CRITICAL INFRASTRUCTURE AND SCADA SYSTEMS SECURITY

The continuous growth of cyber security threats and attacks including the increasing sophistication of the malware is impacting the security of critical infrastructure, industrial control systems, and SCADA control systems. Since the emergence of Internet and World Wide Web technologies, these systems were integrated with the business systems and became more exposed to the cyber threats.

SCADA Security Overview

Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other smaller control system configurations including skid-mounted Programmable Logic Controllers **(**PLC**)** are often found in the industrial sectors and critical infrastructures. These are also known under a general term, Industrial Control System (ICS). A control system is a device or set of devices to manage, command, direct or regulate the behavior of other devices or systems. ICS**s** are typically used in industries such as electrical, water, oil and gas, chemical including experimental and research facilities such as nuclear fusion laboratories. The reliable operation of modern infrastructures depends on computerized systems and SCADA systems.

The Presidential Decision Directive 63 document established the framework to protect the critical infrastructure and the Presidential document of 2003, the National Strategy to Secure Cyberspace stated that securing SCADA systems is a national priority.

The critical infrastructure includes telecommunication, transportation, energy, banking, finance, water supply, emergency services, government services, agriculture, and other fundamental systems and services that are critical to the security, economic prosperity, and social well-being of the public. The critical infrastructure is characterized by interdependencies (physical, cyber, geographic, and logical) and complexity (collections of interacting components). Cyber interdependencies are a result of the pervasive computerization and automation of infrastructures. The critical infrastructure disruptions can directly and indirectly affect other infrastructures, impact large geographic regions, and send ripples throughout the national and global economy. For example, under normal operating conditions, the electric power infrastructure requires fuels (natural gas and petroleum), transportation, water, banking and finance, telecommunication, and SCADA systems for monitoring and control.

SCADA systems are exposed to the same cyberspace threats like any business system because they share the common vulnerabilities with the traditional Information Technology (IT) systems. Also, most SCADA systems are not protected with appropriate security safeguards. The operating personnel are lacking the security training and awareness. Threats against SCADA systems are ranked high in the list of government concerns, since terrorists have threatened to attack several SCADA systems of critical infrastructure and successfully launched near-disastrous attacks. In addition, recent attacks are becoming more sophisticated and the notion of what kind of vulnerabilities actually matter is constantly changing. For example, timing attacks

are now common threats, whereas only a few years ago they were considered exotic. The threats are often poorly understood and ignored, and the vast majority of organizations lag in realizing secure infrastructures. In complexly interactive systems whose elements are tightly coupled, great accidents are inevitable. Vulnerabilities and attacks could be at different levels – software controlling or controlled device, application, storage, data access, LAN, enterprise, Internet, communications.

Improving SCADA Security

Internet and global e-business application requirements demand that companies increasingly implement computing infrastructures specifically designed for at least 99.999 percent availability. High availability of the environment, at least 99.999 is the equivalent of less than 5.3 minutes of downtime a year. This is also a requirement for the SCADA networks. In response to these trends, government and SCADA owners need to address increased security and support for high availability.

More efforts should be planned to reduce the vulnerabilities and improve the security operations of these systems. It is necessary to address not only the individual vulnerabilities, but the breadth of risks that can interfere with critical operations.

In control systems, a component failure greatly increases the likelihood of multiple simultaneous failures. Also, the high-speed of SCADA networks facilitates the quick propagation of malicious code. We provide sound and innovative approaches for security management.

Innovative Risk Management Approaches

Information security management is a continual cyclical process comprised of key phases such as assessment (risk management approach), policy, implementation, training, and auditing. Risk management characterizes an overall process to identify, measure, control, and minimize losses associated with uncertain events or risks. The first phase called risk assessment includes analyzing assets, identifying vulnerabilities and potential risks due to threats, risk reducing measures, and decisions related to the acceptance, avoidance, or transfer of risk. Risk assessment characterizes both the process and the result of analyzing and assessing risk. The second phase includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures. General models for managing risk through its various phases are available for IT systems. However, methods for risk management that are based on automated tools and intelligent techniques are more beneficial to SCADA systems because they require minimum or no human intervention in controlling the processes.

The key issue in managing the risk is reducing the vulnerabilities and causes of the vulnerabilities. A vulnerability is a problem that can be exploited by an attacker. To measure risk in a system, it is necessary to identify the vulnerabilities, threats, and asset values. In assessing

the risk for SCADA systems, use of general methods for risk analysis including specific conditions and characteristics of a control system need to be applied.

Another important issue is applying vulnerability management life cycle that offers guidance on design and operational processes and technologies needed to find and remediate security weaknesses before they are exploited. It is imperative to analyze risk as a function of asset value, threat and vulnerability. New concepts to analyze the threats and vulnerabilities have to be applied regularly and uniformly.

Although security management including its component - risk management, is an evolving research area, many of the principal developments in other areas such as control theory, dynamic systems, real-time and complex systems, system identification, information theory, etc could provide an impulse to increase the efficiency and effectiveness of risk management for better protection of SCADA computing systems.

We identify key activities necessary to conduct an accurate assessment of risks. Along with these key activities, in order to enforce a minimum level of security of SCADA systems, we apply engineering solutions based on system identification and process control model methods which are vital for security risk management of control systems. Analysis of security risks for SCADA control systems using risk management and decision making based on advanced approaches and sound data are the norm. These methods are beneficial to ensure security protection and meet business needs and user requirements.

Process Control Techniques

Security problem is about to understand what the problem is and how to manage it. The application of process control model is our strategy. The SCADA network and the endpoints that populate it can be expressed as a closed loop process control problem. When assessing the risks, it is required to evaluate the threats and potential attack methods including the target endpoints and the probability, or, risk that a cyber attack will succeed. By using process control model, we can identify metrics that have greater impact on security. We can identify inputs, outputs, and the feedback in a network as well as for endpoints. For example, we can add time constraints to associate it with the control process. Then the model is used for identifying the risk to be introduced in a network and setting a low limit to endpoints for security criteria. When approaching the problem of security using closed loop process control model, we need to identify those components (nodes) in SCADA network that can assist with the basic modes of control: proportional, integral, and derivative controls.

A device can be a control node – a place used to enforce a condition or extract data for the purpose of managing the process. A control node can have the capability to decide about the traffic or the status of the device. In other words, the device reporting data can enable a human to make decisions in support of either derivative or integral control functions. Most of the devices in a SCADA network, with a few exceptions, can be categorized as performing derivative

controls. By using log data collected by a device, we can enable an integral control. Following these activities, we get a mapping of devices (hardware, software, logs, alerts, probes, correlation) to control modes. Next, we identify the control signals using metrics that are security relevant such as failed login attempts, firewall rule violations, access attempts, alerts, new software requests, new protocol connections, network access requests, etc. By using this model, we can set a more accurate and acceptable limit of risk for SCADA networks to protect more effectively.

Therefore, use of engineering methods based on system identification and process control lead to building more accurate and more complete models for improving security risk management of SCADA control systems. Thus, the standards for risk management should be reevaluated and enhanced accordingly to ensure more secure SCADA control systems.