Control System Cyber-Security Workshop (CS)2/HEP

Sunday 14 October 2007 - Sunday 14 October 2007

Crowne Plaza Hotel

Book of Abstracts

Contents

1

Welcome

Author: Stefan Lueders[1]

[1] *CERN*

3

Discussion

4

Role Based Access Control for the Accelerator Control System at CERN

Author: Suzanne Gysin[1]

Co-authors: Andrey Petrov [1]; Carl Schumann [1]; Grzegorz Kruk [2]; Kris Kostro [3]; Pierre Charrue [3]; Stephen Page [3]; Verena Kain [3]; Wojciech Gajewski [3]

[1] *FNAL*

[2] *CDEN*

[3] *CERN*

Given the significant dangers of LHC operations, access control to the accelerator controls system is required. This paper describes the requirements, design, and implementation of Role Based Access Control (RBAC) for the LHC & injectors controls systems. It is an overview of the two main components of RBAC: authentication and authorization, and the tools needed to manage access control data. We begin by stating the main requirements of RBAC and then describe the architecture and its implementation. RBAC is developed by LAFS a collaboration between CERN and Fermilab.

5

Control System Cyber Security Measures at the Advanced Photon Source

Author: Deborah Quock[1]

[1] *Argonne National Laboratory*

Large accelerator facilities such as the Advanced Photon Source (APS) typically are operated by a diverse set of integrated control systems such as IOCs, PLCs, and FPGAs. At APS, the supervisory controls software that connects and unifies these programmable units is Experimental Physics and Industrial Control System (EPICS). Layered on top of EPICS is the relational database Web-viewable software tool Integrated Relational Model of Installed Systems (IRMIS) that was designed and implemented at APS to provide intuitive and easily navigated views of the APS control system software and hardware components.

This layered control system structure at APS comes with inherent cyber security risks. The software security measures that have been investigated and are available for the APS control system are presented in this paper.

6

Update on the CERN Computing and Network Infrastructure for Controls (CNIC)

Author: Stefan Lueders[1]

[1] *CERN*

Over the last few years, modern accelerator and experiment control systems are based more and more on commoncommercial-off-the-shelf products (VME crates, PLCs, SCADA systems, etc.), on Windows or Linux PCs, and on communication infrastructures using Ethernet and TCP/IP. Despite the benefits coming with this (r)evolution, new vulnerabilities are inherited, too: Worms and viruses spread within seconds via the Ethernet cable, and attackers are becoming interested in control systems. Unfortunately, control PCs cannot be patched as fast as office PCs. Even worse, vulnerability scans at CERN using standard IT tools have shown that commercial automation systems lack fundamental security precautions: Some systems crashed during the scan, others could easily be stopped or their process data be altered. During the two years following the presentation of the CNIC security policy at ICALEPCS2005, a "defense-in depth"approach has been applied to protect CERN's control systems. This presentation will give a review of its thorough implementation and its deployment. Particularly, measures to secure the controls network and tools for user-driven management of Windows and Linux control PCs will be discussed.

7

Remote Access to Alice

Author: Peter Chochula[1]

Co-authors: Andre Augustinus [1]; Lennart Jirden [1]; Peter Rosinsky [1]

[1] *CERN*

In the design of the control system for the ALICE experiment much emphasis has been put on cyber security. The control system operates on a dedicated network isolated from the campus network and remote access is only granted via a set of Windows Server 2003 machines configured as application gateways. The operator consoles are also separated from the control system by means of a cluster of terminal servers. Computer virtualization techniques are deployed to grant time-restricted access for sensitive tasks such as control system modifications. This paper will describe the global access control architecture and the policy and operational rules defined. The role-based authorization schema will also be described as well as the tools implemented to achieve this task. The authentication based on smartcard certificates will also be discussed.

8

Secure Remote Operation of Light Source Beamline Controls with FreeNX

Author: Zhijian Yin[1]

Co-author: Peter Siddons [1]

[1] *Brookhaven National Lab*

In light source beamlines, there are times when remote operations from users are desired. This becomes challenging, considering cybersecurity has been dramatically tightened throughout many facilities. Remote X-windows display to Unix/Linux workstations at the facilities, either with straight x traffic or tunneling through ssh (ssh -XC), is quite slow over long distance, thus not quite suitable for remote control/operations. We implemented a solution that employs the open source FreeNX technology. With its efficient compression technology, the bandwidth usage is quite small and the response time from long distance is very impressive. The setup we have, involves a freenx server configured on the linux workstation at the facility and free downloadable clients (Windows, Mac, Linux) at the remote site to connect to the freenx servers. All traffic are tunneled through ssh, and special keys can be used to further security. The response time is so good that remote operations are routinely performed. We believe this technology can have great implications for other facilities, including those for the high energy physics community.

