Lathrop, S.D., Gates, C.L., Massie, D.D. and Hill J.M.D.

Risk Assessment of a Power Plant: Evaluating the Security of a Supervisory Control and Data Acquisition (SCADA) System

ABSTRACT

With the increased potential of a bona fide cyber terrorist attack and the possibility of a future "war in the wires", we must continue to sterilize the networks connected to critical infrastructures. This paper provides a risk assessment of an existing operational computer network used to control a boiler system generating power and heat for an installation. The methodology used in evaluating the security of the system is described along with specific recommendations for minimizing the risk associated with connecting the network to the Internet for the purposes of remote data collection and administration. Our assessment and proposed recommendations may be applied to any critical infrastructure with a requirement for remote administration and/or data collection.

INTRODUCTION

As an aftermath of the terrorist events that transpired on September 11th, 2001, the President of the United States created the Office of Homeland Security to analyze, plan and coordinate the interior defense of our country. One of the critical components of this new organization was the creation of the President's Critical Infrastructure Protection Board (CIPB) tasked "to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems" ("Executive Order on Critical Infrastructure Protection"). Within a year, the organization in conjunction with computer security experts from academia, industry, and government, produced a draft national strategy to secure cyberspace which outlines some of the critical steps required for the United States to secure its information systems from deliberate cyber attacks. The key sectors addressed in this document were the critical infrastructures such as banking and finance, transportation, and electrical power. This document was recently finalized and endorsed by the President of the United States (Clarke and Schmidt 2003).

The forensics analysis of al Qaeda computers seized from the caves of Afghanistan in the spring of 2002, suggest an extremely high level of interest from this terrorist group into how to remotely control, through the Internet, electrical substations, pipelines, dams, and communication grids (Gellman 2002). The devices used to control such systems remotely are called supervisory control and data acquisition, or SCADA, systems. They use their own application protocol but employ the standard Transmission Control Protocol/Internet Protocol (TCP/IP) protocol used by computers to communicate across the Internet and local intranets. The computer devices used to control critical systems and protocols they use to communicate are often not well understood except for the vendors who develop them. Because they are not as common as the familiar Internet application protocols they are not subject to the constant scrutiny of the Information Assurance community. However, the threat against such systems is real. One utility reported 100,000 scans a month in 2001 (Dagle, Widergren et al. 2002).

The problem with such a situation is that assuming information systems are secured because the nodes on the network and the protocols used to communicate are obscure, is a fatal mistake. Obscurity only slows the development of attacks on the system. Given enough time and money to replicate the devices used in the system, a motivated cyber agent or cyber warrior will develop tools to attack the system. The proliferation of such tools to the computer underground is then trivial (Welch 2002).

In this paper we describe a risk assessment of a power plant's information system. The power plant is real and operational with a network of control devices and computers controlling the plant's

central boilers. The plant is capable of producing over 5MW of electricity as well as central heating. Ultimately, the goal of the project is to reduce the cost of operating the plant by remotely administering the system and enabling a software application to dynamically control the mechanical equipment. The software makes decisions based on several attributes such as electrical and fuel tariffs, ambient air temperature and the number of personnel on site. The purpose of the assessment is to identify specific threats and vulnerabilities of the system and then take the necessary steps to minimize the risk associated with connecting the network to the Internet. In order to fully evaluate the network, we conducted a penetration test using open source software tools that both cyber attackers (i.e. computer hackers) and computer security professionals use to evaluate network security. We emphasize open source tools because these tools are freely available for download on the World Wide Web (WWW) and, thus, could be obtained by anyone. An organization with more resources could purchase more advanced tools or modify the open source software tools to fit their needs.

FACILITIES AND MOTIVATION

The central plant was originally built in 1903 as a heating facility. However, upgrades over time have changed it into a cogeneration facility that is capable of providing up to 5.2 MW of emergency power. The plant consists of two 1.25 MW steam turbines and one 1.65 MW steam turbine. High pressure (1.2 MPa) and low pressure (184 kPa) steam lines, acting as the condenser for the plant, provide heat to buildings. Due to steam pipe losses and process loads, only 40% of the steam condensate returns to the central plant. Make-up feed water, from a local reservoir, is mixed with the condensation that returns from the heating load. Once mixed, the water is pumped to any combination of the three boilers in the system. In 1993, a 1.2 MW diesel generator, intended for peak shaving (demand reduction), was added to the plant.

The organization purchases grid electrical power under a fixed price of demand [kW] plus energy charges [kWh], which varies by time of year. Since electricity can usually be purchased for less cost than producing it on site, local power generation is only economical for peak shaving or when cogeneration is possible. Since the only condensing capability is from the heating and processing loads, the steam turbines can only be economically run during winter months. The diesel generator may be operated at any time of year, however waste heat recovery is not possible with the current configuration.

