INFORMATION TECHNOLOGY SECURITY AT THE ADVANCED PHOTON SOURCE*

K. Sidorowicz, W. McDowell, ANL, Argonne, Il 60439, U.S.A.

Abstract

The proliferation of "botnets," phishing schemes, denial-of-service attacks, root kits, and other cyber attack schemes designed to capture a system or network creates a climate of concern for system administrators, especially for those managing accelerator and large experimental-physics facilities, as they are very public targets. This paper will describe the steps being taken at the Advanced Photon Source (APS) to protect the infrastructure of the overall network with emphasis on security for the APS control system.

INTRODUCTION

The network at the APS is typical of the networks found in large research institutions: it supports a wide variety of applications and resources, and it is dual purpose in that it supports both the administrative systems as well as the scientific systems. The APS network supports office applications, timecards, financial reporting, the wireless systems, backups, Windows PCs, Macs, Linux systems, Unix workstations, beamlines, the accelerator control system, and the interface between the beamlines and the control system.

Cyber security was considered in the initial design of the system by using defense-in-depth techniques and segmenting the system to separate components. For example, the accelerator core control system can be disconnected from the APS core and operate the systems without interruption.

THE NETWORKS

Figure 1 details the connection to the intra-laboratory networks and through these networks to the internet. The network uses a Cisco 6509 series catalyst switch with a firewall services module (FWSM) based on the Cisco Pix firewall. This allows APS to place a Tier 1 firewall in the switch, which provides the first step in the defense-in-depth protection [1].

The 6509 switch feeds a set of networks that comprise our visitor space. These networks include Visitor Wireless in the Central Laboratory/Office (CLO) building, the Conference Center, and the beamline area. In addition this layer supports video conferencing and the Vocera wireless voice over IP intercom system used by the technical groups to optimize rapid service to the beamline users. The Tier 1 firewall then delivers the packets to the Tier 2 firewall.

The Tier 2 firewall shown in Figure 1 is directly connected to the 6509 and consists of a Sidewinder G2 Cluster Security Appliance. The G2 provides a three-tiered defense-in-depth approach by using application awareness, which ensures in-depth knowledge of a complete breadth of applications; application control, which enables granular policy controls on a per-rule basis; and attack protection, which provides in-depth detection of attacks from layers 3 through 7. The G2 also integrates virus protection and spam filtering. This combination of functions greatly reduces the training requirements for the staff, as one interface controls many filtering functions.

The clustered nature of the Tier 2 firewall provides the redundancy needed to operate the critical systems of the APS. The firewall isolates the APS demilitarized zone (DMZ), which protects the internal trusted network from devices and services accessible from the Internet. To increase reliability, the Tier 2 firewall is redundantly connected to the APS core network, which in turn supports the APS trusted networks. APS has several trusted networks that are isolated from each other for security purposes. The first of these networks supports general computing, offices, and administrative functions. Secondly, the core supports the accelerator control network. The third support trusted network is for the beamlines and experiment areas. Each experimental group is isolated and no group sees traffic from any other group. This provides a secure environment for the experimenters, some of whom might be competitors. Each of these areas has associated server farms.

THE APS ACCELERATOR CONTROL SYSTEM

A short review of the APS accelerator control system will enhance the understanding of the cyber security required. The control system itself is a typical modern system based on the standard control system model that consists of operator interfaces, a network, and computer-controlled interfaces to hardware. The network provides a generalized communication path between the host computers, operator workstations, input/output crates, and other hardware that comprise the control system. The network is an integral part of all modern control systems, and network performance will determine many characteristics of a control system.

The accelerator control system itself has been implemented using the Experimental Physics and Industrial Control System (EPICS) software toolkit. At the APS, the control room operator interfaces (OPIs) are Sun Microsystems Unix workstations. The front-end computer or input/output controller (IOC) provides direct control to the input/output interfaces for each accelerator subsystem. At APS the standard crate uses the VME or VXI bus standard, Ethernet-based network communications, and a variety of signal and subnetwork interfaces. APS also supports the EPICS brick (ebrick), which is designed to be a low-cost solution for an IOC

*Work supported by U.S. Department of Energy, Office of Science, Office of Basic Energy Sciences, under Contract No. DE-AC02-CH11357.

