riptech℠

Understanding SCADA System Security Vulnerabilities

Talking Points

- **Executive Summary**
- **Common Misconceptions about SCADA System Security**
- **Common Vulnerabilities Affecting SCADA Networks**
- **Tactics to Strengthen SCADA System Security**
- **About Riptech**

EXECUTIVE SUMMARY

In October 1999, a computer hacker publicly announced his intention to release a report outlining how to break into power company networks and shut down the power grids of 30 United States utility companies[i]. This event, which coincided with warnings from one federal Government agency that "one person with a computer, a modem, and a telephone line anywhere in the world can potentially…cause a power outage in an entire region"[ii], resulted in heightened industry concern about network security.

Since these announcements, heated debates have ensued concerning the level of security for backbone operations systems of utilities (commonly referred to as supervisory control and data acquisition (SCADA) systems). Based on extensive experience gained by assessing the security posture of many of the nation's largest utility companies, the following article sheds light on just how vulnerable utility networks are to cyber attack. The article also explains the types of vulnerabilities commonly found at utility companies, as well as remediation strategies that utility companies should adopt to mitigate risk.

[i] "The Next Y2K?" *Utilities IT*, February 2000.

[ii] Remarks of John Tritak, Director of the Critical Infrastructure Assurance Office (CIAO) as quoted in "The Next Y2K?" *Utilities IT*, February 2000.

COMMON MISCONCEPTIONS ABOUT SCADA SYSTEM SECURITY

At the heart of the issue of SCADA system security are three major misconceptions that are commonly held by utility managers. The experiences of Riptech network security professionals point to the misconceptions, listed on the following page, as the major obstacles to the implementation of the best possible information security strategies.

- **MISCONCEPTION #1** – *"The SCADA system resides on a physically separate, stand-alone network."*

Most SCADA systems were originally built before and often separate from other corporate networks. As a result, IT managers typically operate on the assumption that these systems cannot be accessed through corporate networks or from remote access points. Unfortunately, this belief is usually fallacious.

In reality, SCADA networks and corporate IT systems are often bridged as a result of two key changes in information management practices. First, the demand for remote access computing has encouraged many utilities to establish connections to the SCADA system that enable SCADA engineers to monitor and control the system from points on the corporate network. Second, many utilities have added connections between corporate networks and SCADA networks in order to allow corporate decision makers to obtain instant access to critical data about the status of their operational systems. Often, these connections are implemented without a full understanding of the corresponding security risks. In fact, the security strategy for utility corporate network infrastructures rarely accounts for the fact that access to these systems might allow unauthorized access and control of SCADA systems.

- **MISCONCEPTION #2** – *"Connections between SCADA systems and other corporate networks are protected by strong access controls."*

Many of the interconnections between corporate networks and SCADA systems require the integration of systems with different communications standards. The result is often an infrastructure that is engineered to move data successfully between two unique systems. Due to the complexity of integrating disparate systems, network engineers often fail to address the added burden of accounting for security risks.

As a result, access controls designed to protect SCADA systems from unauthorized access through corporate networks are usually minimal, which is largely attributable to the fact that network managers often overlook key access points connecting these networks. Although the strategic use of internal firewalls and intrusion detection systems (IDS), coupled with strong password policies, is highly recommended, few utilities protect all entry points to the SCADA system in this manner.

- **MISCONCEPTION #3** – "*SCADA systems require specialized knowledge, making them difficult for network intruders to access and control."*

The above misconception assumes that all attackers of a SCADA system lack the ability to access information about their design and implementation. These assumptions are inappropriate given the changing nature of utility system vulnerabilities in an interconnected environment. Due to the fact that utility companies represent a key component of one of the nation's critical

infrastructures, these companies are likely targets of coordinated attacks by "cyber-terrorists", as opposed to disorganized "hackers." Such attackers are highly motivated, well-funded, and may very well have "insider" knowledge. Further, a well-equipped group of adversaries focused on the goal of utility operations disruption is certain to use all available means to gain a detailed understanding of SCADA systems and their potential vulnerabilities.

Furthering this risk is the increasing availability of information describing the operations of SCADA systems. To support competition in product choices, several standards for the interconnection of SCADA systems and remote terminal units (RTUs) have been published, as have standards for communication between control centers, acceptance of alarms, issuance of controls, and polling of data objects. Further, SCADA providers publish the design and maintenance documents for their products and sell toolkits to help develop software that implements the various standards used in SCADA environments.

Finally, the efforts of utility companies to make efficient use of SCADA system information across their company has led to development of "open" standard SCADA systems. As a result of this development, SCADA system security is often only as strong as the security of the utility's corporate network. While the RTUs on a network may be difficult to access outside of the dedicated serial lines, it is only moderately difficult to penetrate the control panel for the SCADA manager through the corporate network and quickly 'learn' commands by watching actions that are carried out on the screen. Attacks on highly complex systems become much easier when attackers first penetrate the workstations of SCADA operators.