The plant had traditionally been controlled by operators who set its operation based upon their experience. Unfortunately, they often did not operate the plant optimally because they lacked access to certain information. Such information included site population, hourly weather predictions, and electrical price signals. In some cases, the plant operators were not trained in all the subtleties of plant operation. This sub optimal performance can be improved with a clear methodology of how plant equipment operates and interacts.

An artificial intelligence, agent-based software application is being developed that takes input from equipment sensors, building thermal loads and electrical profile coupled with rates from a remote location, and determines the combination of equipment that would afford the least cost option for providing power and heat. This information is used to produce accurate models, which increase the ability to operate the plant efficiently. While this information could be collected manually, operator error would be minimized if the program were fully automated.

The SCADA system uses component off the shelf (COTS) technology. The operating systems and the applications they run, along with the communication protocols used to exchange information between devices, are subject to the same sort of attacks that are used everyday on the Internet. The weakest link, the human element, is subject to attack through social engineering, weak or no passwords, poor policy, and improper configurations.

The security of the system and assurance of its information is paramount. In order to provide the functionality desired, the system must be connected to the Internet. To prevent cyber attacks against the plant requires a risk assessment of the current infrastructure and hardening of the final implementation.

RELATED WORK

Published work in this area is very sparse. This may be because results of such assessments are not releasable to the public or, worse, tests such as described in this paper are not being

conducted. Government and private agencies are continuing to investigate protection and security of critical infrastructure. Their recommendations consists of making industry aware of the threat and potential vulnerabilities associated with their SCADA systems, provide assistance in the form of a training and penetration tests similar to the one described in this paper, and establish partnerships between the National laboratories and industry in order to leverage each organization's expertise. Similar to this paper, their presentation describes the typical vulnerabilities observed in SCADA systems (Dagle, Widergren et al. 2002). The difference between this paper and their presentation is that we present a more thorough risk assessment including results from a vulnerability assessment.

RISK ASSESSMENT

We use the Information Assurance (IA) model (Figure 1) presented by Maconachy as a framework for assessing an information system. The model describes four dimensions: (1) information states, (2) information services, (3) information security measures and countermeasures, and (4) time (Maconachy, Schou et al. 2001).

The power plant uses information that can be in any one of three states at any given point in time: (1) processing, (2) transmission, or (3) storage. When assessing the security of that information, one must consider all three states. The types of security services a system can provide include confidentiality, integrity, availability, authentication, and non-repudiation. We focused our evaluation on the first three services. When considering where one may accept risk, confidentiality may be the least important attribute as the power plant still operates even if an outsider is able to view the information. On the contrary, the integrity of the data is very significant. Any modification of the data may cause damage or loss. For example, a data packet with incorrect values may be sent to a boiler computer that in turn directs the combustion subsystem to over compensate the air to fuel ratio. Or, incorrect information could be feed to the software application, leading to incorrect predictions. In every case availability is important as the loss of data to the system degrades, or possibly, disables power and heat generation. Availability and integrity over time is a particularly important factor for control systems as updates to the controllers happen in real-time. Any disruption to the flow of information can result in the system becoming desynchronized.

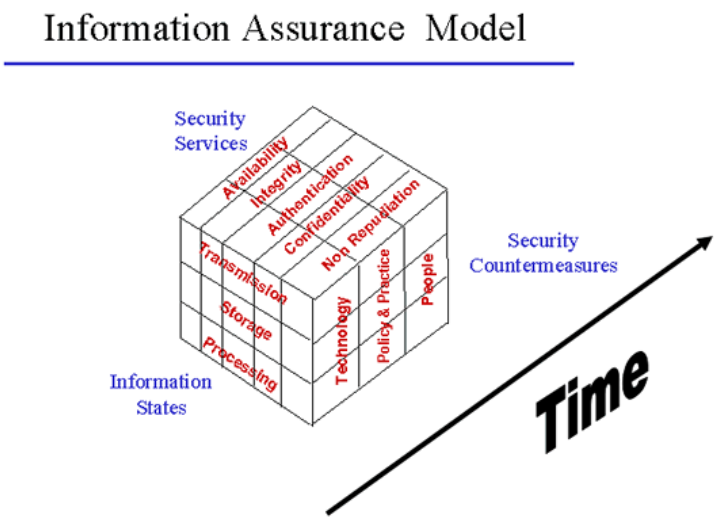

Figure 1: Information Assurance Model

As with any risk assessment process, the ultimate goal is to reduce risk to an acceptable level without giving up the functionality and performance required by the organization. In the context of the Information Assurance model, risk is the probability that a particular threat is manifested against a specific vulnerability in the system that undermines availability, integrity, or confidentiality. One cannot eliminate risk in the information system without physically disconnecting the computers from the network

and burying them in a hole. Obviously such a solution defeats the purpose of deploying and using the technology in the first place.

