8th Control System Cyber-Security Workshop (CS)2/HEP

Report of Contributions

https://indico.cern.ch/e/1270052

Contribution ID: **1** Type: **not specified**

The DC Nightmare

Sunday 8 October 2023 13:35 (35 minutes)

With the growing complexity of the IT hardware and software stack, with the prelevant usage of central computing resources for Internet-facing services, user services but also serving industrial control systems (OT), the design of data centre architectures and in particular networks becoming more and more challenging. This presentation will introduce the dilemma of creating a highly agile and flexible computer center set-up while still trying to maintain security perimeters within. It is bound to fail.

Author: LUEDERS, Stefan (CERN)

Presenter: LUEDERS, Stefan (CERN)

Contribution ID: **2** Type: **not specified**

Intro to the 8th CS2HEP

Sunday 8 October 2023 08:45 (15 minutes)

Contribution ID: **3** Type: **not specified**

How to fight Ransomware

Presenter: PLÖTZENEDER, Birgit (ELI)

Contribution ID: **5** Type: **not specified**

Mitigating Cyber-Threats in remote work: Implementing enhanced measures post-ransomware attack

Sunday 8 October 2023 09:00 (30 minutes)

The global shift to remote work during the COVID-19 pandemic significantly widened our cyber threat landscape, leaving many organisations exposed. A notable case was the successful breach of ESS corporate network by a recognised ransomware group that executed credential stuffing attack. During the 8th Control System Cyber-Security workshop we plan to examine this incident, focusing on the lessons that followed.
We'll delve into the implementation of protective strategies, such as multi-factor authentication (MFA) and Identity and Access Management (IAM), as well as the network segmentation through the security zones and we will also present the use of Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA) solutions for secure application access.

Author: MUDINGAY, Remy (European Spallation Source ERIC)

Co-authors: Mr FORSAT, Amir (European Spallation Source); Mr ARMANET, Stephane (European Spallation Source)

Presenter: MUDINGAY, Remy (European Spallation Source ERIC)

Contribution ID: **7** Type: **not specified**

Cybersecurity risks of SBOM (or git) with automation

Sunday 8 October 2023 14:10 (30 minutes)

Many distributed version control platforms utilizing open-source worldwide collaboration, such as GitLab and GitHub, have built-in mechanisms allowing for robust version-control and smooth automation via e.g. pipelines. At some large-scale research facilities, some also trigger automatic deployments of the latest version of the software to clients otherwise isolated on private networks – creating an undesired interface between the public realm and the systems on the private networks. The risk is hence non-zero that a malicious attack could occur to a git repository which introduces malware or functionality changes, with a successful such automatically deploying the malicious changes to the clients defined in its pipeline.

Therefore, there is a need in the field to start discussing and doing risk assessments for scenarios built on this as a baseline, starting with a simple set of questions:

- How safe are these type of git workflows?
- What protection measures could be taken?
- Has this or similar happened before, and if so, in what scale and what lessons learned has come from this?

Author: BOLLING, Benjamin (European Spallation Source ERIC)

Presenter: BOLLING, Benjamin (European Spallation Source ERIC)

Contribution ID: **8** Type: **not specified**

Software Bill of Material Deep Dive

Sunday 8 October 2023 14:40 (30 minutes)

Supply chain attacks have surged since 2013, offering attackers an easy and lucrative method to breach vital organizational functions. In the past four years alone, notable supply chain attacks have grown fourfold. This trend is predicted to persist unless effective countermeasures are embraced. In the realm of open science, the heavy dependence on open-source code for scientific software development, coupled with diverse technology use in extensive deployments, presents challenges for asset owners to evaluate and eliminate potential vulnerabilities.

New regulations from the US government (White House executive order EO14028) and the EU commission (E.U. Cyber Resilience Act) now require Service and Equipment suppliers involved in government contracts to publish SBOMs for their commercial products. These SBOMs must adhere to a standardized and openly accessible data format, and support automated identification of existing or potential vulnerabilities, along with strategies for effective mitigation.

This presentation will focus on open-source tools and workflows that leverage SBOM standards and help the CERN Accelerator and Technology Sector inventory and manage vulnerabilites across the multiple platforms and programming languages it employs for its operational software.