COMMON SECURITY VULNERABILITIES AFFECTING SCADA NETWORKS

As described in the previous section, corporate networks and SCADA systems are often linked, which means that the security of the SCADA system is only as strong as the security of the corporate network. With pressure from deregulation forcing the rapid adoption of open access capabilities, vulnerabilities in corporate networks are increasing rapidly. The following section outlines several common system vulnerabilities found on SCADA and corporate networks that impact the relative security of SCADA systems:

Public Information Availability

Often, too much information about a utility company corporate network is easily available through routine public queries. This information can be used to initiate a more focused attack against the network. Examples of this vulnerability are listed below:

- Websites often provide data useful to network intruders about company structure, employee names, e-mail addresses, and even corporate network system names

- Domain name service (DNS) servers permit "zone transfers" providing IP addresses, server names, and e-mail information

Insecure Network Architecture

The network architecture design is critical in offering the appropriate amount of segmentation between the Internet, the company's corporate network, and the SCADA network. Network architecture weaknesses can increase the risk that a compromise from the Internet could ultimately result in compromise of the SCADA system. Some common architectural weaknesses include the following:

- Configuration of file transfer protocol (FTP), web, and e-mail servers sometimes inadvertently and unnecessarily provides internal corporate network access.
- Network connections with corporate partners are not secured by firewall, IDS, or virtual private network (VPN) systems consistent with other networks
- Dial-up modem access is authorized unnecessarily and maintenance dial-ups often fail to implement corporate dial access policies
- Firewalls and other network access control mechanisms are not implemented internally, leaving little to no separation between different network segments

Lack of Real-Time Monitoring

- Vast amounts of data from network security devices overwhelm utility information security resources rendering monitoring attempts futile
- Even when intrusion detection systems are implemented, network security staff can only recognize individual attacks, as opposed to organized patterns of attacks over time

TACTICS TO STRENGTHEN SCADA SYSTEM SECURITY

The most effective information security strategies for utility companies blend regular, periodic security assessments with an ongoing attention to security architecture and monitoring. The following steps highlight the major steps to minimize the number and impact of security breaches.

STEP 1: *Regular Vulnerability Assessments*

Many utilities fail to regularly assess the vulnerabilities of their SCADA and Energy Management Systems (EMS) systems, on a regular, re-occurring basis. In addition to assessing operational systems, corporate networks, web servers, and customer management systems should also be assessed to reveal unintended gaps in security, including unknown links between public and private networks, and firewall configuration problems.

STEP 2: Expert Information Security Architecture Design

An overwhelming number of security technologies, networking devices, and configuration options are available to utility companies. While firewalls, IDSs, and VPNs can all help protect networks from malicious attacks, improper configuration and/or product selection can seriously hamper the effectiveness of a security posture. In order to minimize risks associated with network architecture design, utilities should work with information security professionals to ensure that evolving network architectures do not compromise information security.

STEP 3: Managed Security

As companies deploy network security technologies throughout their networks, the need to properly manage and monitor these devices is becoming increasingly complex. Unfortunately, the implementation of "technology-only" solutions without close monitoring and management significantly weakens the effectiveness of security devices. Hiring experienced IT security professionals to monitor network security devices can help to mitigate risk; however this option is cost-prohibitive for most, if not all, utility companies. As a result, many organizations are outsourcing the management and monitoring of security devices to highly specialized, managed security companies. Managed security services ensure that all security devices are configured properly and fully patched, while monitoring the actual activity on each device to detect malicious activity in real time. Managed security services enable corporations to maintain a real-time security monitoring capability at a relatively low cost, and simultaneously increase the value of existing information security devices by enhancing their performance and capabilities.

ABOUT RIPTECH

Riptech [SM], the premier information security services provider, delivers Real-Time Information Protection [SM] through a comprehensive suite of Real-Time Managed Security Services and Security Professional Services. Riptech secures clients through around-the-clock security management, monitoring, analysis and response delivered by security experts in world-class Security Operations Centers using a proprietary, next generation intelligent technology platform. This platform is capable of processing large volumes of network security data to separate actual security threats from false positives in real-time, with nearly limitless scalability. Additionally, Riptech's Security Professional Services group provides security policy development, assessment and auditing, penetration testing, incident forensics, and response. Riptech has secured hundreds of organizations including Fortune 500 companies, emerging e-Businesses, and federal agencies. Founded in 1998 by former U.S. Department of Defense security professionals and market experts, Riptech is headquartered in Alexandria, Virginia.