The model's security countermeasures enable one to reduce risk. These countermeasures include technology; policy, procedures, and practices; and the people within the organization administrating and using the system. Most people will immediately associate security counter measures with computer security applications such as firewalls, anti-virus software, and patches. In most cases, however, the people, policy, and procedures play the most important role in determining the overall security of an information system. Throughout the remainder of the paper we will use the IA model as a roadmap for our discussion. First we will look at the threat and potential attacks against the three security services we studied (confidentiality, integrity, and availability). Then we will look at the vulnerabilities we found as it relates to each of the information states and provide recommendations in terms of the security countermeasures.

The Threat

Based on our penetration test and an analysis of the protocols and platforms used in the power plant, we conclude that there are three major forms of attack against the power plant's infrastructure, each with an increasing degree of severity.

Integrity attack on the information. This type of attack involves modifying the information stored in databases and transmitted across the communication networks. Such an attack's visible end state is an unknown decrease in the efficiency of the power plant's generation of power or heat resulting in a higher cost to operate the plant. Such a scenario involves an attacker modifying the current cost of electrical power, number of personnel, ambient air temperature or data returned from the boiler's sensors that is either stored in the databases or in transit. Modification to the data causes the software relying on the information to incorrectly adjust boilers and either over or under produce steam resulting in an inefficient process, lack of confidence in the design capacity during critical loads, and any competitive edge that the control software was supposed to provide. This is exactly the opposite result desired by the designers of the agent-based control software.

Availability attack on power generation. The second attack is an availability attack (also known as a denial of service attack). The attack causes degradation in the facility's ability to generate power. There are two possible ways an attacker could perform a denial of service attack against the power plant and effectively prevent it from producing power or heat. The first is a very overt, noisy attack where the attacker sends several thousand packets, or "pings of death" in hacker terminology, to control computers running on the power plant's internal network. The victim computer(s) become overwhelmed with packets and are unable to perform their primary function as they are busy attending to the large number of incoming packets. Another possibility for such an overt attack is for the attacker to execute an exploit that effectively shuts down a device on the network responsible for maintaining network connectivity. A network router is an example of such a device, and an exploit in this context is a computer program takes advantage of a particular vulnerability in software. Once the router can no longer perform its connectivity function, communication ceases between computer nodes on the network and information cannot be transferred to the boilers' controllers. This action results in degradation to default operations.

The second and more dangerous method an attacker could use to temporarily disable the power plant is much more covert and relies on the attacker initially gaining access to computer systems within the plant's internal network. Based on our analysis, an attacker could gain access to one or more computers on the network using operating system based attacks, application-based attacks, or social engineering. If access is gained using a normal user account, escalation of privileges may be obtained by attempting "user to administrator" exploits (Skoudis 2002). One would believe that such vulnerable applications and operating systems are not running on SCADA systems used to control boilers, but our assessment shows the contrary.

Once access is gained on a computer within a central plant, the intruder can then launch network-based attacks. Again, the attacker could launch a noisy denial of service attack from within the internal LAN as they are now within the confines of the local network and outside the reach of external security. However, if they wish to remain overt, a serious cyber warrior could take advantage of the weak, unencrypted protocols used in control systems and either create their own packets to

communicate to the boiler controllers or modify the integrity of the packets already in transit. By simply "zeroing" out the data in a controller's registers, the attacker could effectively shut down the power generation capability of the plant.

Confidentiality and integrity attack against the boiler controllers. The final and most devastating attack that a true cyber-terrorist may attempt to exploit would result in physical damage to the plant, and potentially, loss of human life. It is a combined exploit on the confidentiality and integrity of the information that controls the boilers resulting in an explosion and possible physical damage. More research into this final attack is required, but theoretically, it is very possible. We describe it in order to be complete in our analysis, to highlight our concerns with the unencrypted network protocols used in SCADA systems, and to show the relatively ease of such an attack.

Before describing the attack, it is important to understand the primary purpose of a boiler control system. A boiler's controller maintains steam availability and improves efficiency in an effort to reduce cost and emissions. One of the key subsystems of a boiler control system is the combustion subsystem. Its function is to deliver the right mix of air and fuel to the burner at a rate that satisfies the firing rate demand and at a mixture (air/fuel ratio) that provides safe and efficient combustion.