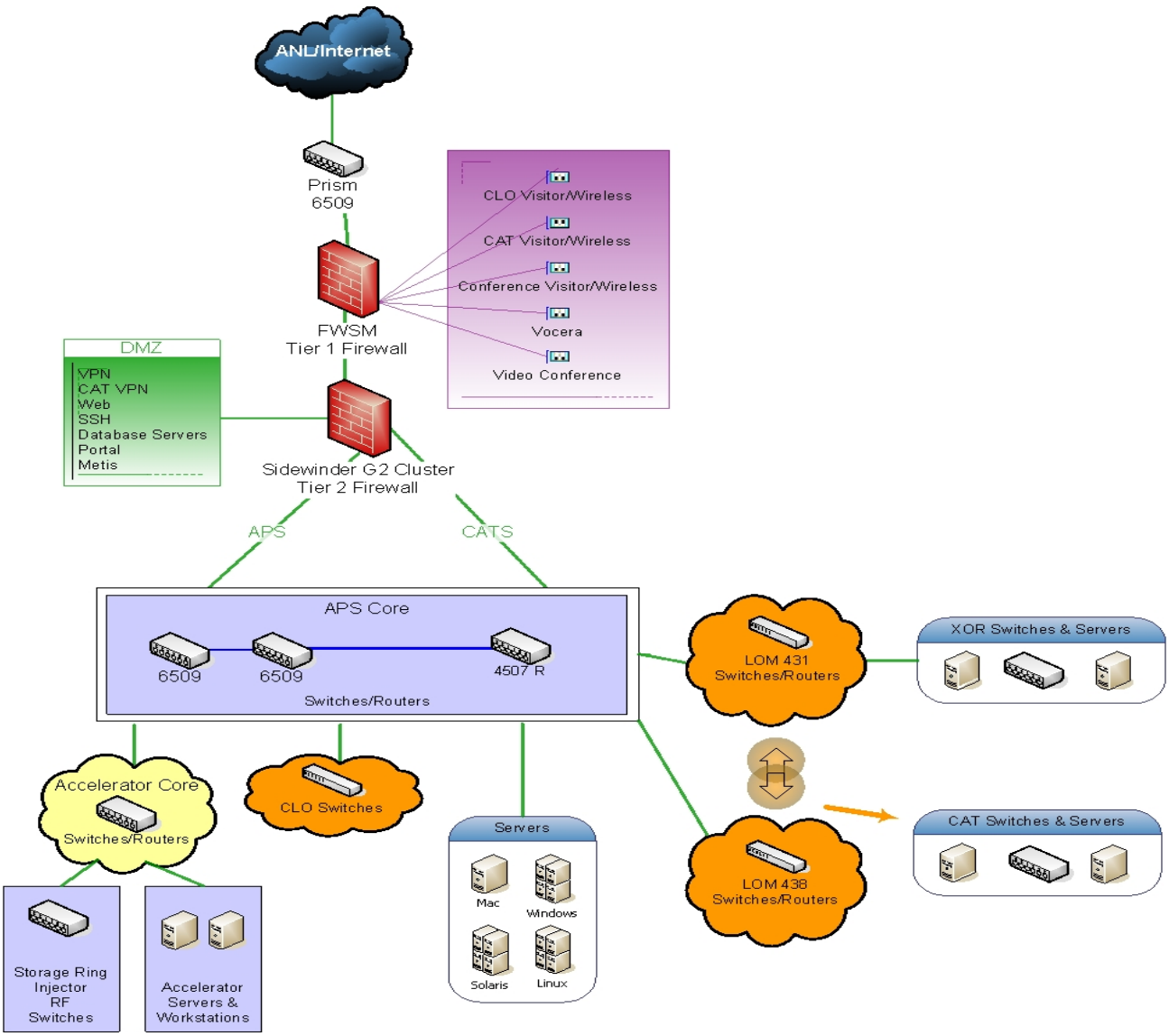

Figure 1: The APS network.

with soft real-time requirements. The current implementation of the brick is based on the PC104 Athena Single Board Computer from Diamond Systems Corporation. This configuration provides a cost-effective solution with sufficient processing power and functionality for soft IOC real-time requirements. A processor provides the IOC or brick with the intelligence to allow it to run its software autonomously with respect to all other devices in the system.

The EPICS core software running in the crate hides hardware dependencies from the high-level software running on the workstation. There are approximately 275 IOCs used in the APS accelerator control system. A real-time operating system, VxWorks, is run in the crate central processing unit (CPU) to provide the basis for the real-time control while the brick uses the Vector Linux standard 5.1 operating system, a Slackware Linux derivative. EPICS uses the TCP/IP networking protocol, a commercial standard supported by all network hardware vendors. The TCP/IP implementation is independent of the particular network medium selected to implement the network. APS uses 10-Mb, 100-Mb, and 1-Gb Ethernet.

