FRAMEWORK TO PROTECT THE INDUSTRIAL CONTROL SYSTEMS IN THE CRITICAL INFRASTRUCTURE

Madawalage Chathuranga Sineth

A dissertation submitted in partial fulfillment of the requirements for
MSc Cyber in Security and Forensics

Department of Computing

Informatics Institute of Technology, Sri Lanka
in collaboration with
University of Westminster, UK

2021

Abstract

Critical Infrastructure (CI) as defined according to this conducted research are the assets which are important to any country where failure, compromise or breach to the CIA concepts would have a major negative impact to the nations national security, economy, public health, safety and social well-being of people. It has been observed that the attacks against these CIs are increasing day by day. Cyber attackers specifically target this area because a successful attack on a single CI can result in loss to the critical or essential services that needs to be up in the country. At the moment, Sri Lanka has no proper guideline, framework or a procedure to secure the Industrial Control Systems (ICS) in the critical infrastructures therefore, this research is focused on establishing a framework to protect the ICS in the CI sector and identify the threats, vulnerabilities and countermeasures in those ICS. The primary data gathering methods that were used are questionnaires and interviews from the domain experts and industry professionals. To address the identified problem, a solution was introduced as a framework where the framework was developed as process based strategy. The framework consists of six main stages to check the applicability of the framework, to identify the ICS components, to conduct the vulnerability assessment, to classify the vulnerabilities according to the risk rating, manage the vulnerabilities, lastly ending with a reassessment to verify if all vulnerabilities are resolved. The targeted audience for the framework is organizations staff and top level management within the organization. To update this framework in the future, machine learning can be introduced to this research. Using machine learning, this framework can be automated. This research was conducted to protect all ICS in a more general way. Further research on this area can be done to deep dive into each and every ICS component in the CI sector.

Keywords: Critical Infrastructure, Industrial Control Systems, Operational Technology, Vulnerabilities, Threats, Risks, Countermeasures