An explosion might occur if you could cause the controller to over compensate the air to fuel mixture. Forcing the controller to over compensate is a matter of writing certain data to the appropriate memory location(s) that triggers such an event. In our analysis, it is not obvious with a terse inspection of the controller's documentation which memory location controls the combustion subsystem, but a diligent cyber warrior backed with state-sponsored or terrorist organizational resource would purchase the equipment and evaluate its operational functionality. It is then trivial to inject a packet or modify a packet in transit to enable such a memory write.

Vulnerabilities and Recommendations

In order to evaluate the vulnerability of the power plant's current information technology infrastructure and provide sound recommendations, we took the approach from an attacker's vantage point and used several active reconnaissance based, *port scanning* tools that an attacker would use to determine the network topology, operating systems, and open TCP ports running on each machine. We also employed several *vulnerability scanners* that attempt to determine the specific vulnerabilities associated with the computers and their software. Passive reconnaissance measures were also employed by searching for publicly available information on the World Wide Web that may be of interest to an attacker.

We also used specific exploitation tools that an attacker would use to further penetrate the network once access was gained through the vulnerability. These exploitation tools included *network monitoring tools* used to monitor network traffic, *password crackers,* to determine the strength of passwords on the system, and various other attack tools designed against specific operating systems and applications to identify security weaknesses.

Because not all tools provide the same information we employed a breadth of tools in conducting our analysis. It is also important to note that despite the fact that we were physically on site for our evaluation, if the current topology was connected directly into a switch or router with access to the Internet, we would have been able to collect similar information. Access to the physical wires is not necessary as the Internet supports protocols that allow transmission between two interconnected devices. We used all open source tools to evaluate the system. These tools are freely available on the Internet. We hypothesize that a true cyber warrior would develop their own in-house tools and purchase the systems described in the paper in order to increase their capability and specifically target the critical infrastructure for which they were attempting to gain access.

Although we did not attempt any social engineering attacks on the personnel running the plant, it appeared that the plant operators would have been very "helpful" in providing useful information such as passwords, types of software running on the system, and other useful information over the phone or even in person if we appeared to be the local "IT" guys. During our visit, when we were connecting our computers into the plant's network we were never questioned or asked what we were doing even though we had no name tags, escorts, etc. There appeared to be only one person in the plant even familiar with the computer systems and that person did not physically work full-time at the plant's location.

We now provide our assessment and specific recommendations for the power plant's information infrastructure by categorizing them using the IA model's security countermeasures (technology, policy, and people) as described by Figure 1. We focus primarily on technology but also briefly address the issues surrounding policy and people.

1) **Technology Recommendations.** When speaking of technology, we are including the hardware, software (both operating system and application), and communication networks. Each has specific vulnerabilities. The discovered network topology from our reconnaissance is shown in Figure 2 depicts the computer name, operating systems guessed by the port scanning tools, open ports discovered, and vulnerabilities found. Note that due to the number of vulnerabilities found, we are highlighting only the critical weaknesses.

Table *2* depicts the purpose of each open port found. It is important to note that this information was gathered by our tools and is not a result of physically going to each machine or reprinting an operation manual.

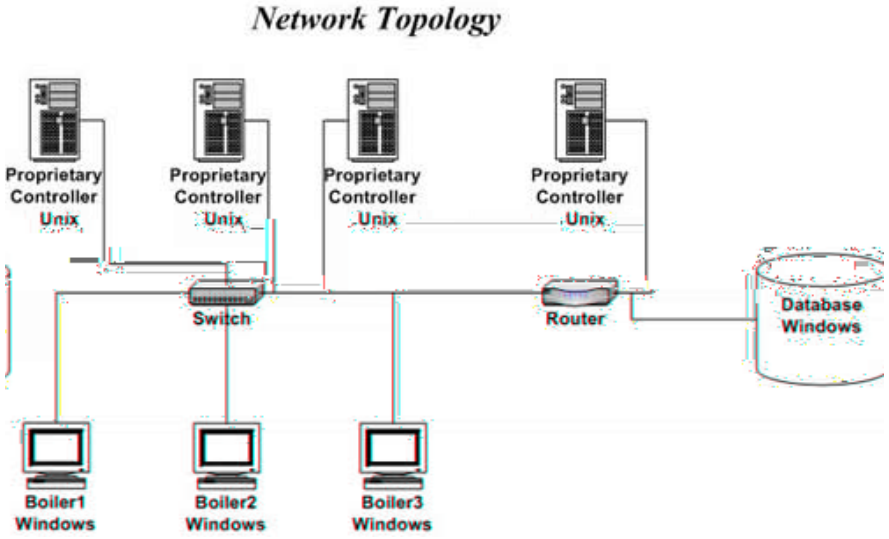

Figure 2: Power Plant Network Topology

There are eight computers connected to the network, each having a static IP address. Four of the computers were running a vendor-specific Unix operating system. The other four computers were running the Windows operating system. Additionally, there are two appliances (a router and a switch) found on the network. The Windows operating systems are familiar to the common hacker and numerous exploits are known to exist against such systems. The proprietary controllers, on the other hand are not common on commercial or government network. The networking protocols identified running on the network included TCP, UDP, IP, HTTP, MODBUS, TFTP, and the Windows specific NETBIOS protocols.

