BROOKHAVEN
NATIONAL LABORATORY

BNL-77911-2007-CP

Cybersecurity and user accountability in the C-AD control system

J.T. Morris, S. Binello, T. D'Ottavio, R.A. Katz

Presented at the International Conference on Accelerator and Large Experimental Physics Control Systems (ICALEPCS 2007)
Knoxville, TN
October 15 – 19, 2007

Collider-Accelerator Department

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

DISCLAIMER

CYBERSECURITY AND USER ACCOUNTABILITY IN THE C-AD CONTROL SYSTEM *

J.T. Morris#, S. Binello, T. D'Ottavio, R.A. Katz, BNL, Upton, New York, USA.

Abstract

A heightened awareness of cybersecurity has led to a review of the procedures that ensure user accountability for actions performed on the computers of the Collider-Accelerator Department (C-AD) Control System. Control system consoles are shared by multiple users in control rooms throughout the C-AD complex. A significant challenge has been the establishment of procedures that securely control and monitor access to these shared consoles without impeding accelerator operations. This paper provides an overview of C-AD cybersecurity strategies with an emphasis on recent enhancements in user authentication and tracking methods.

INTRODUCTION

Cybersecurity has been a major area of concern for C-AD network and system administrators for many years. This paper describes how C-AD cybersecurity efforts have recently expanded in response to a new emphasis on the risks associated with unauthorized access to C-AD computers on site at Brookhaven National Laboratory(BNL). It focuses particularly on attempts to provide individual accountability for all actions taken at the Linux control system computers at C-AD.

CYBERSECURITY REVIEW

In order to ensure uninterrupted operation of the Relativistic Heavy Ion Collider(RHIC) and other C-AD programs, many measures have been put in place to protect the C-AD accelerator controls network from cybersecurity threats. Self auditing software is installed on computers in the controls network to detect unauthorized system changes. BNL's Information Technology Division (ITD) conducts network scans to uncover vulnerabilities in C-AD computers. Critical system log entries are stored locally and forwarded to ITD for redundant logging in central BNL cybersecurity logs. The controls network is separated from the general BNL network by a firewall with restrictive access rules. Two factor authentication using CryptoCard tokens is required in order to gain access to the accelerator controls network. ssh access to the controls network is logged. A web based viewing tool allows system administrators or control room operators to monitor the use of the ssh access gateways. The C-AD Set History System [1] maintains a history of all control system settings. The originating computer and username are recorded for all changes of accelerator equipment settings.

In 2006, new attention was called to cybersecurity issues at BNL A Department of Energy(DOE) cybersecurity audit in September of 2006 focused on cybersecurity threats associated with physical access to computers on site at BNL. During a labwide cybersecurity standdown, all BNL employees received updated cybersecurity training and reviewed the security of their personal computers. Employees were asked to ensure that their passwords complied with DOE password requirements and that their computers had locking screen savers that took effect after a short period of inactivity.

The 2006 cybersecurity review represented a shift in focus for the C-AD cybersecurity program. The risk from insider attacks has historically been considered low in C-AD's research environment. Previous cybersecurity measures primarily focused on attacks from outside the controls network. While the perimeter defense continues to be important, new attention now has to be paid to the vulnerability to inside attacks. The focus on threats from the inside is not unique to DOE. In the Computer Security Institute's "2007 Computer Crime and Security Survey" [2], insider abuse was reported to be the most prevalent security problem. Insider abuse problems were reported more frequently than virus attacks.

The cybersecurity measures reviewed in the October 2006 cybersecurity standdown were intended to provide full individual accountability for all actions taken at BNL computers. Establishing individual accountability aids in both the detection and deterrence of insider abuses. [3] By following established cybersecurity standards, individual accountability can be achieved rather easily for desktop computers that are used in standard office situations. System logs provide a reliable record of who was using a computer at any given time. Many of the computers used for accelerator operation, however, present special cybersecurity problems. Individual accounts do not work well in accelerator control rooms. Many users share computer consoles in control rooms. They do not only share computer consoles, they share console login sessions. Active sessions must be handed off from user to user in order to effectively run an accelerator.

