Click here to view PowerPoint presentation; Press Esc to exit

Network Vulnerability Assessment: A Multi-Layer Approach to Adaptivity

Professor Ann Miller and Professor Kelvin T. Erickson
Department of Electrical and Computer Engineering
University of Missouri – Rolla
Rolla, Missouri 65409-0040
USA

milleran@umr.edu kte@umr.edu

ABSTRACT

Adaptivity requires at least frequent, and ideally real-time, updates and also requires the ability to analyze, respond and reconfigure. Such network management flexibility requires several types of information and capabilities, which include response of the network to node failure, reachability of nodes, and boundary control. The first issue determines how the network will respond to a "problem", which might be caused by an internal defect of the node or by a failure caused by external faults through the environment, accidental user error, or malicious input. In this event, network analysis on reachability can provide input for routing around the disabled node in order to maintain connectivity for as much of the network as possible. Furthermore, up-front reachability analysis also helps to identify potential access which is unwanted and thus aids in intrusion avoidance. The problem is exacerbated when multiple nodes fail, e.g., distributed denial of service. In this case, boundary control is important in order to isolate affected subnets, to keep these nodes from affecting additional nodes, and to provide limited services until the full system can be restored.

This paper presents a multi-layer analysis of a small (30 node) factory automation laboratory, used in Supervisory Control and Data Acquisition (SCADA) applications. Our approach views the network and applications as a system of systems. Network vulnerability is assessed at several layers; results and recommendations are discussed. Finally, considerations for extension and scalability are presented.

1.0 INTRODUCTION

NATO and its member Nations are engaged in Transformation; a significant portion of this involves the shift from platform-centric operations to network-centric or network-enabled operations. In civilian systems as well as in the military arena, computer-based systems are increasingly linked with other systems to form large-scale systems of systems. These networked systems provide opportunities for increased robustness, for example, load balancing and load sharing in electric utilities. These networked systems also pose the risk of cascading failures, with blackouts across utility boundaries as a classic example.

For the military, network-centric warfare includes the capability of sensor-to-shooter operations. In civilian applications as well, for example, factory automation, networks of sensors are connected to larger networks, typically through some form of gateway or access point. There is a wide spectrum in capability and type of sensors. Many provide Supervisory, Control, and Data Acquisition (SCADA) capability. As we move to large-scale systems of networked sensors, there is the need to understand the robustness and the vulnerability of these networks when interconnected with C2 and other critical systems.

Paper presented at the RTO IST Symposium on "Adaptive Defence in Unclassified Networks",
held in Toulouse, France, 19 - 20 April 2004, and published in RTO-MP-IST-041.

Communication connections, especially network connections, are the main security threat to a factory automation system. At the very least, one must connect to a controller in order to program it, usually through serial interface. Most security threats are through a peer-to-peer network where the controllers, personal computers, and communication gateways are connected. The security threats to a factory automation system can be categorized as (1) inside the system by unauthorized users; or (2) outside the system by unauthorized or malicious users. Both types of threats are considered in this paper. All factory automation systems are vulnerable to inside threats. An inside threat is often from an inexperienced employee that tries to access a controller for which s/he is not authorized. Less often, a disgruntled employee can also be a security threat.

This paper first explains the approach and study test bed. Next, the vulnerabilities at the application layer and command packet layer are assessed. Finally, recommendations for further study are presented.

2.0 APPROACH AND STUDY TESTBED

Given the importance of understanding the impact of netted sensors within network-centric operations, the approach in this study was to understand a small network of sensors within a larger application and to assess the vulnerability of the entire system through multiple layers of application, network, and device. While the particular application is that of factory automation, the network topologies examined are similar to those in many other environments, including military communications. And while the application software is specific to SCADA network, it exemplifies the myriad problems encountered with Commercial Off-the-Shelf (COTS) products, particularly those which run in a Microsoft Windows environment controlling sensors consisting of Programmable Logic Controllers (PLCs).