Highlighted vulnerabilities from include the router. It is running a web server that is susceptible to a denial of service attack if the attacker attempts to access a particular script. Such an exploit would enable the attacker to carryout an availability attack on power generation as described previously. The computers running Windows operating system are extremely vulnerable to numerous attacks. In particular, the use of the Network Basic Input/Output System (NETBIOS) has several vulnerabilities. NETBIOS provides the ability to share files or folders across a network through Windows network shares. Although extremely useful, improper configuration of network shares may expose critical system files, or may provide a mechanism for a nefarious user or program to take full control of the computer.

Table 1: Discovered Computer Nodes with Vulnerabilities

COMPUTER NAME	OS	PURPOSE	TCP/ UDP PORTS	VULNERABILITIES IDENTIFIED
Router	Proprietary	Enables routing of network traffic	TCP-80, 520 UDP–53,67, 69,520	Crashes if a remote attacker accesses a script on it
Boiler1 – Boiler3	Windows	Displays boiler information and provides an interface for controlling boiler settings.	TCP-135,139 UDP-135,137, 139	It was possible to log into the remote host using a NULL session. Several local accounts have never changed their password and have passwords that never expire; Most accounts are unused. One account had no password.
Boiler Data Aquis	Windows	Database collecting boiler sensor information	TCP-135,139 UDP-135,137, 139	Same as Boiler1- Boiler3
Proprietary controllers	Unix	Collects and stores boiler sensor information and controls boilers.	TCP-80, 502	Web server is vulnerable to a cross site scripting attack. ModBus protocol subject to session hijacking, man-in-the-middle attacks, and replay attacks

Table 2: Discovered Open Ports

PORTS	TRANSMISSION PROTOCOL	PURPOSE
80	TCP	Web Traffic
135, 137, 139	TCP/UDP	NETBIOS (Network Basic Input/Output) protocol.
502	TCP	ModBus
53	UDP	Domain Name Server
67	UDP	Bootstrap Protocol
69	UDP	Trivial File Transfer Protocol
520	UDP	Router

For example, a specific vulnerability associated with NETBIOS is the “Null session connection”. It is a mechanism that allows an anonymous user to retrieve information (such as user names/passwords and file shares) over the network, or to connect without authentication. It is used primarily by Windows to account for various critical system operations. When one computer needs to retrieve system data from another, the account opens a null session to the other computer to perform the desired tasks. Unfortunately, attackers can also log in as the Null Session. Therefore, if working in a Windows domain environment, you can minimize the information that attackers obtain, but you cannot stop all leakage.

Other significant problems found with the computers running Windows primarily revolved around user accounts. One account had no password making it trivial for an attacker to gain access to this machine as that user. Once an attacker has access as the user they can masquerade as that user anywhere on the network where that user has permissions. Worse, an attacker can attempt a “user to administrator” exploit on the system in order to gain Administrator access. Other accounts had passwords that had never been changed and were breakable. Finally, there were a few unused accounts on the system. These accounts should, at a minimum, be disabled or deleted if possible.

Leaving unused accounts on the system leaves another avenue of approach open for the attacker to gain access.

Finally, the computers running Windows stored passwords in both the legacy LAN Manager (LM) format and the newer, more secure NTLM scheme. In order to support backwards compatibility with older Windows systems, the LM format is the default method of storing passwords. However, it has been shown that password cracking programs can easily break the encryption of passwords stored using the LM format because of the poor implementation of the encryption algorithm.

All of the vulnerabilities found on the computers running the Windows operating system would subject the power plant's information system to the first two attacks described previously. A malicious attacker could either cause plant inefficiencies or temporarily disable power generation by gaining access to either the computer running the database or the computers used for displaying information (i.e. Boiler1-Boiler3) and modify the data so that either the operators take imprudent actions or by sending incorrect data to the controllers.

The proprietary plant control system is a set of control system computers for the plant and combines the functionality of a loop controller, a process logic controller (PLC), and a distributed control system (DCS). The system serves as the storage location for the boilers' sensors and control information. The system has an auto-configured human-machine interface (HMI) and monitoring software located on the Boiler1- Boiler3 computers. The power plant's data acquisition computer uses a software package that contains a database with the current configuration of the boilers. The controllers can be configured remotely from this computer using software. Configurations and control information are transferred over the network from the database to the monitoring software using the ModBus protocol. Finally, the proprietary controllers run a web server to send graphical control measures to web browsers on the workstations.

