Contribution ID: **25** Type: **Talk**

Towards a more resilient and secure EPICS

Thursday 6 June 2019 14:50 (10 minutes)

The typical EPICS system consists of three major categories of hardware asset classes: the local area network (LAN), the operator interfaces (OPI), and the Input/Output Controllers (IOCs) where scientific data such as process variable (PV) values, limits and metadata reside. Most institutions'mission requires that the system be up and running over 95% of the time during service periods and without rebooting for several months. Therefore, any event that could cause service disruption represents a serious concern and must be prevented. However, the current protection measures for EPICS systems assets only consist of border security techniques which do not prevent a user with access from controlling the entire system once logged in.
Our work proposes to analyze the security challenges facing the EPICS systems. Specifically, we look at three threats models and their potential consequences to the system. First, we consider users who may gain inappropriate access to IOCs and accidentally disturb operations, compromise the integrity of data and/or the validity of scientific experiments. Next, we consider malicious users that launch untargeted attacks by installing self-propagating malware, starting with the first internet-facing hardware asset encountered. Such an event can also lead to a compromise of the IOC database. Finally, we look to study targeted attacks against the hardware assets aiming to disrupt activities at the institutions. These types of attacks are the most serious and costliest as they can lead to a sabotage of the software, damage to equipment, takeover of the entire system and/or launch of distributed denial of service (DDOS) by the adversary.
Our work intends to transform the EPICS software into a resilient, secure cyberinfrastructure that will immediately benefit the high-energy physics community. As such, we plan to integrate security throughout the EPICS software development life cycle using state of the art techniques for vulnerability discovery and for integrity protection of EPICS software products. Next, our work aims to improve and leverage the operating system security services. Common cryptographic libraries will be built for EPICS and memory protection will be enhanced by deploying advanced techniques used in general-purpose operating systems. Finally, we intend to focus on improving network security for EPICS protocols by formally modeling and analyzing EPICS PV gateway, improving security logging and designing a network Intrusion Detection System (IDS) for EPICS PV Gateway.

Authors: HOUNSINOU, Sena (Howard University); Dr BLOOM, Gedare (Howard University)

Presenter: HOUNSINOU, Sena (Howard University)

Session Classification: Core Developments

Track Classification: Core Developments