The testbed for this analysis is the Factory Automation Laboratory within the Electrical and Computer Engineering Department at the University of Missouri – Rolla. The laboratory contains a SCADA network with over thirty PLCs from various vendors and multiple communication networks, as shown in Figure 1. The laboratory has PLCs from Rockwell Automation (ControlLogix, PLC-5, and SLC-500), Modicon (Quantum, Momentum, 984), GE Fanuc (VersaMax, Micro 90-30) and Siemens (S7, TI505 series, Moore APACS). In addition to an Ethernet connection, the laboratory supports Control Net, Data Highway+ (Allen-Bradley), Modbus+ (Modicon), and Series Ninety Protocol (GE Fanuc). In addition, eight workstations in the laboratory support the programming of all the PLCs in the laboratory and provide the human-machine interface (HMI) programming software. The workstations all support the InTouch (Wonderware), RSView (Rockwell Automation), and Genesis (Iconics) HMI packages and can connect to any of the PLCs in the laboratory using the network. The Laboratory contains a few wireless nodes, including both 802.11 and Bluetooth nodes for comparison.

This study examined several network layers. At the application layer, the laboratory supports two control system families, Invensys/WonderWare and Modicon Quantum NOE771-10/FactoryCast, across the network. A system to control a pick-and-place robot arm has been configured that will use one of the PLCs for control; this will be the application for which we examine the relative security of each control system family. Each system family was implemented to allow write access to the PLC on the plant floor.

The SCADA Laboratory network facilities are also accessible from outside the laboratory. The application PLC program is controlled by Wonderware Suite Voyager web server, which can be remotely accessed to control the robot arm.