The proprietary controller user's manual describes the methodology for connecting the system to an Ethernet network and also states that "security is of paramount importance" but does not give any specifics besides mentioning that a firewall should be employed to protect the internal network from the Internet. It does not contain configuration options or details such as firewall recommendation, configuration considerations, and other security precautions that would minimize risk. We could find no mention of a risk analysis in any of the documentation.

We found serious vulnerabilities associated with the proprietary control system and the ModBus protocol it uses to transfer data across the communication network. Each controller has a web server running on it that allows the plant operator to log into it and adjust settings via a standard web browser. These web servers are susceptible to a specific attack (cross site scripting). A cross-site scripting attack is possible when a web server (in this case one of the proprietary controllers) returns content that includes un-sanitized user-provided data (such as username and password). An attacker could create a request to the web server (in the form of a standard URL) with malicious data embedded (such as with JavaScript or VBScript) that redirects certain information (i.e. username and password, session state, etc) to the attacker's computer. The URL is then presented to the user (in our case a plant operator) in the form of a hyperlink. The attacker entices the user with the hyperlink via an email message, an instant message, or a web message board posting (i.e. "I need you to check on the controller's status" "Click here"). If the plant operator follows the link it directs them to the controller's login page. When the plant operator attempts to login the credentials are sent back to the attacker. The plant operator never notices the event, sees only the standard web page after normally logging in, and continues business as usual. The attacker meanwhile has the plant operator's credentials and can log into the boiler controller as if they were the plant operator. This attack may intercept user input, read data from the controller and send it back to the attacker's computer, or, allow code to be run on the target system possibly giving the attacker *root* or *administrator* access (Howard and LeBlanc 2002). Once an individual gains this level of access on a platform they can perform any operation that would be possible by an administrator of that machine. Such operations include reading or writing data to the controller's memory. This vulnerability would allow the attacker to execute any of the three attacks previously described.

The proprietary controllers use a messaging protocol called ModBus to exchange information. ModBus is an application protocol that was initially designed as serial line, master/slave architecture between control devices. It has recently evolved to use a modern Ethernet-based network using the TCP/IP protocol as the underlying transport/network protocols (Figure 3). The ModBus application server listens by default on port 502. (Dube and Camerini 2002; "MODBUS.ORG Home Page" 2003)

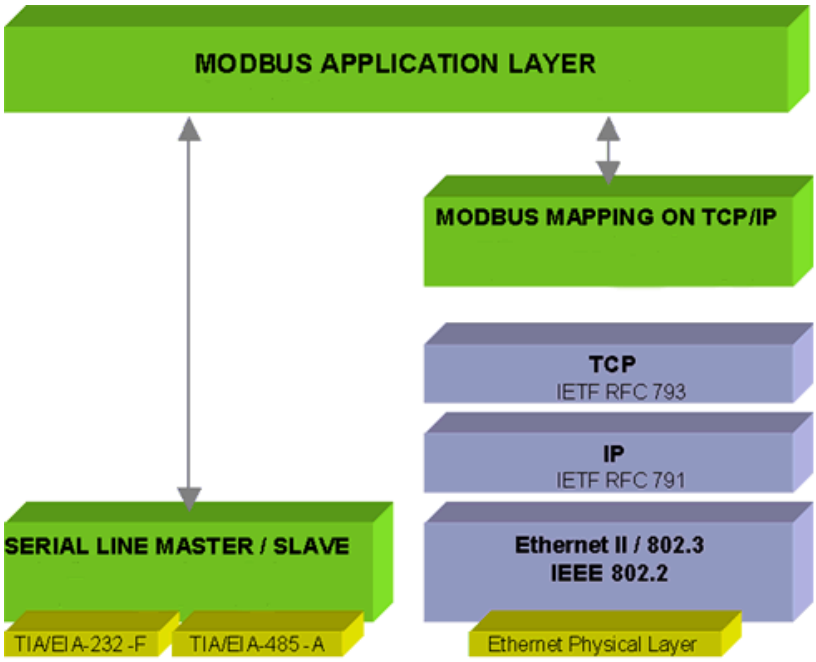

Figure 3: MODBUS Architecture

The ModBus protocol provides communication between computers using function codes that provide both read and write services. A client device (either a workstation or another device) requests a read or write from/to a specific memory location on a controller, and the service replies with either the specific data requested and/or writes the data to its specified memory location which ultimately controls the air/fuel mixture and boiler sensors. Encryption is not used so all transactions are transmitted in the clear and can easily be captured and modified with network monitoring tools. An example packet was sent from a controller to the data acquisition computer. All reads and writes to registers on the controller could be observed, and if we had desired, the data could have been modified. The request for comments (RFC) describing the MODBUS protocol specifically states that it "does not discuss security issues and is not believed to raise any security issues not already endemic to MODBUS communications. Since MODBUS/TCP is based on TCP/IP, it is not inherently secure." The vulnerabilities described that are associated with the proprietary controllers and the ModBus protocol would allow a cyber warrior to execute any of the three attacks described previously.

