SUMMARY OF THE 3RD CONTROL SYSTEM CYBER-SECURITY (CS)2/HEP WORKSHOP

S. Lüders*, CERN, Geneva, Switzerland

Abstract

Over the last decade modern accelerator and experiment control systems have increasingly been based on commercial-off-the-shelf products (VME crates, programmable logic controllers (PLCs), supervisory control and data acquisition (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. The Stuxnet worm of 2010 against a particular Siemens PLC is a unique example for a sophisticated attack against control systems [1].

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 being altered [2].

The 3rd (CS)2/HEP workshop [3] held the weekend before the ICALEPCS2011 conference was intended to raise awareness; exchange good practices, ideas, and implementations; discuss what works & what not as well as their pros & cons; report on security events, lessons learned & successes; and update on progresses made at HEP laboratories around the world in order to secure control systems. This presentation will give a summary of the solutions planned, deployed and the experience gained.

THE FACT OF ATTACK

2010 has seen wide news coverage of a new kind of computer attack, named "Stuxnet", targeting control systems. Due to its level of sophistication, it is widely acknowledged that this attack marks the very first case of a cyber-war of one country against the industrial infrastructure of another, although there is still much speculation about the details. Worse yet, experts recognize that Stuxnet might just be the beginning and that similar attacks, eventually with much less sophistication, but with much more collateral damage, can be expected in the years to come. Stuxnet targeted a special model of the Siemens 400 PLC series. Similar modules are also deployed throughout the world for accelerator controls like cryogenics or vacuum systems as well as the detector control systems in high energy physics (HEP) experiments.

As with Stuxnet's infection vector, several HEP laboratories reported virus attacks through USB sticks. In one case, the insertion of an infected stick bypassed all firewall protection and network segregation measures put in place to secure the corresponding control system network. As those measures were perceived being sufficient, the affected PC did not run any anti-virus software, which would elsewise have easily quarantined that more than 5-year old virus. However, when trying to establish an IRC connection "home", the virus was quickly identified in the control system firewall logs. Nevertheless, it managed to infect two more control PCs before being fully contained.

In September 2009, one site reported the successful attack against a web server used to display controls information to members of the corresponding experiment's collaboration. For that purpose, all control data was replicated onto a publicly visible web server. However, due to negligence, that web server was neither properly updated nor was the web application properly secured: In a first step, the attacker managed to discover a file injection vulnerability which has subsequently been misused to create a remote shell. A vulnerability in the unpatched kernel subsequently gave the attacker full root access. Its prompt detection avoided further damage.

A similar event was detected at an other U.S. site in spring 2011. After having compromised two Internet facing webservers one month earlier, the attacker escalated privileges right in time for the July 4th holiday week-end. Also here, timely attack detection prevented further misuse.

In April 2011, an email phishing attack hit Oak Ridge National Laboratory (ORNL) in the U.S. Of the approximately 500 recipients of the email about 10% clicked on an embedded link designed to install malware. In one case the user had sufficient privilege that was leveraged to install malware on a large number of additional systems at the laboratory. ORNL chose to sever its connection to the Internet, including blocking web access and external email, to prevent data exfiltration. The clean-up and recovery took two weeks before normal functionality was restored.

The ORNL SNS accelerator controls network was designed to be well isolated from the rest of the ORNL network. Consequently the SNS accelerator was able to remain fully operational during this incident.

The European Organization for Nuclear Research (CERN) was luckier in July 2011 where a researcher on SCADA security found a password of one of CERN's control system. This password was listed in a document made unintentionally public. Before the researcher

* With contributions from E. Bonaccorsi (LHCb), P. Charrue (CERN), P. Chochula (ALICE), S. Hartman (ORNL), T. Hakulinen (CERN), T. McGuckin (JLab), T. Sugimoto (Spring8), F. Tilaro (CERN), V. Vuppala (NSCL/MSU).

published his findings on his personal blog later in August 2011, he informed the U.S. Department of Homeland Security who subsequently informed CERN. Even though this password just provided read access to limited information, it was immediately changed and the compromising document removed from that web-server (as well as from the cache of the Google search engine).

