19th International Power System Conference
نوزدهمین کنفرانس بین المللی برق
PSC 2004
98-E-DTC-524

Security of SCADA Systems

M. Sahebi **M.Ghaderpanah**
Dispatching & Control Dept., MATN co.

Keywords: SCADA, Cyber-security, Cyber threats, Vulnerabilities

Abstract:
Nowadays, security has been considered as a highest priority feature in SCADA (Supervisory Control And Data Acquisition) systems besides efficiency, throughput and time-response and makes such Real-Time systems differ from other information processing systems and business applications. Because of the potential risks involved with operations and data processing, concern for the security breaches, information theft and cyber threats, SCADA systems must provide a high level of security for all of their computer-based activities. This paper presents new strategies and approaches to strengthen control systems security

1. Introduction

For several years, security risks have been reported in SCADA systems, upon which many of the critical industries rely to monitor and control sensitive processes and physical functions. Real-time SCADA systems used in oil and gas industry installations have many features that differ from information processing systems used in business applications. Three of the most significant differences concern the design for efficiency, throughput and time critical response. Cyber attacks on energy production and distribution SCADA systems - including electric, oil, gas, and water treatment, as well as on chemical plants containing potentially hazardous substances - could endanger public health and safety, damage the environment, and have serious financial implications, such as loss of production, generation, or distribution of public utilities; compromise of proprietary information; or liability issues. When backups for damaged components are not readily available (e.g., extra-high-voltage transformers for the electric power grid), such damage could have a long-lasting effect. Some threats to nation's industries include: Criminal groups, Foreign intelligence services, Hackers, Hacktivists, Information warfare, Insider threat and Virus writers. In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of risks specific to control systems, as will be described separately in the article.

In order to effectively secure control systems, several challenges must be addressed. These include: the limitations of current security technologies in securing

control systems, the perception that securing control systems may not be economically justifiable, and conflicting priorities within organizations regarding the security of control systems. Government and private industry have initiated several efforts intended to improve the security of control systems. These initiatives include efforts to promote research

and development activities, form information

sharing and analysis centers, and develop new standards. In addition, we have made several recommendations for improving the federal government's critical industry protection efforts, which include control systems.

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business pose significant risks to the control systems and, more important, to the critical operations and industries. For example, telecommunications, power and gas distribution, water supply, public health services, national defense, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, may allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for malicious purposes, including fraud or sabotage.

2. Security Risks

Historically, security concerns about control systems were related primarily to protecting against physical attack and misuse of refining and processing sites or distribution and holding facilities. However, more recently, there has been a growing recognition that control systems are now vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

In certain industries such as chemical, power and gas generation, safety systems are typically implemented to mitigate a disastrous event if control and other systems fail. In addition, to guard against both physical attack and system failure, organizations may establish back-up control centers that include uninterruptible power supplies and backup generators.

2.1. Adopting Standardized Technologies with Known Vulnerabilities

Historically, proprietary hardware, software, and network protocols made it difficult to understand how control systems operated - and therefore how to hack into them. Today, however, to reduce costs and improve performance, organizations have been transitioning from proprietary systems to less expensive, standardized technologies such as Microsoft's Windows and Unix-like operating systems and the common networking protocols used by the Internet. These widely used standardized technologies have commonly known vulnerabilities, and sophisticated and effective exploitation tools are widely available and relatively easy to use.

As a consequence, both the number of people with the knowledge to wage attacks and the number of systems subject to attack have increased. Also, common communication protocols and the emerging use of Extensible Markup Language (commonly referred to as XML) can make it easier for a hacker to interpret the content of communications among the components of a control system.

2.2. Connecting to Other Networks

Enterprises often integrate their control systems with their enterprise networks. This increased connectivity has significant advantages, including providing decision makers with access to real-time information and allowing engineers to monitor and control the process control system from different

points on the enterprise network. In addition, the enterprise networks are often connected to the networks of strategic partners and to the Internet. Furthermore, control systems are increasingly using wide area networks and the Internet to transmit data to their remote or local stations and individual devices.

This convergence of control networks with public and enterprise networks potentially exposes the control systems to additional security vulnerabilities. Unless appropriate security controls are deployed in the enterprise network and the control system network, breaches in enterprise security can affect the operation of control systems.

