Cyber Security Enhancements for CEBAF Controls Network

L.Clancy, B.Cumbia,
Jefferson Lab, 12000 Jefferson Ave., Newport News, VA 23606

Thomas Jefferson National Accelerator Facility
Newport News, Virginia, USA

Abstract

This Poster describes the current projects within the Continuous Electron Beam Accelerator Facility (CEBAF) to enhance Cyber Security with respect to maintaining full control of the CEBAF through its computing systems, including IOCs, low level controllers, network elements, UNIX systems for high level control, and Microsoft OS desktops for general purpose access. The poster will cover the efforts of the System Administration team known as ACE to strictly control and maintain the configuration of all systems and network elements on the CEBAF controls network; out-of-band management of the IOCs using secure protocols and console I/O logging; use of Channel Access Gateways to limit outside access to IOCs; and several other security enhancements.

Configuration Control

Having several different versions of VxWorks running on IOC's, some of which enabled FTP protocol, better configuration controls were needed. A single version of VxWorks with a well known set of enabled options is now being used on all IOC's. The configuration of all PC's, workstations, servers and network equipment has been standardized, documented and strictly controlled.

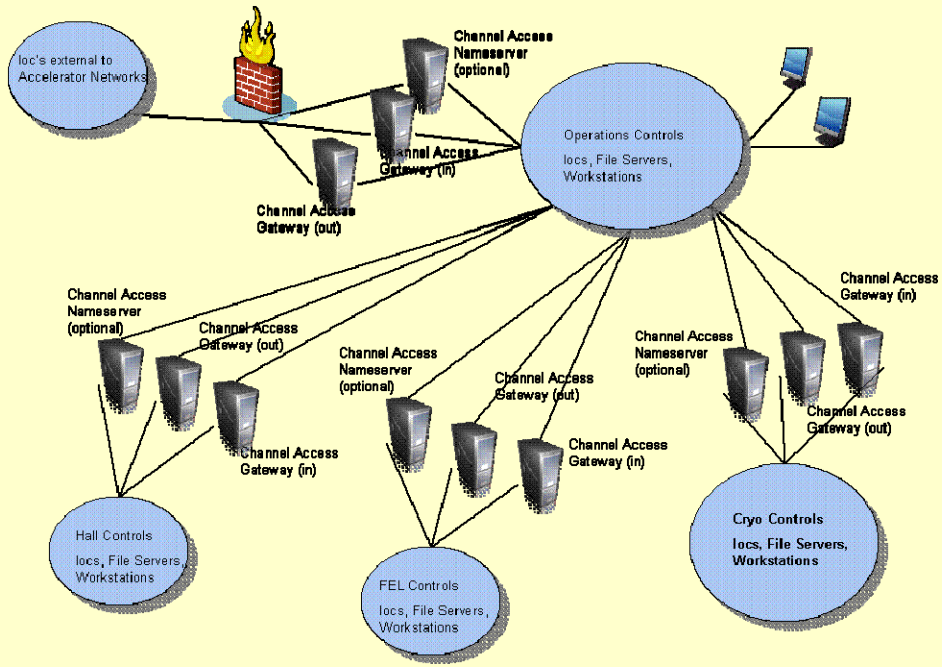
Disable Telnet, RSH and FTP

The out-of-band management of IOCs means that telnet can be turned off at the boundary of the CEBAF network. It is anticipated that telnet will be disabled everywhere when we are convinced that the out-of-band management suffices. RSH protocols are now turned off on all workstations and most servers. RSH protocols are now behind TCP wrappers and allowed only for the few remaining IOCs that boot using RSH. FTP protocol is completely disabled. We use safetp exclusively. The well known fault of these protocols is that they allow unencrypted passwords to traverse the network - easy prey for network sniffers.

Out-of-band IOC management

All CEBAF IOCs are being equipped with serial port console terminal servers. These servers are configured to require SSH version 2 protocol for authentication and encrypted communication, and log all traffic into and out of the IOC console serial port.

Future IOC Segmentation at CEBAF



IOCs now use NFS booting versus RSH

Most CEBAF IOCs have been configured to use NFS booting versus RSH booting. All remaining CEBAF IOCs that still use RSH for booting will soon be changed to NFS. NFS booting allows much tighter control over the filesystems (on the fileserver) that the IOCs have access to. Only two filesystems are exported to IOCs by a given fileserver; one for vxworks, EPICS, and application support files; and the second for IOC output data. RSH booting and filesystem access meant that every filesystem available to the fileserver was also available to the IOC. In addition, RSH booting and file access is much slower than NFS. IOCs using NFS now boot 80% faster than those using RSH. RSH booting also suffered from scalability problems; each file request consumed two pseudo Ttys on the fileserver out of a maximum of 256. This means that a total of 128 files could be open at the same time – far smaller than the number of files needed to boot 158 IOCs in the Accelerator. This meant that IOC recovery after a power outage had to be serialized so that only one or two IOCs were booting simultaneously. It is now possible to boot every IOC simultaneously, so recovery after a power outage is now more than an hour shorter.

PV Nameserver and Channel Access Gateways

A modified channel access nameserver and five channel access gateways are now in service. The motivation for the nameserver and gateways is to reduce broadcast traffic by channel access clients. A broadcast is normally required to resolve each Process Variable (PV) and would be sent to the broadcast address of each network that contains IOCs that have PVs to be monitored. These broadcasts increase the load on the IOCs since every IOC must check to see if it hosts the requested PV. Instead, the nameserver receives all of the broadcast traffic and resolves any PV in CEBAF and the experimental halls. It returns the address of an IOC to use to monitor the PV. If a gateway is available, the gateway address is given rather than the IOC address. A gateway serves as a proxy for real IOCs, meaning that the client monitors a PV from the gateway rather than connecting directly to the IOC. In each of the three experimental halls, a gateway allows clients to monitor all PVs that reside on IOCs in the CEBAF and the other experimental halls. Another gateway within CEBAF allows all PVs in the experimental halls to be monitored by clients within CEBAF. The fifth gateway allows any CEBAF PV to be monitored. This service is especially important when considering segmentation of IOCs onto separate protected networks.

Near term enhancements

The two primary routers that support CEBAF will be upgraded with new chassis, power supplies, supervisor modules, and firewall service modules (FSM) during the next Scheduled Accelerator Downtime (SAD) in early 2008. We anticipate that the FSMs will allow us to further tighten access controls to the IOCs.

Future enhancements

We are investigating segmenting all IOCs within CEBAF onto several internal networks, each supported by a channel access gateway and a fileserver. These internal networks would have no visibility from general purpose CEBAF networks, so that IOCs would be immune from network scanning.

*Work supported by the U.S. Department of Energy, contract DE-AC05-06OR23177

Acknowledgments

The Accelerator Computing Environment (ACE) team is composed of system and network administrators from the Accelerator division and network administrators from the Engineering division. The Ace team members include the authors (LeonClancy & Brad Cumbia), Anthony Cuffe, Theo McGuckin, Theo Larrieu, and Scott Windham.