These few security events dismiss the illusion to believe HEP laboratories are not of interest for adversaries and not under attack. Even when all aforementioned security events have been promptly detected, properly analysed, and finally mitigated, acting in retrospect is a bad strategy. While probably not being a high-level target, security officers of HEPs should prepare counter-measures in order to prevent and protect security events from happing.

CHALLENGES IN CONTROL SYSTEM CYBER-SECURITY

However, control system cyber-security is not easy.

CERN's "Access, Safety and Engineering tools" (ASE) group, widely responsible for personnel access and safety systems at CERN, and the ALICE experiment at CERN have both reported about their challenges when implementing standard control system cyber-security measures.

CERN has set up a working group on the protection of control system [4]. Since then, all control systems at CERN must adhere to the "Computer and Network Infrastructure for Controls (CNIC) Security Policy for Controls" [5] following a "Defense-In-Depth" approach. However, over time, some of the access and safety systems have suffered from problems due to the CERN security policies. The most problematic and hardest to debug in the past have been due to the non-robustness of various off-the-shelf systems to periodic security scans. There have also been other problems due to incompatible security patches as well as expiration of service passwords. In the best case, these problems have been an annoyance to the access and safety team. In the worst case, they have prevented the accelerators from starting and personnel from accessing the controlled zones during the very tight maintenance windows.

The ALICE experiment at CERN is experiencing similar problems: Technical requirements and operational constraints [6][7] often directly collide with security measures. ALICE reported that the regular LHC technical stops (2-4 days) are insufficiently short to properly apply all pending security patches. In addition, the CPU consumption of anti-virus software is still one of the top-5 most resource demanding programs.

OVERCOMING THE CHALLENGE

In order to mitigate their problems, CERN ASE has suggested publishing security scan data, i.e., scan schedules, history, and results. This shall allow to correlate scans with the system monitoring data, system failures, and to help prepare for interventions and maintenance. In order to validate the robustness of network-connected devices, CERN's ASE group is considering the TRoIE test-bench, where equipment can be stress-tested and qualified in a controlled environment (see below). The TRoIE test procedure might also be used defining a conformity specification of CERN security measures. The associated requirements could be given to equipment and system vendors during the project definition phase. This document should be sufficiently authoritative and contractual to truly deliver the message to the vendors of the importance of hardening their equipment to the risks of today's computing environments.

Network Segregation, Compartmentalization and Border Control are Essential

The safe and stable operation of the ALICE experiment at CERN is assured by the Detector Control System (DCS), based on a commercial SCADA system PVSS II. The DCS is running on an isolated network, fully compliant with the CERN CNIC standards and rules. The interoperability with external systems is based on the network "exposure and trust" mechanism. DCS hosts can be made visible to external networks by exposing them; remote hosts can be trusted and become accessible from the DCS network. Using these mechanisms, the DCS can largely profit from CERN central computing infrastructure such as name resolution or domain services and reduce the local administrative overhead.

Data produced in ALICE DCS is exchanged with external systems in a secured way. A limited number of data publishers are trusted by the DCS network and central DCS clients can subscribe to the published data using CERN's DIM and DIP data exchange protocols. The DCS then distributes this information to its subsystems using the PVSS II. In the same way, DCS feedback is published to the trusted subscribers. All systems can in addition produce files, which are stored on internal fileservers and automatically mirrored to publicly accessible fileserver located on the CERN general purpose network. Upload of data to the network is subject to strict security policies and is performed by admins upon user's request.

A set of dedicated processes periodically collect condition parameters tagged by detectors for web display and converts them to images which are transferred to a public webserver. The image transfer is based on the concept of private and public fileservers, which assures a complete decoupling of the web services from the DCS infrastructure.

Individual detector control systems are made accessible to remote experts via application gateways, based on Windows Terminal Services. These servers are the only entry point to the system and are accessible only by using user's personal accounts. The use of shared accounts required for the operation is restricted only to the consoles installed in the control room.