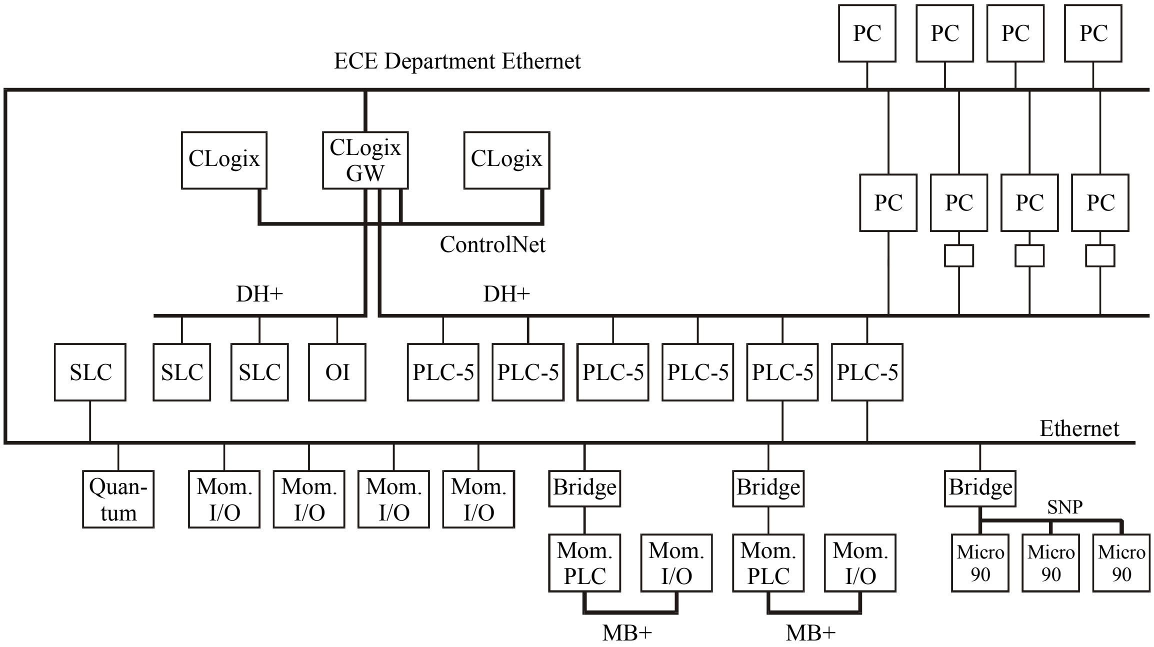


Figure 1: SCADA Network

3.0 APPLICATION LAYER

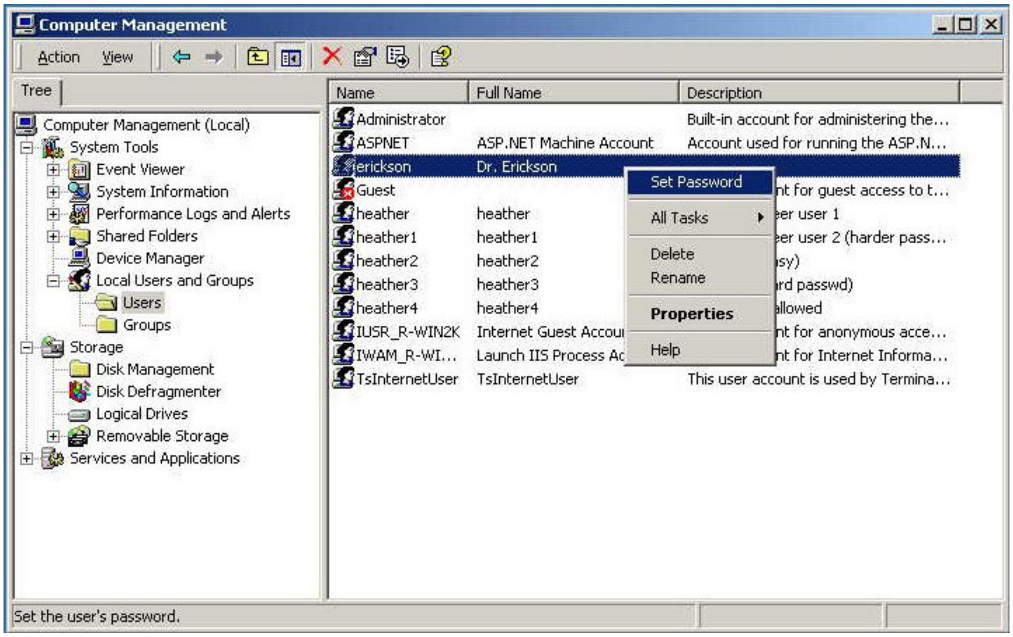
Although the integrity flaws differ, vulnerabilities exist in both control system products. Schneider Electric's NOE771 communication module in conjunction with FactoryCast software uses only passwords to authenticate the user's identity. These passwords are not encrypted or hidden. The SuiteVoyager system by Invensys/Wonderware uses Microsoft NT authentication, rendering it vulnerable to a myriad of attacks. The software itself works in conjunction with Internet Information Services (IIS) and MS SQL Server, both of which have numerous publicly documented vulnerabilities. Details on each control system family follow.

3.1 Assessment of the Invensys A^2 Control System

The Invensys A^2 control system uses Microsoft.NET technology to integrate the many components. The software family relies on Microsoft NT security to safeguard the availability of readable and writeable web pages in Suite Voyage. Implementation of any of the known attacks to NT vulnerabilities would disable the SuiteVoyager(SV) system. However, since SV requires that WonderWare's InTouch must be in runtime mode on a local machine to access the physical system through Suite Voyager, floor operations would not be interrupted unless the attack was targeted at that specific machine.

Susceptibility to External Attacks. Due to the integration of Microsoft software in running Suite Voyager, the system is sensitive to any type of system attack exploiting known vulnerabilities which have not been patched. The key to unauthorized access in Suite Voyager is an administrative login. The antivirus software vendor Sophos has identified a worm called W32/Sluter-A that searches for administrative passwords. This worm searches IP addresses for open ports then checks C$ and Admin$ for administrative passwords. There is also a remote access Trojan virus that allows access to Windows NT/XP/2000 machines. Successful implementation of the Trojan gives the hacker the ability to gather system information, scan the network, and change SQL Server activities.

