RAPHAEL NAIYEJU

STUDENT, MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

SHUBHAM DABRA

STUDENT, MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

VULNERABILITY ASSESSMENT OF THE MODBUS INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS USING PENETRATION TESTING AND CISCO SECURITY AS THE BENCHMARK

The Modbus TCP/IP protocol is widely used in industrial automation and control systems (IACS), systems which handle the automation of various critical infrastructures such as electric, water, water-waste, transportation and oil and natural gas industries. Modbus is also being used as a communication protocol for some Internet of Things (IoT) devices. This protocol, however, lacks security properties and is vulnerable to attacks. Over the past few years there has been an increase in attacks on these systems and their protocols, such as the Stuxnet attack and, most recently, the Venezuela's power outage. This research aims to carry out a vulnerability assessment on the Modbus protocol using penetration testing tools. The assessment includes; (1) identification of the vulnerabilities, (2) impact and evaluation of the vulnerabilities, (3) selection of appropriate counter measures and (4) assessing the experimental results with benchmarks and comparing with the results of other researchers. The SMOD penetration testing tool and the Metasploit framework are used to identify vulnerabilities. Tools such as Wireshark and Ping Plotter will be used to measure their impact. One of the possible countermeasures is the use of deep packet inspection.

Research Advisors: Dr. Pavol Zavarsky, Dr. Dale Lindskog