The LHCb experiment at CERN pursues as similar road in protecting their control network from malicious remote

access. Operational independence and strong isolation from the Internet as well as from central CERN resources have been important design criteria. Depending on a strong perimeter protection, LHCb has deployed a three-tier redundant firewall providing screened subnets and demilitarized zones. A default deny policy has been implemented together with a set of rules based on the needs of the internal devices to be protected as well as statistical analysis of the boundary and internal network traffic. Each bastion host is hardened at the operating system level, reducing the number of installed applications to minimum. Each web server and reverse proxy has been configured to run as a different domain user and is serving pages from a read only shared network file system whose access is filtered both at OS and network layer. X.509 certificates have been issued by a recognized and "trusted" certification authority and have been installed on all web servers in order to protect the confidentially of sensible data such as usernames and passwords. The entire network traffic is also mirrored and analyzed in real time by an open source intrusion detection system based on Snort.

The Japanese SPring-8 facility serves 55 different beam-lines used by more than 10'000 users per year. The corresponding experimental user networks allow for controlling experimental instruments and data acquisition systems attached to these beam-lines. While SPring-8 has already compartmentalized their experimental user network into 55 segments, it is mandatory to have access to the Internet for data transfer as well as providing users with access to mail and web pages. However, this access is often misused by non-essential applications or inappropriate usage like bandwidth exhaustion by media streaming (YouTube, P2P file sharing), unauthorized instrumental control from outside via VPN, and so on. In particular the latter is prohibited as it collides with SPring-8's radiation safety regulations [8]. Moreover, due to web-browsing, several virus infections had already occurred on the experimental user network.

In order to prevent these threats from spreading to other control systems, SPring-8 had deployed the CheckPoint InterSpect610 intrusion protection system (IPS). While this IPS was suitable in the past, it lacked application signature coverage and was not able to block traffic tunneling via the HTTP web protocol. Hence, in 2010 it has been replaced by the so-called "Next Generation Firewall" from PaloAlto (PA-500 and PA-2050). This firewall can detect and block many (file sharing) applications and viruses including tunnelling protocols. Indeed, until today, this next generation firewall has successfully contained the spreading of 287 different P2P applications as well as 140 different types of viruses. Furthermore, their new firewall provides fundamental statistics for future service upgrades.

The earlier mentioned security event at one particular laboratory forced a full re-examination of their network structure and security. Priorities included isolating and firewalling critical subnets, a thorough segregation of the existing network infrastructure into functional domains, the deployment of application gateways between domains as well as stronger use of administrative and network monitoring tools. Remote access is now based on Virtual Private Networks requiring multifactor authentication (Crypto Cards or USB smart cards). All of these actions are being implemented as part of a more active model of accelerator controls network and system security.

A strong model of Defense-in-Depth is now pursued to produce a long-term solution that meets new requirements while minimizing the impact on-going work at the laboratory and allowing for a continuing cycle of monitoring, assessing and updating security.

DEFENSE-IN-DEPTH

The "Defense-In-Depth" approach requires that security measures have to be deployed on every level of the hardware and software stack, and not only at the network layer. Therefore, a more holistic view is necessary.

Top-Down vs. Bottom-Up

At CERN, the accelerator controls group has started creating a security inventory and risk assessment of the control system computers, devices, accounts and applications, with the goal

- to improve security and reliability of the accelerator control infrastructure;
- to identify the most critical security risks in its control systems; and
- to identify solutions to improve their security, including funding and implementation measures.

This inventory is supposed to summarize all risks using a list of security and reliability attributes like patching status, network configuration, installation base for applications, account usage, etc. While taking advantage of already existing data [9] (and their subsequent clean-up), a web-based "Questionnaire" enables system experts to quickly enter data for the remaining attributes.

The first version has been released to CERN's system experts, and the Questionnaire is currently being populated. In a second step, risk factors will be assigned to each of the attributes in order to determine the overall risk. As a side effect, some experts use this information now for accelerator failure-response and maintenance planning.

Compared to CERN's bottom-up approach, the U.S. National Superconducting Cyclotron Laboratory (NSCL) follows a top-down solution aiming for full compliance with the ISO 27000 standard [10] and final certification [11]. Essential for a successful compliance with ISO 27000 is the full support by management as well as support from all stakeholders involved.

Following this standard, NSCL implemented an Information Security Management System called "ARGUS", a framework of policies, procedures, guidelines and associated resources to achieve the security objectives of the organization. OCTAVE Allegro [12] has been chosen as the risk assessment methodology.

