Control System Security: Threat Detection and Management in the Critical Infrastructure

By Eric D Knapp
October, 2009
Introduction

Many of the world’s critical infrastructure networks—such as power, water and other utilities, as well as many manufacturing, processing and transportation systems—are becoming more intelligent. This translates to digital communications to and from a myriad of complex processes and controls. Referred to as Control Systems, these networks represent the heart of the utility company. The control systems are responsible for power generation and distribution, as well as the monitoring of those functions for metering, safety, and other purposes that are critical to the successful distribution of power.

In short, these control systems are vital to the successful operation of those utilities and facilities that make up our critical infrastructures. For that reason, they are a target for cyber attacks—a breach of these systems could result in catastrophic outages, or worse.

These control systems can be secured, using a tiered network security approach similar in design to standard enterprise information security best practices. However, because the networks and protocols used are highly specialized, care and planning is required to ensure that the protective monitoring, blocking and management systems are fully aware of the unique nature of the control system.

This whitepaper discusses how to implement a combination of Deep Packet Inspection (Intrusion Prevention and/or Application and Protocol Monitoring), Database Activity Monitoring, and Security Information & Event Management systems (SIEM) to secure our critical infrastructure. NitroSecurity’s NitroView Enterprise Security Manager combines the necessary functions of SIEM, IPS, Database Monitoring, and Application Monitoring functions into a single solution, and is therefore highly suited for use in control system security.

The implementation of adequate security and monitoring into these networks will further satisfy the specific regulatory compliance requirements of the North American Electric Reliability Corporation standards for Critical Infrastructure Protection (NERC-CIP).

NOTE: This document is a companion to the SANS Analyst Program Whitepaper, “Securing a Smarter Grid: Risk Management in Power Utility networks,” by Matthew E Luallen, which is available at http://www.sans.org/reading_room/analysts_program/
Control System Security Requirements

Step 1. Identifying Critical Assets & Understanding Risk

The SANS Institute defines risk management as a process consisting of:

- The identification of critical assets.
- The identification of weaknesses associated with those assets.
- The probability of loss expectancy.
- The appropriate risk mitigation tactics to continue to ensure the assets sustain value. ¹

Luckily, the process of identifying assets and assessing risk can be facilitated using a variety of available tools, including:

- Vulnerability Assessment (VA) systems, which can discover network attached devices and determine the respective vulnerability of those devices to known exploits and attacks.

- Database Monitoring systems, which can detect available database(s), as well as the presence of sensitive information within those data stores. Database monitors are also an important part of the recommended security of the critical assets themselves. This is because many databases within the control system are accessed directly by applications within less secure business LANs, and even the public Internet.

- Security Information & Event Management (SIEM) systems, which can utilize asset information within a global threat detection, analysis and reporting framework. NitroView Enterprise Security Manager provides VA, asset and inventory management features to specifically facilitate these requirements.

NitroView integrates asset and vulnerability management, allowing the security professional to monitor and analyze cyber assets and associated risks from directly within the SIEM.

The VA system, of course, is critical to the determination of how a given asset is, or isn’t, vulnerable to a given threat or event. This is especially important because of the wide range of asset types and associated vulnerabilities identified by SANS that are relevant to control system security (see “Securing a Smarter Grid: Risk Management in Power Utility networks,” Table 1: Threats to Control System Cyber Assets, http://www.sans.org/reading_room/analysts_program/).

Of the vulnerabilities discussed, exploits fall into several clear categories:

- **Direct**; Lower-level network and protocol vulnerabilities, targeting environmental management systems, PLCs, and other various control systems. These types of attacks are detectable by a SCADA NIDS or NIPS.

- **Direct**; Higher-level applications and session vulnerabilities, targeting systems such as HMI (Human Machine Interface), specific controllers, and systems such as Historian. Most easily detectable through dedicated database or application monitoring, these attacks may also be detectable using SIEM to analyze appropriate logs from key database and application resources.

- **Indirect** attacks, often using a combination of vulnerabilities to identify and exploit critical assets, through a variety of attack vectors. These more sophisticated attacks are only detectable through the correlation of observed activity across multiple systems and networks, using a SIEM.
Step 2. Establishing a Defensible Perimeter with Security Enclaves
The concept of a “Security Enclave” is simple: group critical assets according to function and role so that they can be isolated as much as possible from unauthorized access.

