Security in Industrial Applications

How Ethernet Networks and Web Management Support Secure Communications

A White Paper from GarrettCom, Inc.
Fremont, Calif.
www.GarrettCom.com

GarrettCom™
Ethernet at Its Best℠

INTRODUCTION

This paper explores the state of network security options today at the Ethernet switch level and offers an elementary roadmap for industrial operations to plan for and deploy secure communications systems. Industrial systems need to take advantage of the advanced networking technologies that can support greater efficiency, reliability, and security in plant and remote operations. As SCADA systems, relays, and other industrial control, monitoring and management systems become more intelligent, a rich supply of data is available for improving plant performance and remote maintenance and management. However, as with all technology advances, there are challenges as well as opportunities.

SECURITY OVERVIEW

In today's uncertain world, security stands beside profitability, productivity, performance and control as a key element for maintaining business activities in industrial facilities. Prevention of malicious attacks against business infrastructure has become as vital to ongoing success as has the widespread use of the computer systems which make such attacks so easy and so painful. It is no longer enough to catch the perpetrator during or after the commission of a malicious act; considerable time and expense is being consumed to address how to secure systems to prevent intrusion.

Repercussions from the 2003 power blackout in the Northeastern US were felt throughout the country. Attacks such as the Zobot worm and Mytob bot software effectively shut down well protected computers at CNN, the New York Times and many other places. Imagine how much worse a concentrated and widespread act of industrial sabotage might be.

Until just recently, SCADA (Supervisory Control And Data Acquisition) environments were not considered at risk for cyber attack because of the highly customized nature of these systems. In March 2002, articles were still being written that debunked the concern for more security of utility service providers. Yet this viewpoint is compromised by documented cyber-related incidents, such as the Slammer Worm infiltration of an Ohio Nuclear power plant, and the wireless attack on a sewage-SCADA system in Queensland Australia.

More and more industrial sites are taking advantage of Ethernet as a mature, end-to-end, standards-based networking, communications and data transmission protocol because it offers convenience and efficiency that bring higher performance and lower cost. In addition, the standards that are in place support interoperability among many competing equipment vendors as well as world-wide interconnectivity. At the same time, more extensive use of Ethernet/IP and other well-documented protocols will make hacking and disruption easier if adequate security measures are not taken. Password protection, encryption, access authorization and firewalls are some of the many tools available to protect against cyber invasion.

INDUSTRIAL SECURITY INITIATIVES

While there are similarities between security in enterprise business IT systems (which protects activities such as bank and stock transactions and on-line purchases), and that required by industrial control systems, several groups have been chartered to address the technology opportunities and challenges specific to industrial applications. At the broadest level, the Instrumentation Systems and Automation Society (ISA) and the National Institute of Standards and Technology (NIST) are looking at overall security practices for industry. (See APPENDIX A)

On a more specific industrial level, there are groups such as the North American Electric Reliability Council, which has been named by the US DoE as the electric energy sector's coordinator for critical infrastructure protection. The NAERC's Critical Infrastructure Protection Committee addresses security concerns and provides guidelines and requirements for utility systems including SCADA and EMS.

ETHERNET SECURITY – THE SWITCH VENDOR'S OPPORTUNITY

No single vendor or single technology is going to make industry safe from intentional cyber attacks. Nonetheless, it is critical that vendors of industrial equipment look at ways in which to support the overall security effort. Standards-based Ethernet networks, with cost effective hardware and software available from many competing vendors, can make a significant impact. For example, leading Ethernet switch vendors are adding security in the switch with IEEE and other standards support for security features.

As Ethernet has expanded into outlying industrial facilities, two types of network structures emerge: Local and Remote. The Local Ethernet structure is within the walls of a single facility which can be closely watched, with the only serious security risk being from disgruntled employees or persons who have penetrated the physical security of the plant. Access to data running across this type of Local Ethernet network can be protected by segregating it with VLANs (Virtual Local Area Networks). VLANs can be configured to restrict points of access from the outside world and can employ password protection to provide authorization, authentication, and access control tethered to the Ethernet network itself. Telnet managed by the switch can be used for remote login to the switch manager software.