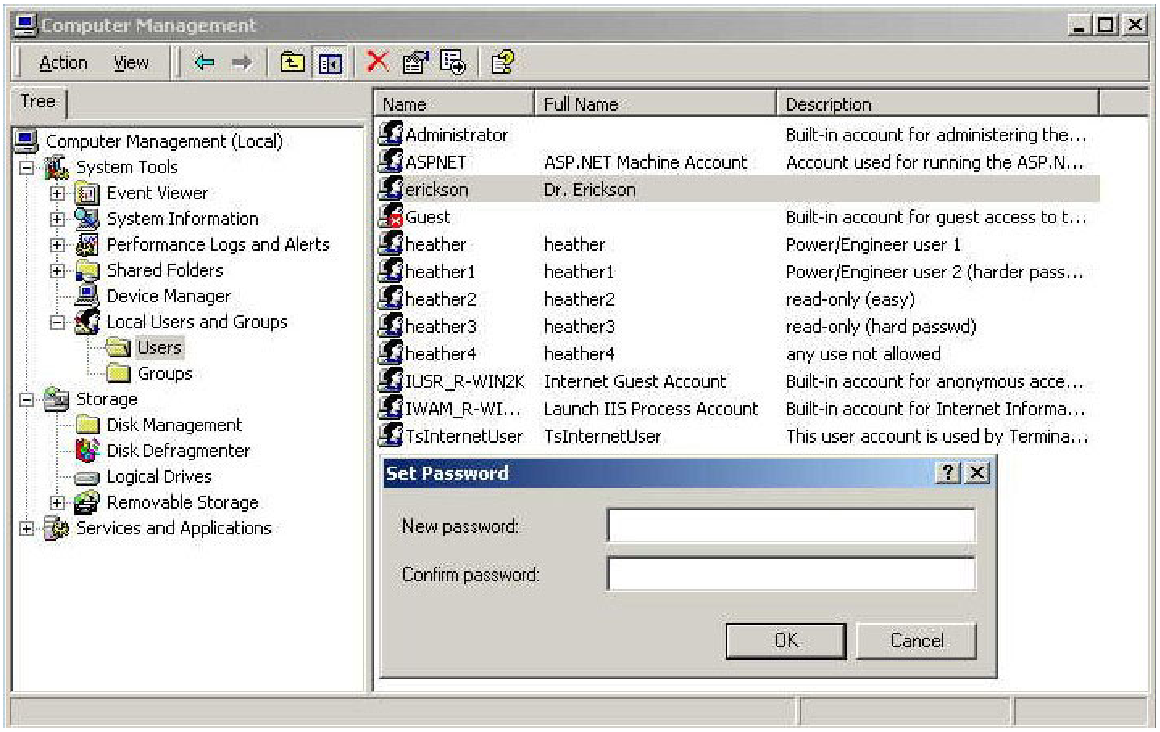
Susceptibility to Internal Attacks. Internal tampering is very easy by anyone with administrative rights on the server machine. With admininstrative access, one could alter the user profile for any user in the MS Server 2000 system. Since SuiteVoyager relies on the server for user information, any changes would prevent the user from entering the system. A simple scenario illustrates this concept. An administrative user leaves, with the terminal still logged in. While the administrator is away from the terminal, the attacker takes a seat. The attacker opens the administrative tools and enters the Users folder. Passwords can be changed from here by simply right clicking and entering the new password. The server does not ask for a confirmation of the old password before changing to the newly entered password. Figures 2, 3, and 4 show this sequence of action.



Name	Full Name	Description
Administrator		Built-in account for administering the...
ASPNET	ASP.NET Machine Account	Account used for running the ASP.N...
erickson	Dr. Erickson	
Guest		nt for guest access to t...
heather	heather	eer user 1
heather1	heather1	eer user 2 (harder pass...
heather2	heather2	sy)
heather3	heather3	rd passwd)
heather4	heather4	llowed
IUSR_R-WIN2K	Internet Guest Accou	nt for anonymous acce...
IWAM_R-WI...	Launch IIS Process Ac	nt for Internet Informa...
TsInternetUser	TsInternetUser	This user account is used by Termina...

Set the user's password.