2.3. Existing Security Technologies

According to industry experts, the use of existing security technologies, as well as strong user authentication and patch management practices, are generally not implemented in control systems because control systems operate in real time, typically are not designed with cyber-security in mind, and usually have limited processing capabilities. Existing security technologies such as authorization, authentication, encryption, intrusion detection, and filtering of network traffic and communications require more bandwidth, processing power, and memory than control system components typically have. Because controller stations are generally designed to do specific tasks, they use low-cost, resource-constrained microprocessors. In fact, some devices in the electrical industry still use the Intel 8088 processor, introduced in 1978. Consequently, it is difficult to install existing security technologies without seriously degrading the performance of the control system.

Further, complex passwords and other strong password practices are not always used to prevent unauthorized access to control systems, in part because this could hinder a rapid response to safety procedures during an emergency. As a result, according to experts, weak passwords that are easy to guess, shared, and infrequently changed are reportedly common in control systems, including the use of default passwords or even no password at all. In addition, although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Consequently, vendor-provided software patches are generally either incompatible or cannot be implemented without compromising service by shutting down "always-on" systems or affecting interdependent operations.

2.4. Insecure Connections

Potential vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access links - such as dial-up modems to equipment and control information - open for remote diagnostics, maintenance, and examination of system status. Such links may not be protected with authentication or encryption, which increases the risk that hackers could use these insecure connections to break into remotely controlled systems.

Also, control systems often use wireless communications systems, which are especially vulnerable to attack, or leased lines that pass through commercial telecommunications facilities. Without encryption to protect data as it flows through these insecure connections or authentication mechanisms to limit access, there is limited protection for the integrity of the information being transmitted.

2.5. Availability of Information

Public information about industries and control systems is available to potential hackers and intruders. In the electric power industry, open sources of information - such as product data and educational videotapes from engineering associations - can be used to understand the basics of the electrical grid. Also, industry publications, maps, and material available on the Internet - is sufficient to allow someone to identify the most heavily loaded transmission lines and the most critical substations in the power grid.

In addition, significant information on control systems is publicly available - including design and maintenance documents, technical standards for the interconnection of control systems and RTUs, and standards for communication among control devices - all of which could assist hackers in understanding the systems and how to attack them. Moreover, there are numerous former employees, vendors, support contractors, and other end users of the same equipment worldwide with inside knowledge of the operation of control systems.

3. Cyber Threats & Securing Challenges

Entities or individuals with malicious intent might take one or more of the following actions to successfully attack control systems:

- Disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators.
- Make unauthorized changes to programmed
- instructions in PLCs, RTUs, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), or even disabling of control equipment.
- Send false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
- Modify the control system software, producing unpredictable results.
- Interfere with the operation of safety systems.

In addition, in control systems that cover a wide geographic area, the remote sites are often unstaffed and may not be physically monitored. If such remote systems are physically breached, the attackers could establish a cyber connection to the control network. Several challenges must be addressed to effectively secure control systems against cyber threats.

3.1. Limitation of Current Cyber-securing Technologies

A significant challenge in effectively securing control systems is the lack of specialized security technologies for these systems. The computing resources in control systems that are needed to perform security functions tend to be quite limited, making it very to use security technologies within control system networks without severely hindering performance. Although technologies such as robust firewalls and strong authentication can be employed to better segment control systems from enterprise networks, research and development could help address the application of security technologies to the control systems themselves. Information security organizations have noted that a gap exists between current security technologies and the need for additional research and development to secure control systems.

Research and development in a wide range of areas could lead to more effective technologies to secure control systems. Areas that have been noted for possible research and development include identifying the types of security technologies needed for different control system applications, determining acceptable performance trade-offs, and recognizing attack patterns for intrusion-detection systems.

3.2. Economical Feasibility

Experts and industry representatives have indicated that organizations may be reluctant to spend more money to secure control systems. Hardening the security of control systems would require industries to expend more resources, including acquiring more personnel, providing training for personnel, and potentially prematurely replacing current systems that typically have a lifespan of about 20 years.

Several vendors suggested that since there has been no confirmed serious cyber attack on U.S. control systems, industry representatives believe the threat of such an attack is low. Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for vendors to fund research to develop more secure control systems.

3.3. Organizational Priorities Conflict

Finally, several experts and industry representatives indicated that the responsibility for securing control systems typically includes two separate groups: IT security personnel and control system engineers and operators. IT security personnel tend to focus on securing enterprise systems, while control system engineers and operators tend to be more concerned with the reliable performance of their control systems. Further, they indicate that, as a result, those two groups do not always fully understand each other's requirements and collaborate to implement secure control systems.