A variety of commercial devices are available for the isolation of an established enclave. Ideally, all implemented devices would be able to provide information into the SIEM, via logging or some other mechanism, to allow for the correlation of all alarm and event activity across all systems. This is crucial to the detection of more sophisticated attacks, which may go undetected when viewed in isolation.

Best practices dictate a layered defense consisting of:

- Firewalls.
- Intrusion Prevention Systems.
- Anti-Virus / Anti-Malware.
- Application White-listing.

In addition, monitoring of specific application, protocol and data access activity is recommended. These systems add valuable context to the SIEM and can be used to identify threats that might otherwise go undetected. Additionally, establishing a relationship between users, applications, and data access provides the detail needed to produce an effective audit trail for compliance purpose. Systems that provide this level of monitoring include:

- Database Activity Monitors (DBM or DAM).
- Application and Protocol Monitors (APM).

Finally, defenses such as physical security and human monitoring control points must be factored into the establishment of an enclave. Less conventional measures, such as deterministic monitoring and filtering, probabilistic risk assessment (PRA), etc. should also be considered for monitoring the interactions among systems, controls, and controllers.

NitroSecurity provides an integrated IPS, DBM, APM and SIEM solution to meet the monitoring, protection, and remediation needs of both the control system and interconnected, outlying networks.

More information about NitroView can be found at nitrosecurity.com
Implementing the layered security, however, can be complex due to the multitude of attack vectors that are present to control systems. In addition, new vectors are continually occurring, primarily through the natural implementation of business applications, and an increasingly smarter distribution grid. Using the example of a power utility, this would include the use of smart meters and other ‘smart grid’ technologies as attack vectors. Vectors are also made available through open wireless access points in field locations, vendor “back doors” into equipment for maintenance and control purposes, etc.

Some common vectors include:

- Grid/distribution networks
- Remote field stations / remote office networks
- Vendor “back doors” (equipment maintenance access)
- Business networks & associated business applications
- Physical access to secure terminals

![Attack Vectors Diagram]
This presents some unique challenges to the security infrastructure. For example, a SIEM must have visibility to these outlying areas, in addition to visibility within the control systems’ enclave. Contemplate the following scenarios:

1. A port scan of control network system ports is detected within a control system — *this is straight forward, and indicates a targeted attack. It is easily detected, and can be correlated against other events by the SIEM.*

2. Multiple scans, consisting of common ports as well as control network system ports, is detected in an adjacent business LAN. File transfers are detected from an outside IP to a corporate web server. That server is later seen communicating to internal firewalls that separate the business LAN from the Control System enclave — *this may indicate a more sophisticated attempt to access the control system through the utility’s business LAN. This requires the SIEM to maintain much broader visibility across all related systems.*

While the exact requirements of any network will vary based on the unique environment being protected, there are several key considerations that should be made when evaluating Intrusion Prevention Systems and other monitoring solutions that defend the perimeter of the enclave.

- They must be able to monitor the required SCADA systems and associated protocols (including modbus, ICCP, DN3P, etc).
- They must be able to monitor both SCADA systems and enterprise network systems, applying disparate sets of detection signatures to each. This is important due to the difference in protocol use between these environments.
- They must be able to operate in-line, reliably, without impact to network operations. Many SCADA systems have network performance and/or latency requirements that must be considered when introducing a device in-line.
- When monitoring database and application activity, the devices must not impact the operation or performance of the databases and applications they are protecting.
- Ideally, these devices should be able to operate concurrently in detection (IDS) and protection (IPS) modes, so that varying degrees of mitigating action can be taken, based upon the severity of the threat. This allows for the generation of alerts without blocking or impeding communication (IDS), while at the same time being able to actively prevent more severe threats from occurring (IPS).
- If deployed in remote stations or internal areas that are non-secured physically, they must themselves be secure² (this is true of SIEM and other security devices as well).

