Abstract

Supervisory Control and Data Acquisition (SCADA) systems were developed to assist in the management, control and monitor of critical infrastructure functions such as gas, water, waste, railway, electricity and traffic. In the past, these systems had little connectivity to the Internet because they ran on dedicated networks with proprietary control protocols and used hardware and software specific to the vendor. As a result, SCADA systems were secure, and did not face challenging vulnerabilities associated with the Internet. The need for remote connectedness, in order to collect and analyse data from remote locations, resulted in SCADA systems being increasingly getting connected to the Internet and corporate networks. Therefore, SCADA systems are no longer immune to cyber-attacks. There are reported cases on cyber-attacks targeted at SCADA systems. This research utilises penetration testing to investigate common SCADA security vulnerabilities. The investigation is conducted through experiments, under two different scenarios. Experiments were conducted using virtual plant environment. The results revealed vulnerabilities which are considered as common by the Idaho National Laboratory and others which are not common. Recommendations are provided on how to mitigate the vulnerabilities discovered in this research.