These conflicting priorities may perpetuate a lack of awareness of IT security strategies that could be deployed to mitigate the vulnerabilities of control systems without affecting their performance. Although research and development will be necessary to develop technologies to secure individual control system devices, IT security technologies are currently available that could be implemented as part of a secure enterprise architecture to protect the perimeter of, and access to, control system networks. These technologies include firewalls, intrusion-detection systems, encryption, authentication, and authorization.

Officials from one company indicated that, to reduce its control system vulnerabilities, it formed a team composed of IT staff, process control engineers, and manufacturing employees. This team worked collaboratively to research vulnerabilities and test fixes and workarounds.

4. Security Strategies

The first step in creating an effective security strategy is to conduct an audit of the company's current SCADA system architecture in terms of hardware, operating systems, networking equipment, and enterprise and field connectivity. This should be done in conjunction with a review of the organization's existing administration and operating policies. A logical approach for structuring the audit is to analyze the entire system, based on the flow of information, starting at the initial collection point, represented by the field equipment. (a typical SCADA system is shown in Fig.1)

4.1. SCADA and Telecommunication

Local and remote access implementations span a wide range of communications media: Internet, LAN, dialup modems, leased-lines, frame relay, ISDN, DSL, cable modems, satellite, microwave, packet radio, wireless LANs, cellular, VPN, browsers, etc. In current technology SCADA systems, the telecom medium does not encrypt the data packets and is transparent to the application, which creates a point of vulnerability. Since most of these telecom media have historically been dedicated to SCADA system operations, the traditional view has been to consider this layer of technology as a relatively low security priority. However, recent industry trends have resulted in relatively secure dedicated networks being replaced by networks shared by a variety of third party users. Since most networks now use Ethernet TCP/IP the default transport protocol, it is prudent to consider implementing the IP Security Protocol (IPSEC) standard at the middleware layer for these shared networks.

Within the SCADA host system, an assessment should examine the technical controls including: latest patches for all embedded software, Network equipment access controls, SCADA and historical servers access controls, Physical security, Console security, Virus protection strategy , and Authorization according to principles of limited access and areas of responsibility.

4.2. User Authentication & Authorization

Securing the user login to a network, system, or application is critical. The user login must have a secure user authentication architecture and be designed to prevent intentional and unintentional misuse by users. Hackers and other adversaries attack user authentication systems to recover user credentials, thereby allowing a hacker to launch attacks with the compromised user's rights. User authentication has two critical goals. First, it must uniquely identify the user. To do this, the SCADA software determines what each user can view and what tasks he or she can perform, based on that user's identity. Second, users must provide credentials to prove they are who they claim to be. While this might seem to be a simple task, many applications have developed proprietary user authentication systems that are insecure, difficult to manage, and very complex for the users.

While authentication uniquely identifies a user and verifies the user is who he or she claims to be, authorization also determines what an authenticated user is allowed to do. Authorization is controlled at three different levels.

- Role-based access control determines what functions a user is able to perform.
- Area of Responsibility (AOR) access control determines what areas of the SCADA system a user can view and control.
- For installations with multiple control centers, appropriate access control determines what areas of the SCADA system a user can see or control at each control center.

Audit logs are helpful in identifying security attacks and performing computer forensics. Directory services allows for logging of all login attempts. Logs are most useful if they are monitored and reviewed on a timely basis. For example, if the operations center is monitoring failed logins, they will identify when a malicious user is trying to guess a password.

4.3. Enterprise Network

The "enterprise" connectivity of the SCADA system is the area of highest vulnerability. This level consists of: Remote SCADA clients, mobile phones, Clients of an online trading/broker system, Accounting, Asset Management, Graphical Information Systems, Work Flow Management, and Web connections to services. Before real-time data is fed into the above systems, it is essential to conduct a thorough risk analysis to assess the level of protection and the necessity of each connection to the SCADA network. The data is made available through the following interface connections:

- **Firewalls.** Most of the above systems communicate with the SCADA database via a border router and firewalls. Firewalls, properly configured, can protect passwords, IP addresses, files and more. However, without a hardened operating system, hackers can directly penetrate private internal networks or create a Denial of Service (DoS) condition, rendering the firewall useless. The most popular firewall-based security approach is the Stateful inspection — intelligent Packet filter.
- **Web and proxy servers.** Most of the web clients are delivered data through web / proxy servers. Proxy servers are critical to recreate TCP/IP packets before passing them to, or from application layer resources such as HTTP and SMTP. The deployment of proxy servers will not, however, eliminate the threat of application layer attacks.
- **Network segmentation.** When designing a system network, it is important that each SCADA network is segmented off into its own IP segment. The use of hubs should be avoided; smart switches should instead be utilized. It is also important to use proper sub-masking techniques to protect the SCADA environment from other network traffic such as file and print commands.

