Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks

Dale Peterson
Director, Network Security Practice
Digital Bond, Inc.
1580 Sawgrass Corporate Parkway, Suite 130
Sunrise, FL 33323

KEYWORDS:

Intrusion Detection, IDS, SCADA, MSSP, Cyber Security

ABSTRACT:

Governments and industry organizations, including ISA, have recognized that Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and other process control networks, referred to as SCADA networks in this paper, are potential targets of attack from hackers, disgruntled insiders, cyber terrorists, and others who want to disrupt the critical infrastructure.

This paper describes how current intrusion detection and cyber security monitoring products and services used in IT enterprise networks can provide early identification of attacks from the most common threat agents. The deficiencies of the current general IT solutions are discussed, and future SCADA specific solutions are described. Special emphasis is placed on how intrusion detection can serve as a compensating security control for the lack of security in field communications.

INTRODUCTION:

In a recent GAO report[1], the US Government identified five trends that have escalated the risks to SCADA networks:

1. adoption of standardized technologies with known vulnerabilities,
2. connectivity of control systems to other networks,
3. constraints on the use of existing security technologies and practices,
4. insecure remote connections, and

5. widespread availability of technical information about control systems.

These trends have moved the SCADA networks from proprietary, closed networks to the arena of Information Technology (IT) with all its cost and performance benefits and IT security challenges. The transformation continues to be gradual and may take ten or more years to complete as expensive legacy systems cannot be replaced overnight. This leaves the SCADA community with a large challenge of providing the appropriate IT security for a mission critical network with systems and applications that were not designed for the general IT environment and its inherent security risks.

New SCADA systems are being designed with better security features and this improvement is likely to continue as customers demand certified secure solutions. A number of efforts are underway to retrofit security onto legacy systems, but these efforts are having limited success and can be expensive. The SCADA community will need to find compensating security controls until secure systems are available and insecure legacy systems are replaced. The intrusion detection and security monitoring discussed in this paper is one possible compensating control.

INTRUSION DETECTION AND SECURITY MONITORING OF NETWORKS:

A strong information security program will include a variety of technical and administrative controls designed to prevent intrusions and unauthorized activities from both internal and external threat agents. However, even with a set of strong security products and security policies it is impossible to insure that a network is secure. For this reason, networks that are mission critical or contain sensitive information are deploying intrusion detection and cyber security monitoring systems.

Consider the physical analogy to this cyber situation. A critical building will have locks on the doors, safes, and other mechanisms to prevent unauthorized access. This same building will also deploy a set of physical monitoring systems, such as cameras and motion detectors, just in case the security is breached. The monitoring systems identify breaches and enable a quick response.

A variety of product and service solutions have been developed to create the cyber equivalent of cameras and motion detectors. These include:

- Network Intrusion Detection Sensor (NIDS) Products – A device that sits on the network and evaluates data traveling over the network. NIDS are typically connected to SPAN ports on switches so a single sensor can evaluate all or most of the traffic on a subnet. The data is compared to data related to a hacking exploit, called a signature. A NIDS may have over 1,000 signatures, and a new signature is typically developed for each new exploit.

- Host Intrusion Detection Sensor (HIDS) Products – Software that is loaded on a host computer system. A HIDS system identifies attacks using signatures or behavior analysis and attempts to prevent the attack. HIDS are generally an active defense that combines attack identification and response.

- Audit Log Analysis Products – Computer systems, applications, infrastructure equipment, and most other IT hardware and software has the capability of generating an audit log. Some of these entries will identify successful and failed intrusion attempts. There are a variety of systems available that will gather log information from various sources and present it in a useful format to a network administrator or security officer.

- Managed Security System Provider (MSSP) Services – Security incidents occur on a 24x7 basis. It requires a team of security experts working around the clock to monitor, evaluate, and quickly respond to information gathered from NIDS, HIDS, audit logs, and other sources. Many companies outsource these tasks to MSSPs. In addition to the manpower, MSSPs have developed sophisticated correlation and analysis engines to process the massive amount of data received on a daily basis. As an example, MSSP engines will reduce five million events a day to two hundred or fewer events that require human evaluation. A small number of product vendors are selling the correlation and analysis engines for large organizations that want to keep this function in house.