There are several technological solutions that one could employ to reduce risk in the system and significantly increase the probability of detecting attacks and being able to respond appropriately. This technology includes such tools as intrusion, detection systems, firewalls, honeynets, integrity maintenance systems, etc. However, overwhelming the people who maintain these systems with new technology are not always the correct answer especially when their ultimate responsibility is to operate a plant. Because of this thought process and our assumption that the power plant's network is part of a much larger network that provides a defense in depth and whose security is constantly monitored by computer security specialists, our recommendations merely provide what we believe to be the *minimum* technical solutions required to reduce the risk of an attack to an acceptable level.

First, a firewall that segments the internal network from the agent-based system and the external network must be installed and configured. It should be configured to block all traffic except for the port required by the agent-based software to perform its analysis. No traffic originating from outside of the network should be allowed into the internal network. This "deny all" policy will prevent attacks against the NETBIOS, http, and MODBUS protocols from a remote attack assuming that the protocol used by the agent-based protocol is secure and the firewall is configured correctly.

All services/ports that are not required must be closed. This prevents all exploits against those services. A good example of this is the NETBIOS service. Since there is no requirement to run Windows "domains" or to allow file shares in this architecture, disabling NETBIOS will preclude the exploits against this protocol. The router's port 80 (web) can be disabled and configured from a HyperTerminal setup instead to preclude a denial of service attack.

There are a few security countermeasures that the designers of the agent-based system will want to include in their final implementation. Integrity maintenance software should be installed on all systems in order to detect any attempts to modify files. In order to secure the transmissions between the agent-based system and the database, a protocol such as secure sockets layer (SSL) or IPSEC should be used with the data that is stored in the database encrypted using a strong encryption algorithm.

The final two recommendations are strongly tied into the policy and training of the people who use the system. The first recommendation is that software patches to operating systems and applications must remain current. Software patching will preclude known vulnerabilities although it is ineffective against unpublished vulnerabilities. Furthermore, system administrators must properly configure the operating and application systems and insure that the policies are set for the best security posture. For example, disabling the Windows LANMANAGER authentication mechanism will insure that only the more secure and stronger encryption implementation found in NTLM is used. Several security checklists exist for system administrators to insure their systems are locked down as much as possible.

Users of the systems must have strong passwords and these passwords must be checked with password cracking software. Most forms of authentication, as well as file and data protection, rely on user-supplied passwords. Every account that is required must have strong passwords and administrator accounts should be especially protected. Any application that is installed for the first time must have the password immediately changed as the hacker ungrounded has a database of default passwords for a myriad of applications.

Finally, as is often quoted in some sports, the best defense is a good offense. Vulnerability assessments from an external source should be performed on a regular basis in order to insure maintenance of the system is taking place and that patches to thwart new vulnerabilities found are current.

Policy Recommendations. Again referring to Figure 1, we see policy and people identified as security countermeasures. In general, policy must be established and enforced in order to minimize the risk of connecting the power plant's internal network to the Internet. Clearly defined roles and responsibilities to defend cyberspace are important for managers, system administrators and users. The network architecture must be documented and critical systems such as proprietary controllers and databases must be identified and the additional security measures to protect these systems should be documented. A rigorous, ongoing risk management process must be established and enforced.

Policy should include procedures for both users and administrators. Some examples include how often passwords are changed, where log files are stored (on the host machine or off-site), how often logs are reviewed, when systems are backed up, and procedures for recovery. Passwords should be changed periodically (i.e. every 3-6 months) in order to prevent an attacker who has acquired the password accounts through other attacks, time to crack those passwords. Given enough time a majority of passwords can be cracked unless they are very strong. Forcing users to change passwords frequently results in bad passwords or re-used passwords. Administrators should have an alternate account for normal logging into the systems, and should use their administrator's account judiciously. A formal procedure should be in place for conducting a vulnerability assessment similar to the one outlined in this paper. Additionally, the policy should address how often training should occur for both users and administrators.