Because Ethernet TCP/IP is the most prevalent transport protocol, encryption at the IP layer (IPSEC), data line layer middleware (L2TP) and transport layer (SSL from Netscape) should be considered. IP Version 6 by default offers greater encryption and security.

4.4. Creating a Security Plan

It is evident from the above discussion that a security breach can potentially occur at any level. A good SCADA security plan must take a number of factors into account:

- The security audit should include an internal vulnerability scan on all devices in the SCADA system.
- The "complete" system (SCADA and corporate networks) must be included in the analysis, so that all risks can be identified and mitigated as a whole.
- The security plan must be built on a framework that allows for ease of implementation and quick action. The foundation of this framework is the set of company IT policies and procedures that address system security. Developing, documenting and enforcing effective security policies represent a significant company effort. Proper implementation of those policies and procedures, however, is critical — not only as part of the security program, but also as a mechanism for reducing legal liabilities and helping to ensure subsequent prosecution of violators. Regular review of these policies should also be conducted, to ensure they are current with the latest hardware and software technologies.

4.5. Security Training

The weakest link in cyber-security might be more of a people issue than a technology issue, according to a survey from the Information Technology Association of America (ITAA) and the META Group. In that survey, respondents cited issues such as employee training (27 percent), information security processes and methods (18 percent), and background checks (11 percent) as areas of weakness. Despite claims that supervisory control and automated data acquisition systems — intelligent devices that control oil and gas pipelines, water transmission and distribution systems and electrical systems — might be the target of a cyber-attack, the survey found a relatively low percentage of respondents expressing a high degree of concern in this area (29 percent felt the likelihood of such an attack to be high or extremely high, whereas 33 percent said the likelihood was low or extremely low). The survey also uncovered interesting views on the best methods for acquiring information security skills. Certification programs pulled the highest ratings (at 48 percent), followed by on-the-job training (40 percent). This complements the directives of the Department of Transportation (DOT) for mandatory SCADA operator training through the use of training simulators. This DOT mandate also provides for security instruction to be included in the required training sessions.

4.6. Security Outsourcing

If security isn't your company's core competency, there are outsourcing resources that are available, which can provide some significant benefits over an in-house approach,

such as:

- **No need for hiring your own security professionals**.
- **Training is part of the package**. A qualified outsourcer will be able to provide you with ongoing support, will be up to date on the latest security issues, and will assist you in separating the security facts from the security myths.
- **24x7 coverage is standard**. This means you won't have to have the necessary in-house staff required for 24-hour monitoring and management of security incidents. A good outsourcer will provide an operations center and incident response team to ensure incidents are handled with care and

managed from detection to resolution, ensuring quality control at every step. Outsourcers have extensive knowledge of the security market, both locally and globally, to keep you informed and make recommendations that will enhance your security program and will allow your business to continue to grow. Many outsourcing firms also offer additional value-added services such as auditing, penetration testing, security policy documentation, security solution design and implementation, disaster recovery, education, monitoring, and proactive management planning.

- **Cost savings are tangible and measurable.** Because information security management is in the hands of experts, this allows you to focus all of your resources on your core competency, thereby increasing internal efficiency. SCADA vendors can be a viable option to outsource this service as they possess intimate knowledge regarding their respective products.

5. Conclusions

Industries have taken a broad look at the cyber-security requirements of control systems and have initiated several efforts to address the technical, economic, and cultural challenges that must be addressed. These cyber-security initiatives include efforts to promote research and development activities, develop process control security policies, and encourage security awareness and information sharing. In summary, it is clear that the systems that monitor and control the sensitive processes and physical functions of the nation's industries are at increasing risk to threats of cyber attacks. Securing these systems poses significant challenges. Both government and industry can help to address these challenges by lending support to ongoing initiatives as well as taking additional steps to overcome barriers that hinder better security.

6. References

[1] Dana A. Shea, Control Systems and the Terrorist Threat, 2003.
[2] Deepak Munshi, Telvent, Security Fundamentals for SCADA Environments, 2002.
[3] Joe Falco, Keith Stouffer, National Institute of Standards and Technology, 2003.
[4] Lance Travis, New Security Technology, 2003.
[5] Securing Wireless LANs, Bultimore Technologies, 2003.
[6] Safe Extending the Security to Midsize and Remote-User Networks, Cisco Systems, 2001.
[7] Embedded Network Security, Interpeak Inc., 2001.

Fig.1. a Typical SCADA System