Figure 2: Start of Administrative Rights Takeover



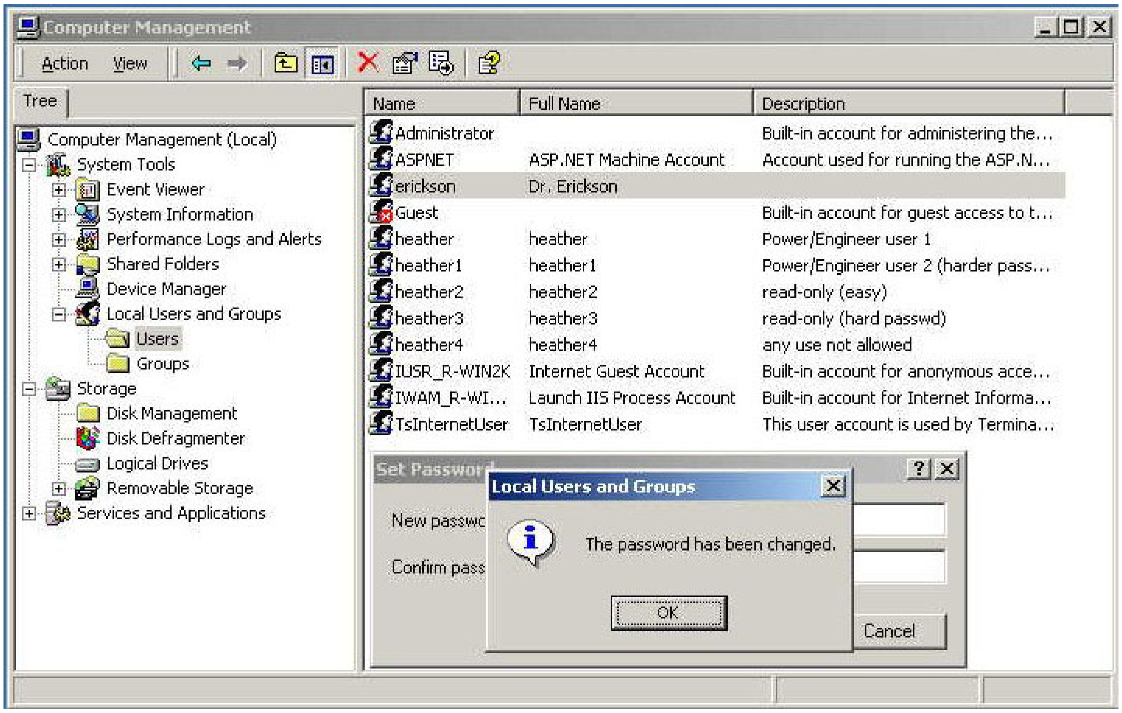
Name	Full Name	Description
Administrator		Built-in account for administering the…
ASPNET	ASP.NET Machine Account	Account used for running the ASP.N…
erickson	Dr. Erickson	
Guest		Built-in account for guest access to t…
heather	heather	Power/Engineer user 1
heather1	heather1	Power/Engineer user 2 (harder pass…
heather2	heather2	read-only (easy)
heather3	heather3	read-only (hard passwd)
heather4	heather4	any use not allowed
IUSR_R-WIN2K	Internet Guest Account	Built-in account for anonymous acce…
IWAM_R-WI…	Launch IIS Process Account	Built-in account for Internet Informa…
TsInternetUser	TsInternetUser	This user account is used by Termina…

Set Password

New password:

Confirm password:

Figure 3: Change of Admin Password without Confirmation of Old Password



Name	Full Name	Description
Administrator		Built-in account for administering the…
ASPNET	ASP.NET Machine Account	Account used for running the ASP.N…
erickson	Dr. Erickson	
Guest		Built-in account for guest access to t…
heather	heather	Power/Engineer user 1
heather1	heather1	Power/Engineer user 2 (harder pass…
heather2	heather2	read-only (easy)
heather3	heather3	read-only (hard passwd)
heather4	heather4	any use not allowed
IUSR_R-WIN2K	Internet Guest Account	Built-in account for anonymous acce…
IWAM_R-WI…	Launch IIS Process Account	Built-in account for Internet Informa…
TsInternetUser	TsInternetUser	This user account is used by Termina…

Set Password

New passwo

Confirm pass

Local Users and Groups

The password has been changed.

Figure 4: Successful Admin Password Takeover

With administrative rights, the intruder has the ability to change a user's status as well as changing remote login/ authentication options, the user group, and the lifetime of the account password.

