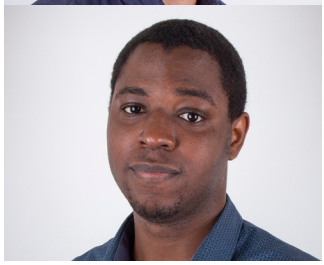
SHUBHAM DABRA

STUDENT, MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

RAPHAEL NAIYEJU

STUDENT, MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT



MEASURING EFFECTIVENESS OF DEEP PACKET INSPECTION TOOLS AND THEIR IMPACT ON LATENCY IN INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS (IACS)

Industrial Automation and Control System (IACS) is a collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes. Since most IACS environments still use legacy systems, soft targets can be found by the attackers with malicious intent. IACS environment uses protocols like Modbus, DNP3 and OPC. Modbus is in the scope of our research. Modbus protocol was not designed with security-in-mind. Therefore, many attacks can be performed in an IACS environment. In this research different Intrusion Detection Systems with Deep Packet Inspection capabilities are used. Deep Packet Inspection (DPI) is an advanced method of examining network traffic that focuses on payload and header of a packet rather than conventional packet filtering that only inspects payload of a packet.

Our research has the following objectives:

- Testing the IACS infrastructure on Modbus protocol with Metasploit Framework
- Testing the effectiveness of different Deep Packet Inspection (DPI) tools Snort, Suricata and Bro using Security Onion in IACS Environment.
- Extracting different signatures from the attacks performed using Metasploit Framework and using them in Snort.
- Measuring impact of Intrusion Detection Systems on availability of the IACS systems.

Research Advisors: Dr. Pavol Zavarsky, Prof. Ron Ruhl