CONTROL SYSTEMS CYBER SECURITY

The U.S. Department of Energy Office of Independent Oversight and Performance has issued a paper titled "21 Steps to Improve Cyber Security of Supervisory Control and Data Acquisition (SCADA) Networks" [2]. APS has addressed these issues by conducting a thorough risk analysis to assess the threats to the APS network. The following categories of threats were identified:

- Environmental, i.e., fire;
- Natural, i.e., hurricanes or tornados;
- Human, i.e., operator errors or disgruntled employees;

- Cyber Threats Common to All Computer Systems, i.e., hackers or insiders; and
- Cyber Threats to Control and Data Acquisition Systems, i.e., threats specific to SCADA hardware insufficiencies, administrative failures, unidentified connections to the control system network, unnecessary services running on the control system network, failure to implement the security features provided by device and system vendors, backdoors in vendor supplied equipment, lack of uninterruptible and redundant power to all equipment, and lack of internal and external intrusion detection systems.

Examined administrative failures included the lack of clearly defined cyber security roles, responsibilities, and authorities for managers, system administrators, and users; the lack of an ongoing risk management process; the lack of a network protection strategy based on the principle of defense-in-depth; the lack of clearly identified cyber security requirements; the lack of effective configuration management processes: the lack of system backups and disaster recovery plans: unlocked computer rooms: common accounts/passwords across multiple computer platforms: unmonitored user accounts: improper work and/or safety procedures that can lead to damage of critical accelerator components; and performing hardware/software upgrades that could render the accelerator inoperative if performed during non-maintenance shutdown periods.

The risk analysis was performed to assure ourselves and our management that we had addressed all of these issues. Each risk as outlined by DOE was addressed in a cyber security risk document. For each threat a matrix was developed that included the likelihood of the threat, the unmitigated risk level, the mitigation applied at APS, and the residual risks with the likelihood of their occurrence.

DEFENSE IN DEPTH

Examining the risk analysis with the aim of improving security has helped direct funding to the items where we can get the most value for each dollar spent. The risk analysis also points out that not all threats to the system come from the outside and the Internet. The firewalls are very good at isolating the SCADA systems from network threats. The system also must be designed to look for internal threats such as connecting an unauthorized computer to the controls network. APS has a live database of allowed MAC addresses for each of our networks. Unauthorized connections are detected by Arpwatch. Arpwatch is a tool that monitors Ethernet activity and keeps a database of Ethernet/IP address pairings. It also reports certain changes via email to the system administrators.

When APS users asked to have a real-time connection to accelerator data it was agreed that letting experimenters connect directly to the APS control system was not a good idea. The solution was to implement EPICS Channel Access (CA) gateways. Channel Access is the EPICS network protocol. The gateway is a proxy server for the Channel Access protocol and thus the accelerator controls data. The gateway has an EPICS Access Security layer that can configure the clients from which hosts may have read or write access to a channel. To isolate a private high reliability network from other networks, the gateway is run on a host equipped with two or more network interface cards. The network and IOC load implied from CA clients residing in other nets is limited and independent from the number and the behavior of those clients. Access can be restricted using the gateway's Access Security Layer. This allows safe connections to the control network from the beamlines and indeed from any of the APS networks.

In addition to the Tier 1 and Tier 2 firewalls, APS restricts accounts on the controls network. Having an account on this network requires 1) that an individual have a need to directly access the system, and 2) management approval. Crypto cards are required to log into the controls servers and remote logins are restricted to a few administrators' workstations. The controls VLAN is not distributed outside of the limited controls network

CONCLUSION

The following steps to securing a SCADA system should be implemented [3]:

- Perform a critical asset identification and risk assessment,
- Create a security policy and provide for regular updates,
- Create a disaster recovery plan with periodic reviews,
- Deploy protective measures, and
- Provide security monitoring and management.

ACKNOWLEDGMENTS

Thanks to Christy Dannenberg and Dave Leibfritz for advice and help with drawings.

REFERENCES

[1] Idaho National Laboratory, "Control Systems Cyber Security: Defense in Depth Strategies," External Report #INL/EXT-06-11478, May 2006, http://csrp.inl.gov/documents/Defense%20in%20Depth%20Strategies.pdf

[2] U.S. Department of Energy, Office of Independent Oversight and Performance Assurance, "21 Steps to Improve Cyber Security of SCADA Networks," http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[3] Eric Byres, David Leversage and Nate Kube, "Security Incidents and Trends in SCADA and Process Industries," The Industrial Ethernet Book, Issue 39, May 2007, http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=1823