However, Ethernet's benefits to industrial applications run far beyond such restricted local applications. Much Ethernet connectivity is deployed beyond a single plant and local-only networks would limit the ability to manage, monitor and collect data from remote operations. Ethernet, using fiber cabling for distance, noise-immunity and security, is deployed throughout widely distributed industrial applications. Interconnecting multiple water treatment plants or power substations within a metropolitan area are typical examples.

Remote industrial Ethernet implementations are very popular applications for monitoring (the Data Acquisition (DA) part of SCADA). They are typically closed systems, which require in-facility access points for information review, as opposed to casual Internet access from the home or from the remote laptop of a maintenance supervisor. Within the closed system, remote monitoring may be possible, eliminating many routine maintenance visits to unmanned outlying operations, with concomitant reduction in costs. It is also easier to identify potential problems and dispatch maintenance or repair teams promptly – often avoiding down time or managing outages.

The only security risk in a closed system is a physical breach of the network, and even in the case of such an event, password protection goes a long way to providing data security. The downside is the lost opportunity for efficiencies and savings because of the limits placed on management and control of industrial operations from afar.

Management Supervision and Control – the SC part of SCADA - of remote sites over Ethernet has traditionally been used less often simply because of concerns regarding security. If these concerns can

be properly addressed, the benefits of controlling the functioning of equipment in remote locations such as power substations, and linking outlying facilities such as aircraft maintenance hubs and other far-flung industrial applications, can be realized. Web access provides very significant efficiency improvements and cost-savings, but this is also the area of greatest threat since the whole world has access to the Internet.

Ethernet equipment vendors must, therefore, take the lead in providing security for Ethernet networks, and furthermore, must support the more broad-based systemic security requirements from such standards bodies as the ISA and NIST and NERC.

Once a closed-loop network is opened to access to and from the web, password protection is no longer enough. While security has multiple components, Ethernet equipment can address security issues by providing protection in the areas of concern documented by the ISA SP99 committee:

- assuring that a user is who he/she claims to be (authentication) and access authorization for that user;
- encryption and validation as data crosses the Internet so that it cannot be easily accessed and stolen;
- filtering and blocking access control;
- providing audit, measurement, monitoring and detection tools.

While Ethernet switch management software can, and should, attend to these components, implementation requires sophisticated security management advice making best use of standards, guidelines and experts.

ETHERNET SECURITY STANDARDS

Where web access is convenient, security does not have to be compromised. Authentication and encryption can be implemented today in industrial environments by using the same standards and controls that handle the world's financial transactions via the web. Through established security standards, network management software can provide this functionality by providing Simple Network

Management Protocol Ver. 3 (SNMP v3), Secure Socket Layer (SSL) and Transport Layer Security (TLS). These features allow an Ethernet switch to handle HyperText Transfer Protocol Secure (HTTPS), the highest level of Web access security available.

Other security strategies available to Ethernet equipment include port security, remote Telnet access security, password protection and remote unit cut-off protection. Appendix B offers a brief primer on the components of some of the most well-known security standards.

BEYOND THE SWITCH

Broader system security policies, physical and functional models, risk analysis, asset management and critical aspects of running and maintaining a security program are addressed in detail by bodies such as SP99 and PCSRF. The open approach of inviting industry wide input and comment will greatly improve security at all levels . . . national, business and personal.

Thanks to the forerunners in the commercial environment, there is a strong base from which industrial users can begin the work of adapting and customizing current security standards and protocols to support industrial applications. But, as they begin to reap the benefits of remote access, care must be taken to avoid security breaches. Commerce has led the way with highly secure financial, medical, and retail applications, however, the complexities of industrial security require careful thought and planning – and in many cases, a different take on a security strategy.

User authentication for controlling access and encryption are not only desirable but essential for secure industrial applications. Ethernet switches with web management can offer a powerful point of control. Additionally, remote web management is desirable *and* feasible with currently available hardware and software, including GUIs for simplicity and ease-of-use. However, complete end-to-end design for security is necessary, and it is incumbent on everyone to work toward highly secure network systems that enable the industry to take advantage of the tremendous time- and cost-savings of web-based networking.

