Cybersecurity and User Accountability in the C-AD Control System

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

Brookhaven National Laboratory, Upton, New York, USA

Collider-Accelerator Department

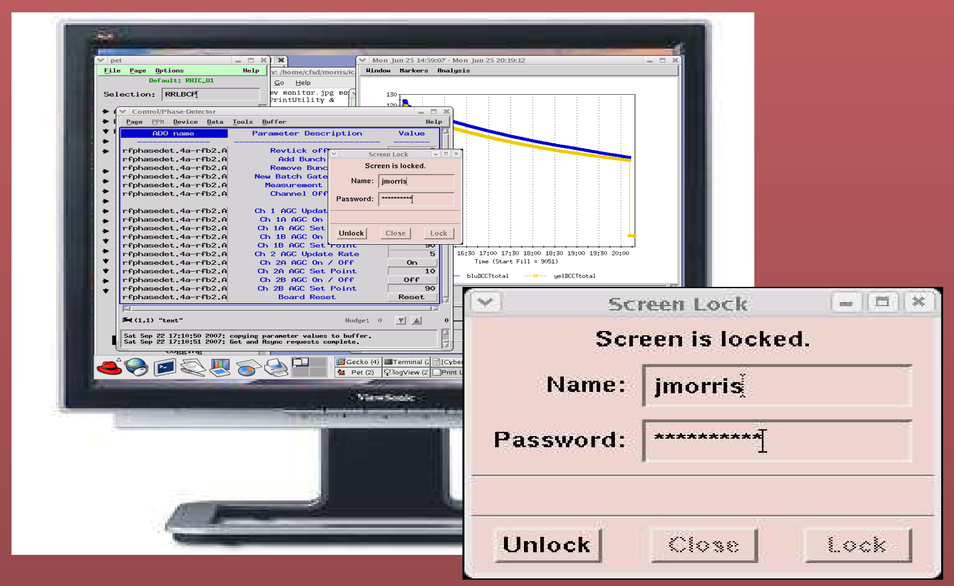
The Goal

Provide individual accountability for all actions taken at Control System computers.

The Problem

- Individual accounts do not work well in control room settings. Many users share computer consoles. Active console sessions must be handed off from user to user.
- Group accounts satisfy operational needs but do not provide individual accountability.

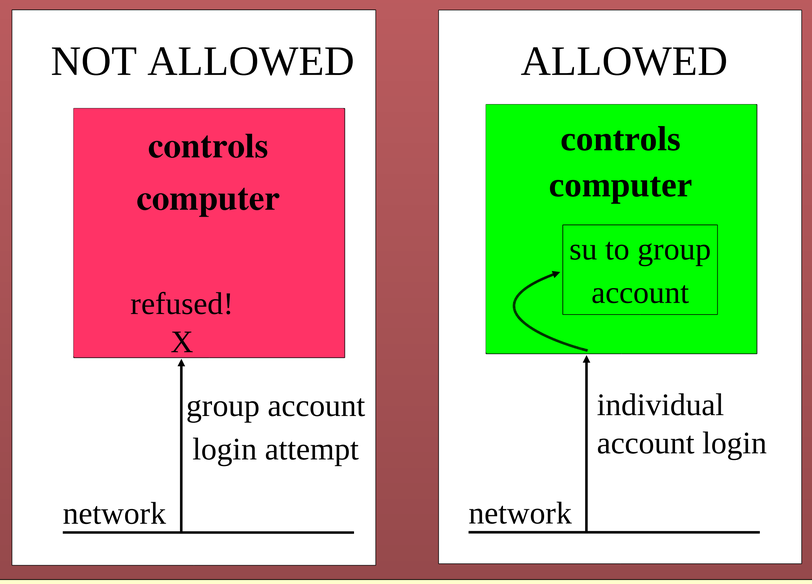
At the Console



The Solution

Use group accounts but require individual authentication for all access to group account sessions.

Over the Network



- Primary login with group account user/password.
- Secondary login via ScreenLock with individual user/password.
- Screen is locked while not in active use, display continues to update while locked.
- Control of group session is transferred from one individual to another with ScreenLock – underlying group session continues uninterrupted.
- Individual authentication with ScreenLock is logged in local system logs and forwarded to central BNL cybersecurity logs.
- The ScreenLock program was developed in-house at C-AD.

- Direct network logins with group account are disallowed using Linux Pluggable Authentication Modules (pam).
- Users first log in with individual credentials and then 'switch user' to group account.
- Switch user(su) operation, including originating individual account, is logged in local system logs and forwarded to central BNL cybersecurity logs.