SUMMARY OF THE CONTROL SYSTEM CYBER-SECURITY (CS)^2/HEP WORKSHOP

S. Lüders*, CERN, Geneva, Switzerland

Abstract

Over the last few years modern accelerator and experiment control systems have increasingly been based on commercial-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 [1]. The (CS)^2/HEP workshop [2] held the weekend before ICALEPCS2007 was intended to present, share, and discuss countermeasures deployed in HEP laboratories in order to secure control systems. This presentation will give a summary of the solutions planned, deployed and the experience gained.

INTRODUCTION

The enormous growth of the worldwide interconnectivity of computing devices (the "Internet") during the last decade offers computer users new means to share and distribute information and data. In industry, this results in an adoption of modern Information Technologies (IT) to their plants and, subsequently, in an increasing integration of the production facilities, i.e. their process control and automation systems, and the data warehouses. Thus, information from the factory floor is now directly available at the management level ("From Shop-Floor to Top-Floor") and can be manipulated from there.

However, with a thorough inter-connection of business and controls network, the risk of suffering from a security breach in distributed process control and automation systems# increases.

This risk can be expressed as in the following formula:

$$Risk = Threat \times Vulnerability \times Consequence$$

The different factors are explained in the following.

Threats

This interconnected world is by far more hostile than a local private controls network. The number of potential "threats" increases as worms and viruses can now easily propagate to control systems and attackers start to become interested in control systems too. Additional threats can be operators or engineers who download configuration data to the wrong device, or broken controls devices that flood the controls network and, thus, bring it to a halt.

The major part of the factor "threat" originates from outside and cannot be significantly reduced. Thus, protective measures have to be implemented to prevent external threats penetrating control systems. These protective measures should also prevent insiders from (deliberate or accidental) unauthorized access.

Vulnerabilities

The adoption of standard modern IT in control systems also exposes their inherent vulnerabilities to the world. Programmable Logic Controllers (PLCs) and other controls devices (even valves or temperature sensors) are nowadays directly connected to Ethernet, but often completely lack security protections [1]. Control PCs are based on Linux and Microsoft Windows operating systems, where the latter is not designed for control systems but for office usage. Even worse, control PCs can not be patched that easily, as this has to be scheduled beforehand. In addition, controls applications may either not be compliant with a particular patch or software licenses to run controls applications may become invalid. Finally, using emailing or web servers has become normal on control systems today; even web cameras and laptops can now be part of them.

The "vulnerability" factor can either be minimized by guaranteeing a prompt fix of published or known vulnerabilities, and/or by adding pro-active measures to secure the unknown, potential or not-fixable vulnerabilities.

Consequences

Within the High-Energy Physics (HEP) community, control systems are used for the operation of the large and complex accelerators and beam lines, the attached experiments, as well as for the technical infrastructure (e.g. power & electricity, cooling & ventilation). All are running a wide variety of control systems, some of them complex, some of them dealing with personnel safety, some of them controlling or protecting very expensive or irreplaceable equipment.

Thus, the consequences from suffering a security incident are inherent to the design of e.g. accelerators or experiments. These assets and their proper operation are

* With contributions from P. Chochula (ALICE), S. Gysin (FNAL), T. Lahey (SLAC), M. Leech (Diamond), T. Ohata (JASRI/SPring-8), D. Quock (ANL), A. Yamashita (SPring-8), Z. Yin (BNL), and T. Zingelman (FNAL).

# Commonly denoted in the following as "control systems", where a "system expert" has the expertise in its configuration.

at stake. A security incident can lead to loss of beam time and physics data, or — even worse — damage to, or destruction of, unique equipment and hardware.

Control System Cyber-Security in HEP

In order to cope with the growing usage of standard IT technologies in control systems, several HEP laboratories worldwide have reviewed their operation principles by taking the aspect of security into account. This paper will give a summary on the Control System Cyber-Security $(CS)^2$/HEP workshop held a day before this year's ICALEPCS [2].

CYBER SECURITY MEASURES AT APS

ANL's D. Quock has presented the "Control System Cyber Security Measures" at the Advanced Photon Source (APS) [3].

Large accelerator facilities such as the APS typically are operated by a diverse set of integrated control systems. The APS control system comprises 80 workstations, about 300 distributed I/O controller (IOCs), 96 PLCs, an assortment of LabView and FPGA controllers, more than 30000 replaceable components, and nearly 700 unique control system software applications. Examples of the variety of controls software used at APS include EPICS, PLC ladder logic, Verilog and VHDL FPGA design diagrams, MySQL relational database, and web programming languages. Other labs operate an equivalent variety of hardware and software.