A single white paper cannot possibly provide the specific guidelines that multiple prestigious industry working committees are laboring to describe. At the same time, this white paper is intended to be

helpful by providing a basic understanding of the security levels that can currently be achieved at the Ethernet switch level, assisting readers in appreciating the multiple levels of industrial network security and the overall complexity required to achieve a highly secure distributed communications system.

APPENDIX A

BRIEF OVERVIEW OF SP99 AND PCSRF

At the vanguard of developing security guidelines for industrial control systems are the Instrumentation, Systems, and Automation Society (ISA) and the National Institute of Standards and Technology (NIST). ISA, through its SP99 committee, has published two technical reports on manufacturing and control systems security that address the growing threats to industrial system security. The NIST Process Control Security Requirements Forum (PCSRF) has issued the System Protection Profile for Industrial Control Systems (SPP-ICS).

The SP99 committee, Manufacturing and Control Systems Security, represents a cross-section of the industrial market with representation from control system vendors, end-users, system integrators, consultants, and cyber security vendors. The first two reports from the committee, which were published in 2004, are: "Security Technologies for Manufacturing and Control Systems" (ISA-TR99.00.01-2004, or TR1) and "Integrating Electronic Security into the Manufacturing and Control Systems Environment" (ISA-TR99.00.02-2004 or TR2).

TR1 provides guidance for using currently available electronic security technologies, without making specific technology recommendations. It categorizes 28 electronic security technologies into five 'buckets":

- authentication and authorization;
- filtering/blocking/access control;
- encryption and data validation;
- audit, measurement, monitoring and detection tools;
- computer software and physical security controls.

Both control engineers and IT management can use the document to understand the opportunities and limitations of deploying IT-based security methods in a real-time environment.

The document provides information on each technology regarding:

- security vulnerabilities addressed by this technology;
- typical deployment;
- known issues and weaknesses;
- assessment of use in the manufacturing and control system environment.

In addition it discusses anticipated future directions, offers recommendations and guidance, and points the reader to information sources and reference material.

While TR1 can be considered a primer, TR2 offers more comprehensive information regarding methodologies and components necessary to create a complete security program, and suggests a process to implement more secure systems. Since most control systems are a combination of newer and legacy components, rather than a "built-from-scratch" environment, each system will require individual evaluation.

Today SP99 is developing a draft of the first of what will be a series of industry standards related to manufacturing security.

The NIST PCSRF's System Protection Profile for Industrial Control Systems (SPP-ICS), released in 2004, is a baseline document that states necessary industrial security requirements at an implementation-independent level. It will be used to create security specifications for specific systems and components, such as a water treatment system or a power substation.

The NIST PCSRF includes a number of members of the SP99 Committee, and is chartered to define common information security requirements for process control systems in the future. The Forum consists of more than 450 members from government, academic, and private sectors.
The current document is an extension of ISO/IEC 15408 Common Criteria. Common Criteria is widely used in secure government operations, such as the FAA. The SPP-ICS looks at these concepts in relation to industrial automation. Industrial facilities can use it to specify security functional requirements for new systems. At the same time, vendors can use it to demonstrate assurance that their products meet these security requirements.

APPENDIX B

SECURITY STANDARDS IN USE IN ETHERNET INSTALLATIONS

The protocols and standards listed below are readily available components that can be used to implement secure Ethernet networks in factories, power substations and other industrial sites.

SNMP

Simple Network Management Protocol, introduced in 1988, is a standard for gathering and managing statistical data about network traffic and the behavior of network components such as switches, hubs, routers and any device which is SNMP enabled. It is based on the manager/agent model and is used in TCP/IP and other networks to monitor and control network devices, and manage configurations, statistics collection, and performance. It is easy to implement, install, and use, and does not place undue burden on the network. Even better, SNMP modules from different vendors work together with minimal effort. However, early versions of SNMP did not adequately address the issue of security.

