SLAC Controls Security Overview

- **Introduction**
  - SLAC has multiple disciplines: Photon Science, Astrophysics, HEP
  - Controls for LCLS, PEP, ILC
  - EPICS and Legacy SLC Controls
- **Use Central and Local Resources**
- **Design with Security in mind**
- **Implement security practices throughout project**

Terri Lahey
lahey@slac.stanford.edu

Centralized Resources: Security

Central Security Team at SLAC

- Experts in security issues
- Interface with DOE
  - Track issues
  - Report to DOE
  - Understands DOE-cyber procedures, which change
- Coordinate Security Reviews
- Help us implement and maintain secure control system
  - remove clear text passwords (ftp,xdm)
  - Block windows ports
  - Tunnel into SLAC
- Coordination of site so other SLAC programs don't impact us.

Centralized Resources: Networks

- Central Management of SLAC Networks and Firewalls improves security
- Network address space defined by central network team
- Central management of switches & routers
- Central Physical Layer support
- Central and local Response to problems
- Controls network managers work with Central Network to meet our needs

Design with Security in mind

- Isolate Control System networks
  - control access to accelerator
  - Some accelerator components require insecure protocols for control equipment, eg. Telnetd, and would be hard to run on main networks
  - Keep non-control traffic off accelerator networks and vice versa
- Use configuration profiles when creating servers
  - Standard implementation reduces chance for security problem (and potential operational problems)
- Use Good Account practices
  - Individual accounts for individuals; disable and delete
  - Common accounts locked down in control rooms for 24x7 operations
- Many more…

Terri Lahey
lahey@slac.stanford.edu

Security Practices

- Upgrade/patch servers according to accelerator schedule
- Channel Access security by user
- Scan networks for security issues:
  - Daily
  - scheduled quarterly/downtime
  - scan node on demand
- wireless on visitornet outside SLAC networks
- IFZ – IP range on every subnet
- disconnect point – test and user buyin if using Central Services
- Special laptops for accelerator physical connection & wireless

Security Practices (2)

Network management

- Register and track network nodes
- Enter control devices in DNS, with fixed IP addresses
- DHCP static addresses
- Router block unregistered nodes
- Track where nodes have been connected
- Upgrade: Enhance current network monitoring by integrating with EPICS

Central Experts for Services

- Central experts for services that require a lot of attention to security
  - web servers
  - application servers
- Central Services
  - Email
  - Account Management
  - Desktop management (build & patching)

Conclusion

- Security of the worst node can cause problems for all – real or perceived
- Implement secure computers, networks and practices using local experts that work with central experts.
- Build secure architecture - know what is happening on your systems/network
- Create good procedures, and revise as needed

Terri Lahey
lahey@slac.stanford.edu