This layered control system structure comes with inherent cyber security risks, and necessitated a comprehensive and up-to-date cyber security implementation. The ANL bases its counter-measures on a "Defense-in-Depth" approach.

Network segregation and firewalls protect at different at the boundaries between ANL and APS networks as well as to the Internet. Remote access to APS control systems is restricted using Virtual Private Networks (VPNs) and Secure Shell (SSH). So-called "portal servers" allow for file transfer and emailing. Control PCs and control equipment like IOCs or PLCs are put under a rigorous configuration management.

Special emphasis has been put on securing web-based control applications. Today, web technologies are getting more and more the focus of attacks using e.g. session hijacking, cross-site scripting, remote file inclusion, or SQL injection. For protection, Secure Socket Layer (SSL) encryption and procedures for using programming languages like PHP, JavaScript, XML, and MySQL have been applied. Lightweight Directory Access Protocol (LDAP) is currently used for user authentication, while Single Sign-On (SSO) is being considered for the future.

NETWORK SECURITY AT DIAMOND

Diamond is a new third-generation light source, which has only recently been completed near Oxford in the UK. As a new facility, M. Leech (Diamond) reported, it was possible to implement an "isolated" accelerator control system network right from the start of operation.

This accelerator network contains all the corresponding EPICS control traffic and all services required to run the accelerator like NFS, FTP for IOC booting, NTP etc. Dedicated routers control the traffic to Diamond's office and beamline networks. A secondary network similar to the primary one hosts other devices, such as video cameras or printers. Both primary and secondary network are under tight access control.

Some servers are dual-homed (i.e. connected to the primary and secondary networks like EPICS gateways, boot server, or SSH Bastion hosts) in order to allow access to services from other Diamond networks. Dual-homed control room workstations disallow incoming connections by firewall rule.

The traffic from the secondary network is routed via a dedicated firewall to other Diamond networks. In order to provide certain internal web pages to external network (with respect to the accelerator network), reverse Apache web proxies have been deployed.

BALANCED SECURITY AT FNAL

The balance between security and usability in the Fermilab accelerator control systems has been presented by T. Zingelman (FNAL)

FNAL has implemented several layers of protection both at the network and at the host level. The network protections include a physical disconnect point, which, in emergency situations, could isolate the entire Accelerator Division network from the rest of the world. The second layer of protection is Access Control Lists (ACLs) in the border routers for the Accelerator Division, which can be quickly changed if needed to block more specific or well understood threats. Redundant PIX firewall devices separate physically the controls network from the rest of the world. These firewalls are setup to deny inbound *and* outbound traffic. Router-based ACLs allow for isolating various dedicated purpose VLANs (virtual LANs).

At the host level, PCs running Windows or Linux are attached to centralized patching and anti-virus systems (the latter only for Windows). Other operating systems such as FreeBSD and Solaris are managed by "professional" system administrators. Embedded systems typically have no permanent storage and depend on servers hosting their boot images.

For remote access, FNAL has implemented a range of methods allowing authenticated users to work on systems in the controls network. VPNs allow PC and MAC users with a controls specific key and a separate username / password login to join their control system. Additional login credentials are required to connect to start e.g. a control system console. UNIX-based Bastion hosts can be used from inside nodes to get out as well as from outside nodes to get in. Logins require Kerberos authentication (or crypto-card hardware tokens) and are time limited. Additional Windows Terminal Servers (WTS) inside the controls network allow viewing embedded web-servers on devices such as scopes and signal analyzers or give local users (such as those in the control room) the possibility to read their email and visit off-site websites.

SECURITY PRACTICES AT SLAC

As T. Lahey explained security at SLAC is inherent to control system design and implementation as well as day to day operations. All aspects are regularly reviewed, and SLAC's controls and IT experts work together on security, networks, data bases, operating systems, web and application servers, and other IT technologies.

The SLAC controls architecture uses an isolated network, with few computers at the "edge" that provide access to control system data and the first hop for authorized users. This network can be physically disconnected from the campus network. All network nodes must be registered with fixed IP addresses. Wireless communication is routed via a separate network. Dedicated laptops for accelerator operation are managed from a controlled pool.