There are a number of commercial NIDS and HIDS vendors, and the open source NIDS and HIDS solutions are well respected and widely used. In general, the commercial vendors offer better support and are easier to use, while the open source solutions are more flexible and the software is available for free.

Special care needs to be taken when selecting an MSSP. The industry is in transition and a number of vendors have gone out of business or have been acquired. When selecting an MSSP consider the following:

- Formal, documented processes for analyzing and acting on an event
- Technical skill of the Secure Operations Center (SOC) staff
- MSSP portal and other tools to look at the events in real time
- Financial stability and focus on the MSSP business
- Vendor neutral or at least support for your systems

Vertical markets associated with high value information and networks are currently implementing these solutions. Financial service, pharmaceutical, e-commerce, and government organizations are some of the early adopters of these solutions.

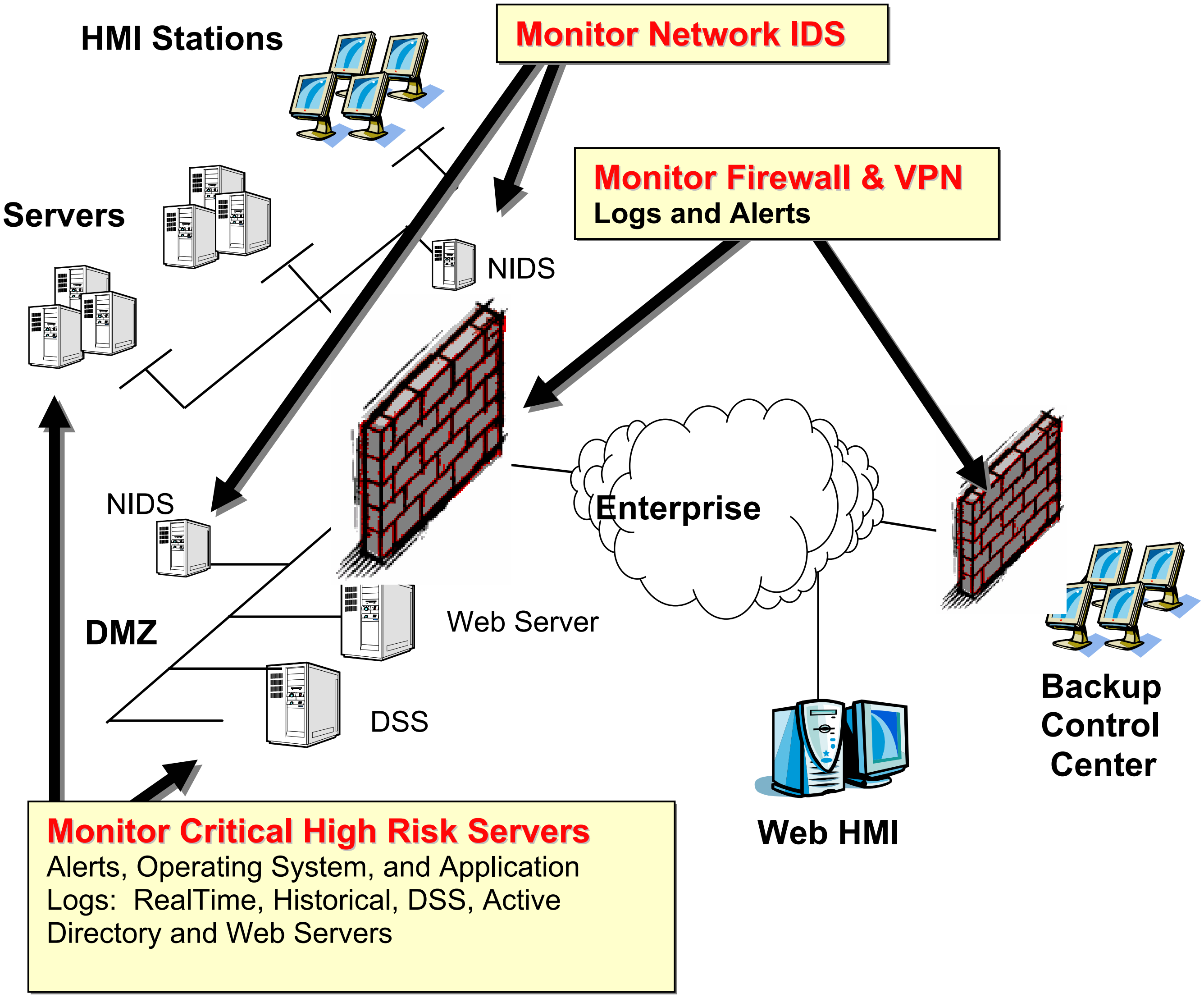
USE OF CURRENT SOLUTIONS IN SCADA NETWORKS:

In recent years, a number of SCADA systems have deployed intrusion detection and security monitoring products and services that were designed for a general purpose IT environment. An example of a very comprehensive deployment using currently available products and services is shown in Figure 1.

The NIDS are placed on the Control Center LAN, to identify attacks against the control servers and HMI, and on the demilitarized zone (DMZ), to identify attacks against decision support servers (DSS), Web servers, and other systems that can be accessed by users on the enterprise.

The firewalls provide perimeter security for the SCADA network, and their audit logs provide information on enterprise users attempting to access the SCADA system. Similarly, audit logs of routers, switches, and other infrastructure systems could be monitored.

Perhaps most importantly, the operating system audit logs of the control servers and other key systems are monitored for security events. Some organizations also monitor web server and database application logs.



Monitor Network IDS

Monitor Firewall & VPN
Logs and Alerts

Monitor Critical High Risk Servers
Alerts, Operating System, and Application Logs: RealTime, Historical, DSS, Active Directory and Web Servers

FIGURE 1 – Cyber Security Monitoring With Currently Available Systems

The monitored information from all of the above logs and the NIDS are sent to a MSSP or evaluated in house. Monitoring the network at various points allows the MSSP to better remove false positive indicators and to more accurately classify the severity of an attack. Below are a few examples to illustrate the benefits:

- Enterprise Attack Stopped At The Firewall – A firewall with a well designed ruleset will stop most attackers on the enterprise network from accessing the Control Center. By monitoring the firewall logs, a security officer will be able to identify attempts to penetrate the firewall and can deal with the disgruntled insider. This also is an early warning mechanism. Perhaps the first attempts fail, but a persistent attacker may eventually get through. By monitoring the logs, the security officer has the ability to limit the time window for an attacker.

- Enterprise Attack Stopped At The DMZ – An attacker on the enterprise network may attack a web server or DSS server on the DMZ. In the Figure 1 monitoring example, the attack would be seen in the firewall logs, the NIDS on the DMZ, and on the server log. Not only would the multiple data points confirm the attack, they could also indicate whether the attack was successful.

- Buffer Overflow Attack On Control Server – A variety of systems, such as HMI, PLCs, and other control servers, need to access control servers. An attacker can access a system or send spoofed buffer overflow messages to a control server. The NIDS will identify the attack, and the control server audit logs will often identify if the attack was successful or not. This also could be true for denial of service attacks and a variety of other attacks.

- Hacking Reconnaissance By A Disgruntled Insider – An attacker typically begins an attack by scanning the network and servers to identify vulnerabilities. The NIDS will identify these scanning attempts, and the attacker can be stopped before he is successful.

A best practice deployment of NIDS and audit log analysis that is performed 24x7 will help identify the intrusion attempts that are most commonly found on TCP/IP networks. Since most of the script kiddies and low to moderate skilled hackers do not develop exploits and lack knowledge of SCADA systems, these technical and administrative controls will stop the most common threat agents.

The HIDS were left off of Figure 1 and not included in this discussion because of the risks involved with adding software to a control server and automated response. The added software issue is the same as anti-virus software. Some of the HIDS software inserts itself in the TCP/IP stack and acts as an intermediary. There could be a number of performance and timing issues with this type of product. Vendors and users must certify the HIDS agent will not conflict with the SCADA application.

Automated response is a more contentious issue in the information security industry today. Both NIDS and HIDS have the ability to automatically reconfigure systems if an intrusion attempt is identified. This automated and fast reaction is designed to prevent exploits. The danger with an automated response is an attacker can potentially force an IDS system to shut down key parts of the network or server. In effect, the attacker can fool the IDS system into attacking itself.