With those tools, the critical information assets, including controls and PLC software & configuration, system documentation, software licenses, etc. have been identified and assigned a relative risk score. This score is combined, categorized and prioritised. The resulting risk is finally mitigated following the controls from ISO 27002 or in-house developed controls. However, acceptance of low or residual risks is possible, too, if properly documented and approved by the management.

Robustness of Controls Devices

Particularly challenging for NSCL have been the hardening of control system platforms such as PLC devices where it was difficult to implement secure software development processes. Focus on such devices has been put on the robustness of industrial control system components by CERN's TRoIE test-bench. Unfortunately, there are no complete and comprehensive security standards yet, which can be followed to secure embedded devices; but several initiatives have been started with the objective of improving the security level and the robustness of industrial systems [13][14].

Therefore, CERN has developed a methodology for automated testing which evaluates the devices' ability to handle erroneous and malicious network traffic. This approach is based on the injection of malformed packets in order to corrupt the normal behaviour of the device and detect possible anomalies. As it is important to enumerate all possible faulty packets for each protocol, TRoIE uses fuzzing and syntax techniques, and lets the tester generating packet sequences in a systematic manner according to the definition of specific protocol syntactic and semantic rules. This technique is generic enough to be applied to any communication protocol, even to industrial ones that exhibit very specific properties and features.

TRoIE is currently under development and a wider publication is under discussion.

CONCLUSIONS

Stuxnet should have been the wake-up call for all those who never believed that control systems could and would be attacked. Indeed, HEP laboratories around the world have seen computer attacks against their facilities, even if these were not dedicated attacks against control systems, yet. However, this should not serve as an argument not to take any action. Continuing to ignore control system cyber-security is grossly negligent.

On the contrary, several HEP labs have started to or do repeatedly review the security protections put in place. Although sometimes cumbersome and difficult to achieve, deploying a "Defense-in-Depth" approach is mandatory and corresponds to good practise. NSCL even goes so far as to aim for full ISO 27000 compliance even on the control system level, a feat which is definitely both an ultimate goal, and a very difficult challenge.

In addition, there was broad consensus that control system cyber-security is more a people problem than a technical one. Establishing a "Security Culture" is needed where system experts, administrators, vendors, and operators cease perceiving "security" as burden but consider it to be an integral part of the system requirements on a par with functional, safety, and maintenance requirements. With such a change of mind-set, a big first step is taken for a better cyber-security of control systems. Subsequent technical steps would then be more easily understood and eventually accepted.

With Stuxnet, a new era has begun. Stay tuned.

REFERENCES

[1] S. Lüders, "Stuxnet and the Impact on Accelerator Control Systems", ICALEPCS, Grenoble, October 2011; these proceedings.

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

[3] 3rd Control System Cyber-Security CS2/HEP Workshop, http://indico.cern.ch/conferenceDisplay.py?confId=120418.

[4] U. Epting et al., "Computing and Network Infrastructure for Controls", ICALEPCS, Geneva, October 2005.

[5] S. Lüders et al., "CNIC Security Policy for Controls", 2011; https://edms.cern.ch/document/584092.

[6] P. Chochula et al., "Computing Architecture of the ALICE Detector Control System", ICALPECS, Grenoble, October 2011; these proceedings.

[7] A. Augustinus et al., "The Wonderland of Operating the ALICE Experiment", ICALPECS, Grenoble, October 2011; these proceedings.

[8] Y. Furukawa et al., "First Operation of the Wide-area Remote Experiment System", ICALPECS, Grenoble, October 2011; these proceedings.

[9] R. Billen et al., "Accelerator Data Foundation: How it All Fits Together", ICALEPCS, Kobe, October 2009.

[10] ISO/IEC, "Information technology — Security techniques — Information security management systems", ISO/IEC27000:2009, 2009.

[11] V. Vuppala et al., "Securing a Control System: Experiences from ISO 27001 Implementation", ICALPECS, Grenoble, October 2011; these proceedings.

[12] Computer Emergency Response Team (CERT) Program, Software Engineering Institute, "The OCTAVE Allegro Guidebook V1.0", Carnegie Mellon University.

[13] ISA SECURE Certification Program; http://www.isasecure.org/Certification-Program.aspx.

[14] Wurldtech Security Technologies Inc., "The Achilles certification"; http://www.wurldtech.com/cyber-security/achilles-certification.aspx.