Basic security, in the form of authentication and encryption, was first proposed in 1998 with SNMPv3. Accepted as a full Internet standard in 2002, SNMPv3 assures that a received message was transmitted by the entity whose identifier appears as the source in the message header, it assures that the message was not altered in transit and that there was not artificial delay or replay. It also provides for the ability to update configuration parameters in SNMP agents, thus enabling complete remote management of SNMP devices, which is an added convenience as Web management comes into play.

It is important to note that SNMPv3 adds several levels of capability, and increasing complexity, to an SNMP implementation. Unless an implementation requires security features, most SNMP deployments will remain at SNMPv1 or SNMPv2. Perhaps the wisest approach for a vendor of Ethernet switches is to continue to offer these earlier versions, as well as SNMPv3, in its network management package to accommodate users with various levels of security requirements.

Communicating SNMPv3 engines share a secret authentication key that is provided by the sending entity. When the receiving entity gets the message, it uses the same secret key to calculate the message authentication code again. If the receiver's version of the code matches the value appended to the incoming message, then the receiver knows that the message can only have originated from the

authorized manager, and that the message was not altered in transit. Note that the shared secret key between sending and receiving parties must be preconfigured by a configuration manager or a network manager, and loaded into the databases of the various SNMP managers and agents.

A separate “privacy facility” enables managers and agents to encrypt messages to prevent eavesdropping by third parties. Again, manager entity and agent entity must share a secret key. When privacy is invoked between a principal and a remote engine, all traffic between them is encrypted using the Data Encryption Standard (DES). The sending entity encrypts the entire message using the DES algorithm and its secret key, and sends the message to the receiving entity, which decrypts it using the DES algorithm and the same secret key.

Another facility, called “access control” makes it possible to configure agents to provide different levels of access to different managers. Unlike authentication, which is done by user, access control is done by group, where a group may be a set of multiple users.

While SNMPv3 provides secure communications between human managers and the various managed elements in a network it is not enough for security of web based applications. For this, Secure Socket Layer (SSL) protocol and its extension the Transport Layer Security (TSL) protocol extend SNMP features to web-based applications.

SSL – Secure Socket Layer

SSL is a protocol designed to enable encrypted, authenticated communications across the Internet, and is used mostly in communications between web browsers and web servers. When a web URL begins with “https”, rather than “http”, this indicates that an SSL connection will be used, providing authentication, as well as privacy and message integrity (through encryption). Another way of explaining SSL is to say that it ensures that the information is sent, unchanged, only to the server to which the sender intended to send it, eliminating eavesdropping, tampering, and message forgery. SSL is use by online shopping sites, among other applications, to safeguard credit card information, and therefore, has already demonstrated a level of security that should be adequate and appropriate for industrial applications.

TLS – Transport Layer Security

TLS is a successor to SSL, using a wider variety of cryptographic algorithms for access security. It is standardized by the Internet Engineering Task Force (IETF). It is a protocol that provides secure communication over a TCP/IP connection such as the Internet. It uses digital certificates for authentication and digital signatures to ensure message integrity, and can use public key cryptography to ensure data privacy. A TLS service negotiates a secure session between two communicating endpoints. TLS is built into recent versions of all major browsers and web servers. Although the TLS and SSL protocols are not interoperable, TLS secure transport can back down to SSL 3.0 if a TLS session cannot be negotiated.

MAC Addressing

Another aspect of network security can be used to block computers from accessing the network by requiring the port to validate the Media Access Control (MAC) address against a known list of approved MAC addresses. If there is an insecure access on a secondary device connected to a switch, these levels of control allow authorized users to continue to access the network while unauthorized packets are dropped.

Remote Security

The further afield the users who have a need to access an industrial network, the more critical it is that the network design provide system-wide protection. Standards such as Remote Authentication Dial In User Service (RADIUS 802.1x), Terminal Access Controller Access Control System (TACACS+) make user identity secure. For additional data security, Secure Shell (SSH) extends total system security by shielding traffic running through the switch. Switch manufacturers assist in the support of data security using these standards, but the implementation requires broader compliance than that available at the individual switch.