The author's recommendation at this point in time is to use log analysis with 24x7 monitoring rather than HIDS or any other type of automated action. Certainly any use of an automated action should be carefully considered prior to implementation.

LIMITATIONS OF CURRENT SOLUTIONS

The primary limitation of the current intrusion detection and cyber security monitoring solutions is they have no knowledge or intelligence of SCADA applications and protocols. While attacks against a Microsoft IIS web server using the http protocol are addressed well, an attack on a SCADA control server using the Modbus protocol is not even considered. So the current systems are excellent against script kiddie hackers and other novices that use exploits easily available on the Internet; they are not adequate to detect attacks by a cyber terrorist, disgruntled insider, or skilled hacker with knowledge of SCADA systems.

SCADA application and protocol intelligence needs to be added to all of the products and services mentioned earlier in this paper.

FUTURE SOLUTIONS

MONITORING OF SCADA APPLICATION AUDIT LOGS

SCADA applications typically log a great deal of information. In fact, many of these logs are written to historian servers and maintained for a variety of important business purposes such as billing, maintenance, and regulatory compliance. The majority of the log entries are operational in nature and are based on sensor information or actuator actions. However, there is a subset of events in the SCADA audit logs that could help identify intrusions or other unauthorized actions. Some examples of useful security information in these SCADA logs are:

- Escalation of user privilege in the SCADA application
- Changing of a display (perhaps to fool an operator)
- Failed login attempts indicating a password cracking effort
- Disabling alarms to hide a physical attack (an example of a blended threat)

The transport of the SCADA logs to a MSSP or correlation engine is straightforward and available today. Control servers generally support syslog or other simple log transport protocols. This could be used to transfer the entire log. Ideally the SCADA application, or an agent program certified by the SCADA vendor, would identify and send only security related entries to save bandwidth and reduce the amount of data a MSSP would need to analyze.

The MSSP and correlation engines will need to be modified to understand the implications of the SCADA logs. Additionally the security staff in the SOC will need to understand SCADA networks and the log formats to gain the full value of this information. In summary, it will take cooperation between the vendors, users, and MSSPs to be successful. This has already occurred for the more mainstream applications such as databases and web servers.

SCADA SIGNATURE SET FOR NIDS

A second type of customization required for SCADA systems is the addition of specialized signatures for NIDS. These signatures will relate to SCADA protocols such as Modbus, PROFIBUS, OPC, and FF. As known vulnerabilities are uncovered for a SCADA application, corresponding signatures can also be developed. Note that it is naïve to expect that vulnerabilities will not be found in SCADA systems when they have been found in virtually every enterprise application. SCADA vendors could also be proactive in developing signatures that would identify the most common attacks on their particular systems.

The SCADA signature set could also be an effective compensating control for a major security problem: field communications. There is virtually no security for control center to field, RTU or PLC, communications. It is simple to fool a field device to take a dangerous command. Conversely, access to a TCP/IP based field device could be used by a cyber-terrorist to attack the SCADA control servers and take down the entire SCADA system. Since field devices have a typical lifetime of ten to twenty years, this problem will be around for a long time even if solutions embedded into SCADA systems were available today.

A SCADA signature set could identify unauthorized or unusual field communication. With the right user interface, a SCADA user could characterize expected field communications in terms of IP addresses, protocols, parameters, and frequency into NIDS signatures. The NIDS would then identify potential attacks via the SCADA field communications. With the right user interface it would be a simple matter to deploy these additional signatures. Since NIDS is a passive system, there would be no negative impact on the network or performance.

INTEGRATION AND SUMMARY

Today, SCADA users can deploy sophisticated intrusion detection and cyber monitoring products and services that will help identify attacks from the most common threat agents. This early identification will help stop the attacks before they are successful or at least limit the damage.

In the future, SCADA specific signature sets for NIDS systems and SCADA application log analysis can be added to the existing IT systems. Ideally, this information and corresponding SCADA knowledge will be integrated into the correlation engines and learned by the SOC staff to provide a true SCADA security monitoring solution.

REFERENCES:

[1]"Critical Infrastructure Protection: Challenges in Securing Control", GAO-04-140T, United States General Accounting Office (GAO), Washington D.C., October 1, 2003