---

Some of the specific SIEM features and capabilities that must be considered include:

- The ability to integrate with Vulnerability Assessment (VA), including Database VA, to identify known vulnerabilities against critical assets.
- The ability to integrate events from the layered defenses (Firewalls, IPS, Database Monitors, etc), and provide correlation between disparate systems.
- Visibility into database and application activity, to ensure the integrity of all transactions to Historian and other databases within the secure enclave.
- The ability to centrally monitor the disparate networks (i.e., the business LAN, control system LAN, etc.), running disparate protocols (i.e., enterprise vs. SCADA), and often located in disparate geographic regions.
- The ability to monitor device configurations, and detect changes to authorized configurations, to ensure that established security enclaves remain properly configured and intact.
- The ability to manage inventories related to critical assets, including vulnerabilities and other relevant system/device information relevant to that asset.
- The ability to baseline both configurations (for change detection) and threat activity (for anomaly detection) within the context of the control system.
- The ability to normalize device messages from disparate security devices and other systems to allow common analysis and correlation between devices (e.g., so that a modbus protocol anomaly and a malformed SMTP session can both be categorized as suspicious protocol activity, despite the disparity in protocols and how the corresponding event messages are structured).
- The ability to control visibility into collected and managed information, so that unauthorized users of the SIEM remain isolated from details about or information collected from protected systems.
- The ability to collect, store and analyze logs or events directly from other specialized control system devices, servers, or applications that may be used. Because of the specialized nature of some systems, the SIEM should be customizable to some extent to support the collection and analysis of common logging formats (e.g., syslog).

The SIEM acts as a central point for the collection and analysis of all relevant information.

If using existing security solutions within the Control System, examine how those systems might be used by the SIEM to provide a more cohesive architecture of control system security management.
Step 3. Obtaining Situational Awareness


“Situational awareness is a widely discussed concept that is not easy to achieve without enduring information overload. It is very important to keep the awareness concise and directed to the parties that have the authority to make swift decisions. For example, immediately after an external party alerted the company to a new threat, the control network operator sees a breaker close after a failed login attempt by an individual that is not supposed to be using a Cyber Asset. This combination of awareness—blurred across physical, cyber and operational domains—can provide invaluable insight to the current operating state of the asset itself. The only effective way to truly manage the number of cyber security events (as well as correlate activity) is to deploy and utilize robust Security Information and Event Management (SIEM).”

Using a content- and context-aware SIEM such as NitroView Enterprise Security Manager is ideal for the required situational awareness. Context about location (network and geographic location), identity (user and IP), vulnerability (asset information vs. exploit targets), etc. are only possible using a SIEM, which is capable of fully integrating details about application and protocol usage (i.e., content) and details about assets, users, and activity (context) with the normal threat management capabilities of SIEM.

NitroView’s visibility into application content allows for much broader threat detection capability, as well as additional context around overall threat activity.

This provides, in addition to the monitoring and threat detection capabilities required to secure the critical infrastructure, all of the relevant information required to maintain an audit trail of all security activity, for purposes of NERC-CIP compliance.
Step 4. Incident Detection, Analysis and Response

Because of the catastrophic potential of a successful cyber attack against the critical infrastructure, incident response time (the time between detection & remediation) is of the utmost importance. Before a cyber security professional can be granted the authority to move, impede or disable operations based upon an incident, the incident must be detected, the operator must be alerted of the incident, and if any additional investigations are required—to determine the source of an attack, the affected systems, or other relevant details—those investigations must occur rapidly.

Therefore, in addition to the recommended practices outlined by Mr. Luallen in “Securing a Smarter Grid: Risk Management in Power Utility networks,” the responsiveness of the underlying systems must also be evaluated. This is an especially important consideration for the SIEM, which is the central and primary tool for the identification, investigation and remediation of threats.

NitroView’s Configuration Management Dashboards allow for change events to be managed and correlated against other threat activity. Specific device configurations can also be viewed directly from within the system (shown)
Conclusion

The nature of a utility control system presents a cyber security challenge: these systems are a prime target for cyber attack, and the results of a successful attack could be devastating across corporate, political and socio-economic borders. In addition, the interdependence of new technologies and applications upon these controls—such as Smart Grids, web-based applications, and even smart phone SCADA control applications—has blurred the defensive wall between the control system’s secure enclave. The result is a highly complex system that is difficult to monitor and secure.

However, by understanding the requirements of the control system, its assets, and their vulnerabilities, an enclave can be established using a layered security approach. This requires a unique set of requirements for firewalls, Intrusion Prevention Systems, Database Monitors, and other security devices. It also requires the implementation of a Security Information and Event Management (SIEM) solution that is capable of providing visibility within that enclave—as well as to all other related networks, systems, users and applications outside of the enclave.

The end result is a comprehensive, layered Cyber Security architecture capable of detecting, analyzing and responding to threats against the critical infrastructure.