Susceptibility to Buffer Overflow Attacks. The complete integration of Microsoft software within the Invensys system makes SuiteVoyager vulnerable to this type of attack. Reported buffer overflow vulnerabilities include: (i) Windows 2000 operating system file, ntdll.dll used to react with the system's kernel. (ii) other critically rated advisories relate to a buffer overflow vulnerabilities in MS SQL Server; and (iii) MS IIS also has buffer overflow vulnerabilities: (1) crashing IIS Server by sending overlong SebDAV, PROPFIND, or SEARCH requests; (2) exploitation of buffer overflow in the Server Side Include File handling code; (3) a cross-site scripting bug; and (4) a denial of service flaw that requires the hacker to upload files to the server.

3.2 Assessment of the Schneider Automation Control System.

Attacks on this system were focused on interrupting the webserver module or gaining access to the system. The module and FactoryCast software rely on password protection only to deter intruders. One major flaw that relates to both the external and internal threat is the possibility of someone copying the FactoryCast software. By using the same destination file, an outsider could overwrite all of the parameters set by the original engineer. All that is needed is the IP address of the NOE module.

Susceptibility to External Attack. The external attack was simulated by retrieving the password file of the NOE module through the file transport protocol (ftp). Read permission userID and password are not encrypted and can be found in a file named userlist.dat in the main directory of the webserver. Write permission is controlled through a password only and is also not encrypted. This "write" password resides at the address …rdt/password.rde. The FTP password file is the only encrypted file in the system. The file is in the following form: USERID:encrypted password. Files such as these can be deciphered using common cracking programs.

Susceptibility to Internal Attack. This system appears very friendly to internal attacks. Anyone with access to the FactoryCast program (even outside the organization) can change the write access password by transferring a new security file to the module. The external attacker also has this capability. However, the read access file cannot be changed unless the module is powered down and restarted. One quirk in the system is that one only needs read access to change the ftp access password. Also, the internal attacker has the ability to copy the FactoryCast program and re-implement it to control the same system with different parameters. The only safeguard against such actions is the time/date matching that the module performs when downloading changes to the program. This time/date matching requires that the source program and the namespace be transferred on the same day and close to the same time. This helps protect changes to the variables, but does nothing to protect the aforementioned password flaws.

Susceptibility to Buffer Overflow Attack. A successful attack was generated by using the write-back privileges on the data page of the website. When using the data editor to provide a setpoint for a feedback proportional-integral-derivative (PID) control system, the operator could easily enter a value that is outside the range of the controller.

4.0 COMMAND PACKET LAYER

To examine the vulnerabilities at the command packet layer, the behaviour of three different Allen-Bradley PLC Ethernet interfaces were analyzed: (1) PLC-5/20E processor; (2) SLC-5/05 processor; and (3) ControlLogix ENET interface. Both the PLC-5/20E and SLC-5/05 processors have built-in mechanisms for handling a DoS attack.

The PLC-5/20E and SLC-5/05 processors have a built-in web server, so Denial of Service (DoS) attacks were tried by flooding port 80 with packets. When presented with high levels of Ethernet packets, the communication port is temporarily closed [1]. Specifically, if the port receives more than 16 Ethernet frames within 10 ms, the processor disables receive interrupts for 6 ms. After the 6 ms interval, receive interrupts are re-enabled and sets the limit to 8 frames within 10 ms. Only when the processor receives no more than 8 frames within 10 ms does it increase the limit to 16 frames. The processor also tracks the number of these network "storms." Flooding the port resulted in successful Denial of Service attacks. No solutions were found to prevent the DoS attack. It should be noted that these attacks were generated by simply flooding the PLCs with data and did not require any significant level of expertise.

For the ControlLogix ENET module, the response to a DoS attack was different. It gave no response to a small amount of data , but as the amount of data sent to it and the speed of transmission were increased it started responding by sending arbitrary data. This returned data was not decoded.