Automated patching and scanning of control PCs is performed regularly during accelerator downtimes.

Additional, T. Lahey mentioned SLAC's efforts to migrate to a central user credential management using strong authentication.

"DEFENSE-IN-DEPTH" AT CERN

CERN has currently reviewed its Security Policy for Controls. Its thorough implementation ("CNIC" — Computing and Network Infrastructure for Controls) also is based on a "Defense-in-Depth" approach [4], which covers four major pillars: "Network Security", "Central Installation Schemes", "Authorization & Authentication", and "User Training". Additionally, the Security Policy also defines rules to deal with "Incident Reporting & Recovery", as well as with regular security audits.

In order to contain and control its network traffic, the CERN network has been separated into defined "Network Domains", with "Domain Administrators" taking full responsibility and who supervise the stringent rules for connecting devices to it. The traffic crossing any two Domains is restricted to a minimum by the usage of routing tables, with only mandatory traffic passing such boundaries. Visibility of the Internet is blocked by rule. Remote access (e.g. from the office, from home, or from laptops) is exclusively possible via dedicated WTS clusters or SSH gateways using CERN credentials.

"Central Installation Schemes" for Linux and Windows PCs have been developed, which allow a system expert to take over full flexibility of the configuration of the PCs of his system, and full responsibility for securing it. The operating systems, patches, antivirus software, and basic software applications themselves continue to be managed and maintained by the IT service providers. It is up to the system expert to apply those in a timely manner. Finally, such schemes also help the expert to recover from a security incident.

Several dedicated authentication & authorization schemes have been developed at CERN and two are explained next.

RBAC for the Large Hadron Collider

The LHC is using Role Based Access Control (RBAC) for its control systems as presented by S. Gysin (FNAL).

An accident in the LHC has the potential to be extremely dangerous; it could be devastating to instruments and detectors. Therefore, CERN has developed multiple safety mechanisms, and hardware and software interlocks.

The RBAC implementation [5] is explicitly focused to protect device properties, but not general resources such as processes or PCs. RBAC assigns people to roles ("authentication") and gives these roles permissions ("authorization"). One advantage of this is that RBAC is preventative rather reactive. Authentication is done via CERN's Windows ("NICE") web interface based on SOAP (Simple Object Access Protocol) or with X.509 certificates. Authorization is done by extracting the permissions from the RBAC database and loading the applicable set into the front-end devices being accessed. The user logs in with his NICE credentials and receives a digitally signed RBAC token. The token is passed to the device via the Controls Middleware (CMW). Subsequently the CMW of the front-end device verifies the token signature and the expiration data, and finally checks an "Access Map" to match the roles in the token to the corresponding permissions.

RBAC was developed in collaboration with LAFS, a FNAL project that contributes controls software to the LHC. It was deployed in June 2007 and has been in operation since.

Local and Remote Access Control at ALICE

P. Chochula (CERN) presented how the ALICE experiment controls local and remote user access [6]. Their Detector Control System (DCS) operates about 1000 network devices, including PCs, power supplies, PLCs, front-end cards, and single-board computers.

The DCS is structured into 20 main systems, which cover the detectors and services. The corresponding DCS network is based on CNIC recommendations, and is not directly accessible from external networks. Each system is controlled by several "Worker Nodes", which execute the control tasks. One additional node for each system, called "Operator Node", is setup to run the user interface. These Operator Nodes are based on the WTS.

The ALICE authentication scheme is based on central credentials. Actions granted to standard users are limited to starting the user interface of their DCS. Experts are in addition able to log into Worker Nodes, copy data and modify the software settings. The authorization is deployed per detector and is technically implemented through Active Directory security groups. Advanced privileges, such as rights to operate the detector or to access the Worker Nodes are possible only from dedicated gateways. These require authentication based on SmartCards storing the user's certificate.

The main operation tool of the DCS is a commercial SCADA system called PVSS from ETM. All users must additionally authenticate to PVSS, reusing their Windows ("NICE") credentials. This allows for separation of potentially dangerous actions (such as detector operation or modification of operational and alert limits) from standard monitoring tasks.

Remote access is granted via application gateways which use the same setup as the Operator Nodes. Users must first establish connection to this gateway and are then authorized to access the internal network devices.