Group accounts have historically been used to satisfy the operational needs of the control room settings at C-AD. A designated list of individuals was given access to the group account password. New login sessions at control room consoles had to be started by one of these individuals. Once a group session was started, the console was available to any user in the control room. Locking screen savers were disabled so that users had easy access to the computer and the screen displays remained active and visible. This is extremely important for accelerator operations since many control room screens are used for comfort displays. Operators rarely interact with the computers that drive these displays but the displays must be visible at all times. This group account configuration satisfied operational needs but it

*Work performed under the auspices of the U.S. Department of Energy

#jtm@bnl.gov

did not provide individual accountability for actions taken at the control room consoles.

CYBERSECURITY ENHANCEMENTS

The existence of group accounts in the C-AD controls network was considered a cybersecurity risk. In January of 2007, C-AD staff and ITD staff examined ways to minimize the risks associated with the use of group accounts. Several new cybersecurity measures were put into place.

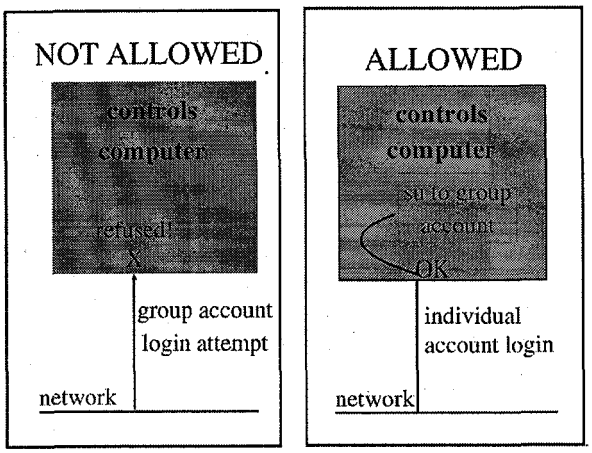


Figure 1: Network Access Method for Group Accounts

Network Access

It was agreed that new restrictions would be placed on network access to group accounts. Direct network logins with group account are disallowed using Pluggable Authentication Modules for Linux (Linux-PAM) [4]. A control system user can only gain network access to a group account by first logging in with an individual account. The user may then 'switch user' to the group account with the su command. A two layer authentication is effectively required with user supplying both individual and group account credentials. The su operation, including originating individual account, is logged in local system logs and forwarded to central BNL cybersecurity logs. The history in these logs can then identify which individuals have gained access to the group account at any given time. The use of ssh instead of su for the 'switch user' operation is being considered. This has the advantage of easily preserving X window forwarding. We need to ensure that logging of the ssh operation is done in a way that reliably provides the identity of the originating user.

It was also agreed that membership in a group account would be strictly managed. All individuals given the group account password are required to sign a log and agree to follow safe practices when using the group account. In addition, group accounts are limited to use on a designated list of computers in designated locations. The group account is not available on any other control system computers. Group account members must use their personal accounts for work outside the control room. Special restrictions may be applied in network firewalls to further restrict traffic from computers with group accounts.

Monitoring and Controlling Console Access

The actions defined above provide risk mitigation but they do not provide true individual accountability for users working at control room consoles with group accounts. Various measures were considered to monitor and control physical access to control room consoles. The use of card readers at control room entry points was considered. This was determined to be impractical for most C-AD control rooms. Card readers could only be practical in locations where access routes are limited and the area in question is used by a very limited number of people. When the number of individuals present in a control room at one time is large, the card reader record can not do a good job of identifying an individual responsible for an action taken at one of the control room consoles.

