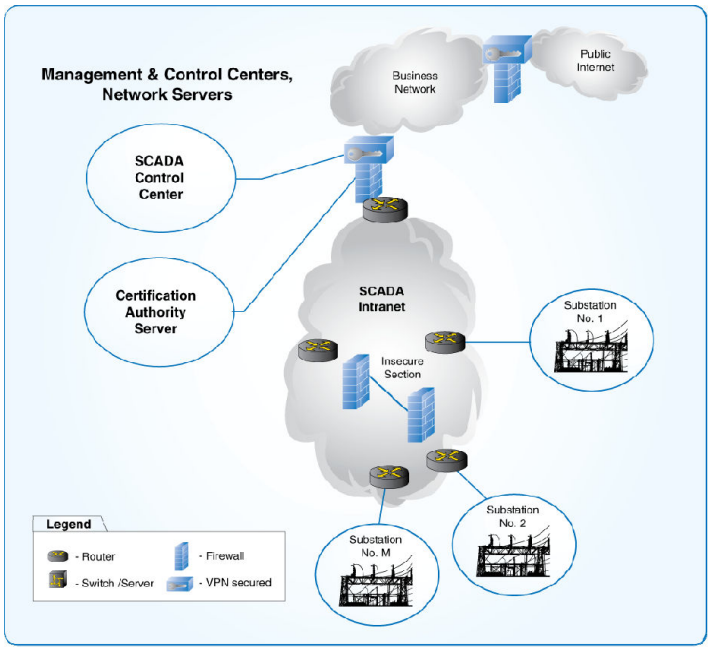

Fig.1 Reference SCADA control network

2.7 Time Synchronization

Real-time clocks in each piece of SCADA and network equipment should be synchronized, and the correct time should be logged along with each entry in the event log. To that end, NTP (Network Time Protocol) and IEEE 1588 are used. The older NTP is widely used throughout the Internet and is accurate in the face of a wide range of network latencies and varying conditions. The much newer IEEE 1588 addresses the clock synchronization requirements of measurement and control systems. Service for both protocols may be provided by standalone equipment or by components of other network equipment or of general purpose computer equipment. The required time precision is not in the scope of NERC CIP, although it does require extensive logging on all equipment to make security event analysis possible and effective.

2.8 Network and Security Management

SCADA protocols, telecommunication networks, and TCP/IP networks may use different management methods. Standardization effort on IEC 62351 should also lead to a generic management information model and a MIB (Management Information Base) module for security management of control protocols and communication networks. It is not in the scope of this paper to discuss security aspects of management protocols in detail. SNMP (Simple Network Management Protocol) is traditionally used to

manage IP network resources such as routers, firewalls and servers. SNMP may also be used to provide integrated management of SCADA applications and control networks. SNMPv3 includes the security features fundamentally required by NERC CIP: message integrity, authentication and encryption.
See RFC 2574 and RFC 3826. Security management applied to SCADA networks and applications includes monitoring, analyzing, providing security and responding to incidents. This includes dynamic adaptation to new security requirements as they change, prioritization of security vulnerabilities, and mapping them onto management of the following: AAA (e.g. RADIUS), security keys, traffic filtering, IDS, logging, etc. Integrated security management systems for SCADA and general networks are emerging on the market. An integrated security system can include easy audit log accessibility, centralized user authentication, integrated key management, security logging and dynamic firewall configurability through a centralized control centre [10].

3 Conclusion

A networked SCADA application can be secured to a high level by implementing, as appropriate, the techniques, protocols, network topologies, and policies illustrated in the reference SCADA control network in this paper. Whether planning a new SCADA implementation or securing an existing one, the selection of equipment, software, and techniques used to ensure security must take into account the following:

- an evaluation of security risks and of the vulnerability to those risks,
- corporate security policy, which itself should reflect the requirements of NERC CIP, and
- an evaluation of the trade-offs between complexity and performance.

The critical asset cyber security framework that applies to SCADA systems and networks is provided in NERC CIP standards 002-009. In this paper, we have shown how these requirements map onto and can be realized using secure communications equipment that includes the following general features: security monitoring, logging and security notifications, authentication control at interactive access points, access logging including dial-up devices, anti-virus software, IDS, security patches, security upgrades to the software, and the ability to enable only those ports and services required for operations.
Secure communications equipment and methods include the following:

- Encrypted authentication at all levels and authorization service e.g. RADIUS
- Secure SCADA control protocols e.g. using TLS, see IEC 62351
- Firewalls to protect each SCADA site and dedicated DMZs for servers and hosts
- Secure management e.g. via SNMPv3, secure administrator access e.g. via SSH and HTTPS
- IPsec tunnels on insecure network sections which implement authentication but not necessarily encryption
- Time synchronization for SCADA and network equipment
- Integrated IDS system for SCADA and network equipment
- PKI for cryptographic public key management, and/or efficient cryptographic secret key management
- Integrated security management for SCADA and network systems that includes security audit log retrieval and user authentication

References:

[1] North American Electric Reliability Council (NERC), Critical Infrastructure Protection Committee, NERC Standard CIP-002 through -009, Cyber Security, June 2006

[2] IEC 62351 Power systems management and associated information exchange Data and communication security, 2006-2007.

[3] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, Second Public Draft, Sept. 2007.

[4] Cleveland, F., IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encryption, Transmission and Distribution, Conference and Exhibition 2005/2006 IEEE PES, Page(s):1079 – 1087 Digital Object Identifier 10.1109/TDC.2006.1668652

[5] Marzio Pozzuoli, RuggedSwitch Reliability, Immunity, Performance, available at http://www.ruggedcom.com

[6] The Automation of New and Existing Substations: Why and How, CIGRE Study Committee B5, available at http://grouper.ieee.org/groups/1525/CIGRE3 4.07/Document/, August 2003.

[7] Michael Galea, Marzio Pozzuoli, Redundancy in Substation LANs with Rapid Spanning Tree Protocol (IEEE 802.1w), Electric Energy T&D Magazine, Sept.-Oct. 2003, pp. 66-68.

[8] NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, provides general guidance for the selection of firewalls and the firewall policies.

[9] NIST SP 800-77 Guide to IPsec VPNs, December 2005

[10] Gauntlet security system, available at http://www.teltone.com

[11] John Mairs, VPNs: A Beginner's Guide, McGraw-Hill Co., 2002, ISBN 0-07-219181-3.

[12] Federal Agency Regulatory Commission (FERC) "FERC approves new reliability standards for cyber security", http://www.ferc.gov/news/ January 2008

[13] A. MacDonald, Make the most of maintenance resources with wireless substation monitoring, Joseph, 03/23/2007, Energy Tech Magazine.

[14] 802.11 Wireless Networks: The Definitive Guide, Matthew S. Gast, O'Reilly, CA, April 2005.