SECURE NETWORKS AT SPRING-8

T. Ohata (JASRI/SPring-8) gave his perspective on secure networks for control systems at SPring-8 [7]. SPring-8, a third-generation open user facility for synchrotron radiation, accepts many experiment users coming from external institutes. Since these users construct their own control system at each beamline, they require a fast, stable, and secure network environment to perform their experiments.

Initially, a firewall system has been deployed to protect the SPring-8 network from outer intrusion. Since risks cannot be avoided by only one single method, SPring-8 has adopted several additional means to achieve a secure network environment:

Network segregation has been the most important, and nowadays the range and the scale of networking problems in cases of incidents are controlled by firewalls and VLANs. Incidents are, thus, prevented from spreading. Therefore, the facility as a whole and other experiments in particular are protected and can continue operation. Furthermore, an Intrusion Protection System (IPS) has been installed. Traditional SNMP (Simple Network Management Protocol) network traffic monitoring system and newer sFlow analyzer allow for real-time analysis and restoration from problems of the network infrastructure.

In addition, patch management systems for major operating systems have been produced, and regular vulnerability scans are carried out.

Wide Area Remote Control

The "Wide Area Remote Control for SPring-8" (WARCS) has been presented by A. Yamashita (SPring-8). WARCS is a system which allows experts to access the accelerator's control PCs from the outside of the SPring-8 campus. The network for the SPring-8 accelerator control systems is strictly shielded by firewalls from the Internet. When an accelerator expert gets a phone call from the operation crew, he should access the control PCs by "making a tunnel" in the firewall using the WARCS system. However, A. Yamashita reported that out of several tunneling tools available on the market, none met their requirements.

Therefore, SPring-8 has build its own tool, WARCS, to satisfy their needs using a combination of the Linux firewall (IPTABLES), the secure IP tunnel program "Zebedee", Apache's HTTP server, the SQLite database program, and PYTHON glue scripts. Client programs for different operating systems (Windows, Macintosh and Linux) have been produced.

WARCS has been deployed at the beginning of 2004 and was successfully operated since then.

SECURE REMOTE OPERATION AT NSLS

As with SPring-8, remote operation compatibilities for users of National Synchrotron Light Source (NSLS) beamlines at the BNL are desirable. As in many of the synchrotron light source facilities, Linux workstations running X-Windows are employed for controlling the beamline optics and the experimental end stations.

Remote X displays, however, are over longer distances too slow; network latency and the large round trip time for X-traffic make the remote display unresponsive. On the other hand, cyber-security requirements at BNL demand for usage of VPN or SSH for remote access.

Z. Yin (BNL) discussed a solution that employs the open source FreeNX technology [8]. Their setup involved a FreeNX server configured on a Linux workstation at BNL, and free downloadable clients from NoMachine.com (Windows, Mac, and Linux) for remote users to connect to these FreeNX servers. All traffic is tunnelled through SSL, and special keys can be used to improve security further.

With the efficient compression of the NX technology and using proxy-server/cache files to minimize the round trip traffic, the bandwidth usage is finally quite small and response times over long distances have been very good. Thus, this resulted in a very responsive remote display (remote desktop), such that operations from outside BNL are now routinely performed by quite a number of scientists from their home institutions.

A VIEW FROM INDUSTRY

"The HEP community is not alone" has been the message of CERN's S. Lüders, since control systems in HEP are using more-or-less the same commercial-of-the-shelf hardware, software, protocols and methods as industry does. Even the impact and the consequences of a security breach in HEP can be as severe as in industry.

Therefore, Industry and governmental authorities, driven by the fear of terrorism after 9/11, have begun to review the consequences of a security incident on the so-called "Critical Infrastructure", i.e. those industrial sectors on which everyday living strongly depends — sectors like electricity providers, oil & gas companies, water & waste plants, chemical & pharmaceutical factories, and the transport sector. The demand for "Critical Infrastructure Protection" has led to a consolidation of world-wide efforts with respect to "Control System Cyber-Security" $(CS)^2$ and produced a substantial number of initiatives, standards & guidelines, and regulations.

Unfortunately, several incidents in industry have recently proven that the risks coming from security breaches are not fiction anymore, and the resulting consequences can be severe [9].

In order to mitigate those incidents and the risks presented above, both industry associations and governmental organizations have produced a high number of standards. The ISA SP99 "Manufacturing and Control Systems Security" is of exceptional importance. Less complex and much more pragmatic have been the "Good Practices" recommendations of the U.K. CPNI [10].