9

Network and computer security in the Fermilab Accelerator Control System

Author: Tim Zingelman[1]

[1] *Fermi National Accelerator Lab*

The balance between security and usability in the Fermilab Accelerator Control System will be presented. The control system contains a wide variety of systems, with varying abilities to protect themselves and varying risks to other systems on the network. The community of Physicists, Engineers, Computer Professionals and others who repair, maintain and constantly improve this control system need to have sufficient access to the systems to remain productive, while keeping out the unwanted traffic. We have achieved the current balance by using a wide range of tools and methods. This presentation will discuss these tools and methods.

10

WARCS -Wide Area Remote Control for SPring-8

Author: Akihiro Yamashita[1]

Co-author: Yukito Furukawa [1]

[1] *SPring-8*

WARCS (Wide Area Remote Control for SPring-8) is a system which allows experts to access machine control computers from the outside of SPring-8 campus. Computer network for SPring-8 machine control is strictly protected by firewalls from the internet. When a machine expert get a phone call from the operation crew at troble, he/she can access computers “making a tunnel” in the firewall with WARCS system. There are several tunnel tools available in the market, but we could not find one to meet our requirements. Requirements are as follows. 1.The experts can access under shift leader’s permission. 2. No system access to the gateway server from outside. 3. Only one server account. 4. Easy operation. We build our own tunneling tool, WARCS, to satisfy above requests with combination of linux firewall system (iptables), secure ip tunnel program (Zebedee), http server (Apache), database program (SQLite) and glue scripts (python). We build client programs for multi operation system (Windows, Macintosh and Linux). WARCS deployed at the beginning of 2004. Since the it has been successfully operated safely.

11

Cyber-Threats, Cyber-Vulnerabilities, and Cyber-Risks

Author: Stefan Lueders[1]

[1] *CERN*

An emerging trend in Control Systems is the growing usage of general IT standards, tools, protocols, and methods. Due to this adoption, also common weaknesses and vulnerabilities have been inherited by those Control Systems.

This presentation will cover the risk equation: threat, vulnerabilities, and consequences.

12

Perspective on secure network for control systems in SPring-8

Author: Toru OHATA[1]

Co-authors: Miho ISHII [1]; Ryotaro TANAKA [1]; Toru FUKUI [2]

[1] *JASRI/SPring-8*

[2] *RIKEN/SPring-8*

SPring-8, a third-generation open user facility of synchrotron radiation, accepts many experiment users coming from outside facilities. The users, which constructed their own control system at each beam-line, require a fast, stable and secure network environment to perform their experiments. At first, we installed firewall systems to protect the network from outer intrusion. However, the users connect own PCs to the network. If a PC is carriers of some kind of computer virus, there is a possibility that the network affects fatal damage, because a firewall have no effect on attack from the inside. The modern IT has a lot of risks against the network system for control and data acquisition. All risks cannot be avoided by only one method. To achieve a secure network environment, we adopted various approaches. Network segregation designing is the most important thing. The range and the scale of the network trouble are controlled by

firewall and VLAN when an incident occurs. The network trouble is prevented from spreading, and we can defend other experiments and a facility operation. Intrusion detection and quarantine are also important. We installed intrusion protection system (IPS), because attacks for vulnerabilities are hard to protect by a firewall. Traditional SNMP monitoring system and newer sFlow analyzer help realtime analysis and restoration from problems of a network infrastructure. We introduced these traffic monitoring systems. In addition, we prepared patch management systems for major OS and carried out a vulnerability scan regularly. We will discuss details in the workshop.

13

Control System Cyber-Security in Industry

HEP is not that particular with respect to control system cyber-security. Many standards have been already developed in Industry and by governmental agencies.

This presentation will give a short summary of the efforts going on outside HEP.

14

Accelerator Control-System Network Security at Diamond Light Source

Author: Mike Leech[1]

[1] *Diamond Light Source*

Diamond is a new third-generation light source, which has only recently been completed near Oxford in the UK. As a new facility, it was possible to implement an 'isolated' accelerator control system network right from the start of operation. Of course, isolating the network leads to inevitable usability issues. This presentation will give an overview of Diamonds control network, the trade-offs between security and usability that have been made and plans for improving security in the future.

15

Security Experiences in SLAC Controls

Author: Terri Lahey[1]

[1] *SLAC*

The security implemented by each laboratory program and department is important to the laboratory as a whole, and to the health of each program. SLAC Controls team members work with central IT experts in security, networks, Oracle, Windows and UNIX, enhancing our ability to deliver secure control systems that meet project requirements. This talk presents some solutions and experiences at SLAC, including the need to design a

secure architecture, servers, procedures, and to revise them throughout the project.