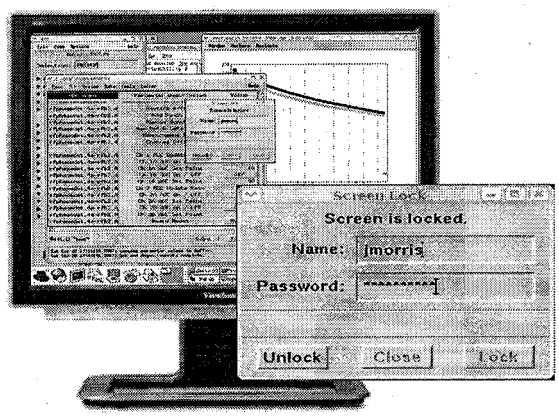
The use of video cameras was also considered. Operators and others who spend much of their time in the control room raised strong objections. They viewed cameras as an invasion of privacy. It was also noted that in some circumstances the video record might have little value. Someone with malicious intent could conceal their identity or disable a camera before using the console. The use of card readers or video cameras would also require the installation and maintenance of significant new infrastructure at C-AD.

Another alternative considered was the use of RFID tags. A user wearing an RFID tag may become authorized based on proximity to the control room console. The RFID solution offers the possibility of transferring console control from one user to another without the entry of a password. Commercial RFID systems are available that keep logs of individual access to the computers in the system. This option was rejected due to the fact that no commercial RFID user authorization systems were found for Linux systems. We also recognized, however, that the system has a serious security vulnerability if password entry is not used along with the RFID tag. A misplaced RFID tag can provide easy anonymous access to the control system for anybody who finds the tag.

ScreenLock

The solution chosen to monitor and control access to C-AD Linux control room consoles was a software screen lock. The ScreenLock program, developed in house for Linux systems at C-AD, requires a user to pass an individual authentication layer to gain access to a group account session. ScreenLock is similar in function to a commercial product called TSL-PRO™, which is only available for Windows systems. In order to start a group account session at a Linux control room console, the user first performs an ordinary desktop login with group account username and password. Before the computer becomes available for use, the ScreenLock program prompts for a secondary login with individual username and password. Group account credentials will not be accepted by the ScreenLock program. Individual authentication with ScreenLock is accomplished using a

library interface to Linux-PAM authentication modules. A record of the user authentication is logged in local system



logs and forwarded to central BNL cybersecurity logs.

Figure 2: ScreenLock at Group Account Console

Once a group session is established at a control room console, control of the group session is transferred from one individual to another with ScreenLock When a user leaves a console, the screen can be manually locked. The next user of that console must enter his or her individual account username and password to gain access. The underlying group account session continues uninterrupted during this transfer. If the computer is left idle for a short period of time, the ScreenLock automatically takes effect and locks the computer. Note that the display continues to update while the ScreenLock is in effect. This is particularly important for control room screens that are used for comfort displays.

The added layer of authentication required by ScreenLock is extra work for users but it is considered a preferred alternative to other measures such as cameras or card readers. We believe that it provides a higher level of individual accountability than these other approaches. The primary weakness of the ScreenLock approach is its reliance on user compliance. User compliance is essential in order to achieve cybersecurity goals with the ScreenLock approach. Control of a login session can be transferred without reauthentication if users do not follow proper procedures. User training in the use of ScreenLock is important.

CONCLUSION

The enhanced cybersecurity measures for console access described in this paper have been in place in the C-AD Main Control Room since late August of this year. They provide a greatly enhanced level of individual accountability without interfering significantly with the efficient use of control room consoles. The same approach is planned for other smaller control rooms in the C-AD accelerator complex.

Network restrictions with Linux-PAM are in the process of being fully implemented. For a small set of computers, direct network access with a group account is still necessary to allow management of server processes that run under the group account. Alternative mechanisms of server process management are being considered. Full implementation of network restrictions is expected by the end of this year.

ACKNOWLEDGEMENTS

I would like to thank John J. Woods of C-AD for his invaluable help in the investigation of cybersecurity solutions.

REFERENCES

[1] T. D'Ottavio, W. Fu, D.P. Ottavio, "Tracking Accelerator Settings", ICALEPCS 2007, October 2007

[2] Computer Security Institute, "2007 Computer Crime and Security Survey"

[3] "Federal Plan for Cyber Security and Information Assurance Research and Development", National Science and Technology Council, Interagency Working Group on Cyber Security and Information Assurance, April, 2006, p. 39-40

[4] "Reference Guide for Red Hat Enterprise Linux 4.5.0, Chapter 16: Pluggable Authentication Modules (PAM)", http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/en-US/Reference_Guide/