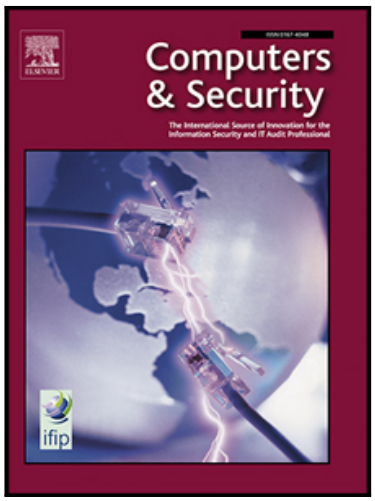
Accepted Manuscript




# Attack Detection / Prevention System Against Cyber Attack in Industrial Control Systems

Ercan Nurcan YILMAZ , Serkan GÖNEN

PII: S0167-4048(18)30331-6
DOI: 10.1016/j.cose.2018.04.004
Reference: COSE 1326

To appear in: *Computers & Security*

Received date: 7 January 2018
Revised date: 31 March 2018
Accepted date: 4 April 2018

Please cite this article as: Ercan Nurcan YILMAZ , Serkan GÖNEN , Attack Detection / Prevention System Against Cyber Attack in Industrial Control Systems, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.04.004

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

# Attack Detection / Prevention System Against Cyber Attack in Industrial Control Systems

Ercan Nurcan YILMAZ
Gazi University, Faculty of Technology, Electrical-Electronic Engineering
Ankara, Turkey
enyilmaz@gazi.edu.tr

Serkan GÖNEN
Gazi University, Graduate School of Natural and Applied Sciences, Information Security Engineering
Ankara, Turkey
serkangonen@gmail.com

***Abstract*: Industrial control systems (ICS) are vital for countries' industrial facilities and critical infrastructures. However, there are not enough security assessments against cyber attacks carried out on ICS for not preventing business continuity. New attacks are being made every day against these systems. Threats and attacks against critical infrastructures must be detected for protecting human life and assets. For this reason, detection has become more important than the prevention of attacks. In this study, vulnerability and attack detection analysis was carried out on programmable logic controllers (PLC), one of the most important components of ICS, in the testbed and a rule set was created to detect active start / stop attacks targeting. In this case, with writing this rule table, similar attacks will be prevented without harming the critical systems. In the analysis, mirroring technique was used to prevent the detection system from imposing additional load to the existing system and affecting the operation of the system negatively. In the test environment, Siemens S-7 1200 (Firmware 2.2) PLC devices were used. Smoothsec system, which is not used in industrial systems, is used for detection and rule table. It is assessed that this novel approach will provide significant contributions to attract attention to vulnerabilities and the security analysis of industrial control systems.**

***Keywords*: Start / Stop attack; vulnerability analysis; traffic analysis; industrial control systems; PLC security; intrusion detection, pattern.**

## I. INTRODUCTION

Industrial Control Systems (ICS) are used in the management and maintenance of critical infrastructures, which are usually geographically distributed, such as gas, water, production, transportation and power distribution systems. Industrial control systems consist of several subcomponents such as Programmable Logic Controller (PLC), Human Machine Interface (HMI), Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) [1]. In old generation Industrial Control Systems (ICS), these components used to communicate with private internal networks and specific protocols were used for these private networks. Therefore, ICS isolated from external networks were considered to be safe from cyber attacks and cyber security was substantially neglected. However, in order to control and monitor a geographically dispersed structure, an Internet or intranet connectivity was needed in the next generation systems [2-4]. In addition, the usage of COTS (Commercial off-the-shelf) and the development of hybrid integrated protocols such as ModBUS / TCP have made ICS more vulnerable to various cyber attacks [5, 6]. Along with the developing process, new vulnerabilities have emerged that cannot be detected beforehand [7].

Industrial control systems are responsible for controlling and monitoring many critical infrastructures. For this reason, detecting a security vulnerability in industrial control systems causes these systems to become potential targets of attackers. Seizing control of the system can cause the entire infrastructure to become paralyzed. This may result not only in economic damage, but also in the fact that citizens cannot receive important services in their lives [8]. Operation of more than 100 power plants stopped in the United States on August 14 2003. The cause of this disaster was a bug in communication systems and about 50 million people living in the US and Canada were affected by this disaster and 10 major airports and the New York metro could not serve properly. Another cyber attack on waste management facilities in Queensland, Australia, caused a large amount of waste to be discharged into public places. Numerous attacks occur on ICS, another one is the Stuxnet Worm, one of the most sophisticated computer worms thought to be targeted at the Iran Nuclear program and affected more than 100,000 computer systems, have also been reported [9].

The above-mentioned exemplary attack events emphasize the fact that ICS are highly vulnerable to attack. For this reason, industrial control systems have become one of the primary targets of cyber terrorism and cyber warfare. As a result, it is crucial to analyze in depth to reveal existing vulnerabilities of components (PLC, HMI, RTU, MTU,

Download English Version:

https://daneshyari.com/en/article/6883838

Download Persian Version:

https://daneshyari.com/article/6883838

Daneshyari.com