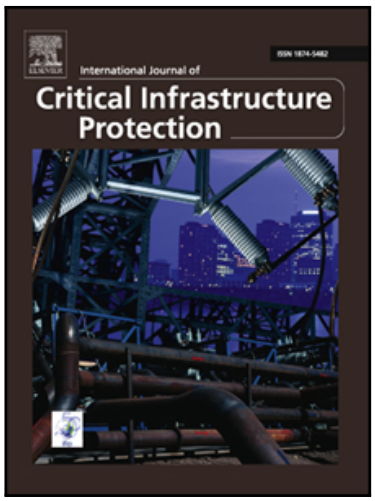

Extending the Cyber-Attack Landscape for SCADA-based Critical Infrastructure

Nicholas R. Rodofile, Kenneth Radke, Ernest Foo

PII: S1874-5482(17)30027-6
DOI: https://doi.org/10.1016/j.ijcip.2019.01.002
Reference: IJCIP 287

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 24 February 2017
Revised date: 1 December 2018
Accepted date: 27 January 2019

Please cite this article as: Nicholas R. Rodofile, Kenneth Radke, Ernest Foo, Extending the Cyber-Attack Landscape for SCADA-based Critical Infrastructure, *International Journal of Critical Infrastructure Protection* (2019), doi: https://doi.org/10.1016/j.ijcip.2019.01.002

Extending the Cyber-Attack Landscape for SCADA-based Critical Infrastructure

Nicholas R. Rodofile*, Kenneth Radke, Ernest Foo

Queensland University of Technology
Science and Engineering Faculty
School of Computer Science and Electrical Engineering
Information Security Discipline

Abstract

The move from point-to-point serial communication to traditional information technology (IT) networks has created new challenges in providing cyber-security for supervisory control and data acquisition (SCADA) systems in critical infrastructure. Current research on the attack landscape for critical infrastructure concentrates on either IT-based or protocol specific attacks. However, there is limited research focus on "the bigger picture", the combination of IT attacks and critical infrastructure protocol attacks, and little consideration of cyber-attacks targeting an entire SCADA-based critical infrastructure system. Due to such narrow research, there is a complete lack of focus when comprehending full-scale cyber attacks on SCADA-based critical infrastructure systems. As a result, new attacks combining various vulnerabilities in engineering systems and IT systems are yet to be discovered.

In this paper, we collated existing known attacks, identified and combined the existing range of attack landscapes, expanded and "filled the gaps" in the landscape, thus presenting a complete cyber-attack framework that perceives attacks against entire SCADA-based critical infrastructure. Our framework identifies four attack types, *traditional IT-based attacks, protocol specific attacks, configuration-based attacks* and *control process attacks*, allowing us to describe practical attacks. The benefit of recognizing the range of attacks on entire critical systems is that it allows us to defend against attacks with far greater efficiency and intelligence. To support the validity of our presented framework, we present a case study demonstrating a series of attacks on physical Distributed Network Protocol 3 (DNP3) critical infrastructure equipment.

Keywords: Cyber-attack framework, critical infrastructure attack, DNP3, SCADA security

*Corresponding author
Email addresses: n.rodofile@qut.edu.au (Nicholas R. Rodofile), k.radke@qut.edu.au (Kenneth Radke), e.foo@qut.edu.au (Ernest Foo)