People Recommendations. Looking closely at security measures and counter measures, it is apparent that policy, technology, and people together have a synergistic effect on the security of an information system. Of these three elements, people are the most important. We believe that one of the main problems in the security of a SCADA network is that the people running the system, although well versed in the mechanical and electrical components of the system, often have little or no knowledge in how to secure the information technology. Most of the recommendations involve keeping up with the latest software patches. This involves training the system administrators to remain current

with the latest vulnerabilities, running their own vulnerability assessment tools, and applying the latest patches. Note that such a methodology will not stop unknown attacks that a full-fledged cyber-warrior may launch, but these measures will preclude easy attacks.

More education and training is required. People must build, install, configure, and maintain the technical aspects of information systems. If technology is implemented improperly or is used without the correct policies and procedures to support it, these technologies can actually *reduce* the overall security of an information system. Finally, it is people who must hire, retain, and sometimes fire other people who use and maintain these information systems. Without education and training in such matters information security measures are nearly worthless.

FUTURE WORK

Based on our findings a more in depth security of the MODBUS protocol and the proprietary system are required. Clearly, the MODBUS protocol is vulnerable to attack and anyone could easily inject or modify data. The application should be encrypted using a strong encryption algorithm and a mutual authentication scheme should be put in place. In order to clearly identify the capabilities of the proprietary control system and what aspects of the boiler system it can control, more analysis is required. The purpose of each memory location requires investigation in order to determine what physical aspect of the boiler control system can be influenced. It is clear to us that by modifying or injecting packets destined for a controller can temporarily disable a system. What is not clear is the physical damage that may be caused with such an attack. From a vendor's standpoint, more work is required to determine what steps an administrator of a proprietary system should take in order to properly secure their system. The manual should include these steps. After the implementation of the agent-based system and our recommendations, a re-evaluation of security should take place.

CONCLUSION

In this study we conducted a risk assessment of a real power plant's supervisory control and data acquisition systems (SCADA). The methodology described and proposed recommendations may be applied to any critical infrastructure with a requirement for remote administration and/or data collection. There are several vulnerabilities associated with the current network that a motivated cyber attacker could, at a minimum cause inefficiencies in the system or disable it, and in the worse case, cause physical damage. Our recommendations include technical, policy, and training recommendations. Additionally, we conducted a cursory examination of the MODBUS protocol and determined that, because data transmission is unencrypted, it is vulnerable to passive and active eavesdropping, session hijacking, man in the middle, and replay attacks. Work needs to continue on improving the security of this protocol.

Assuring information is not an all or nothing endeavor. One must balance the desired functionality and performance required in an information system along with security. There is no "secure" or "non-secure" technical solution. Security includes the entire environment to include technology, the policies, and the people—and it is not free. One must determine what level of risk is acceptable and then make every effort to minimize that risk with appropriate security solutions. We would argue that in a critical infrastructure, such as a power plant, where the cost of physical damage is immeasurable monetarily, one must make every effort to secure their information system from a cyber attack.

Acknowledgement

The primary author would like to acknowledge COL (Dr.) Daniel Ragsdale for sparking his interest in information assurance and critical infrastructure protection.

REFERENCES

Clarke, R. A. and H. A. Schmidt (2003). The National Strategy To Secure CyberSpace. Washington D.C., The President's Critical Infrastructure Protection Board**:** 65.

Dagle, J., S. Widergren, et al. (2002). Enhancing the Security of Supervisory Control and Data Acquisition (SCADA) Systems: The Lifeblood of Modern Energy Infrastructures. IEEE Power Engineering Society Winter Meeting, New York City, NY, IEEE.

Dube, D. and J. Camerini. (2002). "MODBUS Application Protocol: Internet Draft." Retrieved February 7, 2003, from http://www.ietf.org/internet-drafts/draft-dube-modbus-applproto-00.txt.

"Executive Order on Critical Infrastructure Protection." Retrieved January 29, 2003, from http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html.

Gellman, B. (2002). Cyber-Attacks by Al Qaeda Feared. Washington Post. Washington D.C.**:** 4.

Howard, M. and D. LeBlanc (2002). Writing Secure Code. Redmond, WA, Microsoft Press.

Maconachy, W. V., C. D. Schou, et al. (2001). A Model for Information Assurance: An Integrated Approach. 2001 IEEE Information Assurance Workshop, West Point, NY.

"MODBUS.ORG Home Page."(2003). Retrieved February 15, 2003, from http://www.modbus.org/default.htm.

Skoudis, E. (2002). Counter Hack. Upper Saddle River, NJ, Prentice Hall PTR.

Welch, D. (2002). Adversary Threat Taxonomy. IEEE Information Assurance Workshop, West Point, NY, IEEE.