Contribution ID: **25** Type: **not specified**

Internet of Things on Accelerator Control Networks

Sunday, 8 October 2017 12:10 (25 minutes)

The European Organization for Particle Physics (CERN) faces today different types of hardware that gets integrated into the accelerator complex. While integrating Internet of Things (IoT) devices in mission-critical networks with industrial control systems, it puts their directly controlled assets at risk and possibly endanger the whole connected facility.
IoT devices introduce vulnerabilities, either by malicious intention or by wrong configuration. For this reason, we scan for IoT devices on CERN networks on a regular base. We detected unprotected ports for changing the configuration for printers or thermometers and several web-cams of the same model that are prone to remote code execution. Attackers can use remote code execution to gain access to the internal network from the outside and dig further while operating on a trustworthy device. Based on these findings, we suggest to run regular scans on any network to detect IoT devices and check their configurations properly.

Summary

Primary author: OSER, Pascal (Hochschule Karlsruhe, Technik und Wirtschaft (DE))

Presenter: OSER, Pascal (Hochschule Karlsruhe, Technik und Wirtschaft (DE))