Author: COPY, Brice (CERN)

Presenter: COPY, Brice (CERN)

Contribution ID: **9** Type: **not specified**

Upcoming CERN Accelerator-IT Governance

Sunday 8 October 2023 10:20 (1 hour)

A new CERN IT governance model was put in place in 2021 between the CERN IT department and the Accelerator and Technology Sector (ATS) in view of preparing the Accelerator control system infrastructure for the LHC high luminosity era. Flagship projects such as the adoption of containerization technology and orchestrators or the review of the network isolation for Accelerator control offer unique opportunities to streamline our DevOps processes and to improve the overall security of our control system. This talk with present the motivation behind these initiatives and discuss the potential benefits we expect in terms of security.

Author: VANDEN EYNDEN, Marc (CERN)

Presenter: VANDEN EYNDEN, Marc (CERN)

Contribution ID: **10** Type: **not specified**

SLAC Initiatives in Accelerator Cyber Security

Sunday 8 October 2023 11:20 (40 minutes)

We describe a program at SLAC to truly understand accelerator cyber vulnerabilities as they exist at SLAC and similar facilities, improve accelerator cyber security generally, engage the U.S. Dept. of Energy in collaboration and funding, and provide the concomitant upgrades to EPICS Base for the accelerator community.

Author: Mr WHITE, Gregory R (SLAC)

Presenter: Mr WHITE, Gregory R (SLAC)

Contribution ID: **11** Type: **not specified**

Sanzu : A secure graphical remote access solution

Sunday 8 October 2023 09:30 (25 minutes)

Today more and more control systems are accessed and administered remotely. However many of the existing solutions are not satisfying because they are either unsecure, bad in term of performance or proprietary softwares. For example in 2019, Kasperky found 37 vulnerabilities in four different implementations of VNC.
That's why we created our own graphical remote access solution written in rust.
During the 8th Control System Cyber-Security Workshop, we plan to focus on presenting our open-source graphical remote access solution called Sanzu. We will focus on the two main usages of our tool:
Firstly we will talk about Sanzu as a secure replacement for existing remote access solutions like VNC. Then we will dive into the use of Sanzu to provide a remote web browser with the goal of mitigating attacks targeting web browsers on computers with access to critical infrastructures.

Author: FRINGANT, Antonin

Presenter: FRINGANT, Antonin

Contribution ID: **12** Type: **not specified**

CERN Computer Security Controls

Sunday 8 October 2023 15:30 (30 minutes)

Like any other organization, university or enterprise, CERN is permanently under attack. The risks — legally or financially, to CERN's operation or reputation — cannot be neglected.

The CERN Computer Security Team has been mandated to protect the operations and reputation of CERN against cyber-threats. In this presentation we will go through the different defense mechanisms — controls — the Team is providing in order to prevent, protect, detect and respond to any kind of abuse, attack or intrusion against CERN's computing facilities, devices, accounts, services & control systems in an agile, complex and heterogenous environment and while keeping a good balance between "academia", "operations" and "computer security".

Author: LUEDERS, Stefan (CERN)

Presenter: LUEDERS, Stefan (CERN)

Contribution ID: **13** Type: **not specified**

Epics Security Technical Plan

Sunday 8 October 2023 13:00 (35 minutes)

A presentation of the 2 years implementation plan primarily undertaken by Osprey DCS, SLAC and ORNL and funded by the US Department of Energy

The plan wll update PVXS (C++) and core-pva (Java, in CS-Studio/Phoebus) to support secure network connections based on the industry standard Transport Layer Security (TLS) technology. PVA clients that search for PV names will be able to indicate support for TLS authenticated and encrypted communications. PVA servers that support TLS will be able to accept such search requests and initiate the creation of a secure communication session. PVA servers that support secure connections will prefer TLS over regular unsecured connections. Server authentication will be accomplished by providing an X.509 certificate and optional client authentication will be achieved in the same way.

The updated pvAccess protocol will provide robust authorization in an end-to-end encrypted, fully authenticated, efficient and manageable framework for control systems access. The implementation is planned to be completely backward compatible, with secure and non-secure clients and servers interoperating seamlessly.

Author: Mr MCINTYRE, Georg (Level-N)

Presenter: Mr MCINTYRE, Georg (Level-N)