[Keynote]: No-Trust-Zone Architecture for Securing Supervisory Control and Data Acquisition

Authors : Michael Okeke, Andrew Blyth

Abstract : Supervisory Control And Data Acquisition (SCADA) as the state of the art Industrial Control Systems (ICS) are used in many different critical infrastructures, from smart home to energy systems and from locomotives train system to planes. Security of SCADA systems is vital since many lives depend on it for daily activities and deviation from normal operation could be disastrous to the environment as well as lives. This paper describes how No-Trust-Zone (NTZ) architecture could be incorporated into SCADA Systems in order to reduce the chances of malicious intent. The architecture is made up of two distinctive parts which are; the field devices such as; sensors, PLCs pumps, and actuators. The second part of the architecture is designed following lambda architecture, which is made up of a detection algorithm based on Particle Swarm Optimization (PSO) and Hadoop framework for data processing and storage. Apache Spark will be a part of the lambda architecture for real-time analysis of packets for anomalies detection.