In order to follow-up the findings of its vulnerability test stand [1], CERN has raised (the lack of) Control System Cyber Security at several conferences and workshops, and interacted with major vendors of control systems. Their reaction was not really encouraging ("There is no market demand"), but the trend is going in the right direction. The "Procurement Language" document of the U.S. Idaho National Laboratory [11] might be able to change this, if users in industry demand security of control systems in their call for tenders.

Finally, S. Lüders has given an overview on the activities of the major players in this field: The Process Control Systems Forum is aiming to "accelerate the design, development, and deployment of more secure control and legacy systems." Private companies like Wurldtech or Digitalbond perform sophisticated vulnerability tests (incl. certification) and provide tools for intrusion detection systems. Future conferences and existing discussion groups like the European Information Exchange on SCADA Security ("EuroSCSIE") invite the HEP community to join — HEP is not alone.

SUMMARY

Due to the continuing integration of common IT technology into control systems, the corresponding IT security vulnerabilities and cyber-attackers end up threatening control systems, and, thus, HEP facilities' operation and assets. However, control systems demand a different approach to security than office systems do.

Several physics laboratories worldwide have presented their implementations on the Control System Cyber-Security (CS)^2 workshop at the ICALPECS 2007. The common baseline follows a "Defense-in-Depth" approach focussing on network protection and segregation, authorization & authentication, centralized PC installation schemes, and collaboration of IT and controls experts.

Perimeter protections through firewalls and strict network segregation in order to shield control networks from others have been implemented in all labs. This also enables decoupling a control network from the rest of the lab (i.e. world) in emergency cases. Furthermore, at light sources, additional segregation lead to a separation between the accelerator control network and the dedicated networks for beamline users. Special measures have been put in place for data exchange and allowing experts and users for remote access, e.g. using VPNs, VNC, WTS, or remote X terminals though SSH tunnels.

Centralized authentication and authorization schemes for operating systems and SCADA application as well as for front-end devices have become very important, and access control schemes have been deployed at several labs. However, these implementations have also revealed the inherent complexity of access control.

Central PC installation and patch management schemes have proven to be necessary for increasing security.

All these solutions do and will further benefit from corporation between IT and controls experts as well as from initiatives in industry and by governmental bodies.

ACKNOWLEDGEMENTS

The author would like to thank all the presenters and participants of the (CS)^2/HEP workshop as well as the ICALEPCS local organization committee for making this workshop such a success.

REFERENCES

[1] S. Lüders, "Control Systems Under Attack ?", ICALEPCS, Geneva, October 2005.

[2] Control System Cyber-Security CS2/HEP Workshop, http://indico.cern.ch/conferenceDisplay.py?confId=13367

[3] K. Sidorowicz and W. McDowell, "Information Technology Security at the Advanced Photon Source", these proceedings.

[4] S. Lüders, "Update on the CERN Computing and Networking Infrastructure for Controls (CNIC)", these proceedings.

[5] S. Gysin et al., "Role-Based Access Control for the Accelerator Control System at CERN"; K. Kostro et al., "Role-Based Authorization in Equipment Access at CERN"; and A. Petrov et al., "User Authentication for Role-Based Access Control", these proceedings.

[6] P. Chochula, "Cyber Security in ALICE", these proceedings.

[7] M. Ishii et al., "Construction and Management of a Secure Network in SPring-8", ICALEPCS, Geneva, October 2005.

[8] Z. Yin and P. Siddons, "Secure Remote Operation of Light Source Beamline Controls with FreeNX", these proceedings.

[9] The Register, 2000, http://www.theregister.co.uk/2000/04/27russia_welcomes_hack_attacks; Computer Crime Research Centre, 2005, http://www.crime-research.org/analytics/1718; CSO online, 2005, http://www2.csoonline.com/exclusives/column.html?CID=32893; eWeek.com, 2005, http://www.eweek.com/article2/0,1759,1849914,00.asp; SANDIA Labs, "Penetration Testing of Industrial Control Systems", SAND2005-2846P, 2005; Security Focus, 2005, http://www.securityfocus.com/news/6767 and 11465.

[10] Centre for the Protection of the National Infrastructure (CPNI), "Good Practice Guidelines Parts 1-7", London, 2006.

[11] G. Finco et al., "Cyber Security Procurement Language for Control Systems", Idaho National Labs, 2007, http://www.msisac.org/scada.