For the PLC-5/20E and the SLC-5/05, their behaviour was tested when an operator interface was communicating with the processor and not through the web server, which has limited capability. A small batch control application program was running in the PLC and a workstation was providing the operator interface with a Invensys/Wonderware InTouch run-time screen. When this screen is displayed, the InTouch communication server periodically (every second) polls the PLC for changes in the status of objects on the screen and sends operator commands to the PLC. A second workstation was set up with a client program to capture the data packets between the InTouch application and the PLC. The IP addresses in the captured data packets were verified with the IP addresses of the host machines and the PLCs. Then the hex dump was analyzed to obtain the source and destination port numbers. This analysis indicated that the PLC-5 and SLC-5 communicated on port 2222. The client program was modified to connect to the PLC-5 or SLC-5 at the port 2222. The VB client successfully connected to the PLCs/SLC and some raw data were sent from the client. After receiving 26 bytes of data, the PLCs/SLC (server) closed the port connection to the client.

5.0 CONCLUSIONS AND EXTENSIONS

At the application layer, this study examined two commonly used commercial control system families, Invensys/WonderWare and Modicon Quantum NOE771-10/FactoryCast. A system to control a pick-and-place robot arm was configured that used one of the PLCs for control; this was the application for which we examined the relative security of each control system family. Each system family was implemented to allow write access to the PLC on the plant floor. Although the integrity flaws differed, vulnerabilities were found in both control system products. Schneider Electric's NOE771 communication module in conjunction with FactoryCast software uses only passwords to authenticate the user's identity. These passwords are not encrypted or hidden. The SuiteVoyager system by Invensys/Wonderware uses Microsoft NT authentication, rendering it vulnerable to a myriad of attacks. The software itself works in conjunction with Internet Information Services (IIS) and MS SQL Server, both of which have numerous documented vulnerabilities.

Both products are susceptible to external attacks, including buffer overflow attacks. Both products are susceptible to internal attacks. It should be noted that these attacks do not require any significant level of expertise on the part of the attacker. This illustrates the need to carefully evaluate COTS products for security as well as functionality prior to vendor selection.

Buffer overflows were also generated at the command packet level, resulting in successful Denial of Service attacks. No solutions were found to prevent the DoS attack. Again, this attack did not require a significant level of expertise. However, a fail-safe feature in the PLCs shut down the PLCs to avoid further corruption or attack.

There are several possible avenues for future work. Possible extensions include:

1. Expansion of the buffer overflow attack to flood the PLCs so that when the time-out is completed and the PLC opens the communication port the attack continues.
2. Analysis of the **CIP** (Control and Information Protocol), **Ethernet /IP** (Ethernet /Industrial Protocol) protocol formats so that data meaningful to the PLC-5 and SLC-5 PLCs can be transmitted.
3. Step 2 would then allow design of attacks beyond Denial of Service, specifically to take control of the PLCs remotely.
4. Analysis of the data returned by the ControlLogix ENET module to the client program. This would allow additional attack generation.
5. Detailed modeling and reachability analysis of the SCADA network using a Network Analyzer. There are two types of analyses which we think would be of interest in both commercial and military environments:
   (a) Analysis of just the IP portion of the network, to determine which hosts can connect to the gateway services, and thus who may be able to use the control functions. This analysis will be of interest if there are access control mechanisms, such as firewalls or access control lists in routers, in place in the IP network.

   (b) Some SCADA networks support devices that forward messages between different networks (e.g. between DeviceNet and Data Highway, or between two ControlNets). These devices are analogous to routers in an IP network. The analysis could be applied to the control networks themselves, if a model for the addressing system and the way these routers work can be added to the existing IP model. If the functionality of the IP gateways can similarly be modeled, then the analyzer could be used to determine which devices on a SCADA network could be controlled from which places on the IP network. This analysis would superior to the IP-only analysis, if there is significant functionality in the gateway and control message routing software. In that case, there might be, for example, public read access to some SCADA devices and more controlled access to others.

In conclusion, this study has assessed the vulnerabilities of two of the most commonly used COTS software packages for networks of SCADA sensors consisting of PLCs. It has also demonstrated the susceptibility of such sensor networks to DoS attacks at the command packet level. The need for adaptivity measures, such as boundary control based on reachability, is clearly identified.

ACKNOWLEDGEMENT

This work was partially funded by the Los Alamos National Lab, subcontract 64314-001-03. Their support is gratefully acknowledged.

REFERENCE

[1] Allen-Bradley, *Product Release Notes: Ethernet PLC-5 Programmable Controllers*, pub. 1785-RN003D-EN-P, 2002.