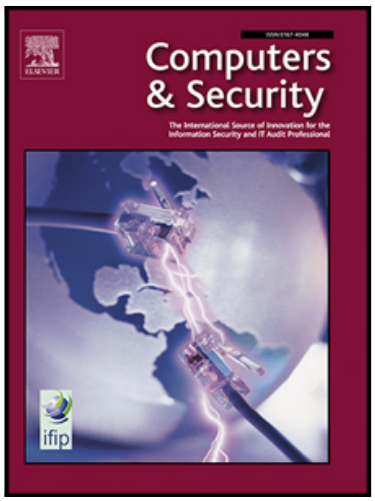

Anomaly Detection for Industrial Control Systems using Process Mining

David Myers, Suriadi Suriadi, Kenneth Radke, Ernest Foo

PII: S0167-4048(18)30679-5
DOI: 10.1016/j.cose.2018.06.002
Reference: COSE 1355

To appear in: *Computers & Security*

Received date: 25 September 2017
Revised date: 12 May 2018
Accepted date: 5 June 2018

Please cite this article as: David Myers, Suriadi Suriadi, Kenneth Radke, Ernest Foo, Anomaly Detection for Industrial Control Systems using Process Mining, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.06.002

Anomaly Detection for Industrial Control Systems using Process Mining

David Myers[a], Suriadi Suriadi[a], Kenneth Radke[a], Ernest Foo[a]

[a]*Queensland University of Technology (QUT), Australia*

Abstract

Industrial control systems (ICS) are moving from dedicated communications to switched and routed corporate networks, exposing them to the Internet and placing them at risk of cyber-attacks. Existing methods of detecting cyber-attacks, such as intrusion detection systems (IDSs), are commonly implemented in ICS and SCADA networks. However, these devices do not detect more complex threats that manifest themselves gradually over a period of time through a combination of unusual sequencing of activities, such as process-related attacks. During the normal operation of ICSs, ICS devices record device logs, capturing their industrial processes over time. These logs are a rich source of information that should be analysed in order to detect such process-related attacks.

In this paper, we present a novel process mining anomaly detection method for identifying anomalous behaviour and cyber-attacks using ICS data logs and the conformance checking analysis technique from the process mining discipline. A conformance checking analysis uses logs captured from production systems with a process model (which captures the expected behaviours of a system) to determine the extent to which real behaviours (captured in the logs) matches the expected behaviours (captured in the process model). The contributions of this paper include an experimentally derived recommendation for logging practices on ICS devices, for the purpose of process mining-based analysis; a formalised approach for pre-processing and transforming device logs from ICS systems into event logs suitable for process mining analysis; guidance on how to create a process model for ICSs and how to apply the created process model through a conformance checking analysis to identify anomalous behaviours. Our anomaly detection method has been successfully applied in detecting ICS cyber-attacks, which the widely used IDS Snort does not detect, using logs derived from industry standard ICS devices.

Keywords: ICS, SCADA, Critical Infrastructure, Security, Cyber Attack, Process Mining

1. Introduction

Industrial control systems (ICSs) include supervisory control and data acquisition (SCADA) systems. A typical ICS or SCADA network consists of devices such as programmable logic controllers (PLCs), which are controlled through the use of human-machine interfaces (HMIs) [1, 2]. In addition to PLCs and HMIs, ICS and SCADA networks can use remote terminal units (RTUs) to control devices such as sensors in the network, which are in turn operated by master terminal units (MTU) [2]. As SCADA networks can be spread over large geographical areas, SCADA devices are moving from dedicated communication equipment such as serial links to Ethernet based switched and routed networks, connected to corporate networks through specialised gateways [3]. This allows SCADA and ICS devices to be controlled through one central location and simplifies management of the devices [3]. However, connecting these SCADA devices to corporate networks potentially exposes them to the Internet, placing the devices at risk of cyber attacks.

There have been several cyber attacks on critical infrastructure, including ICS and SCADA networks [4]. ICS and SCADA networks typically have security measures implemented to detect these cyber attacks, most commonly by using intrusion detection systems (IDS). While real-time detection is the ultimate goal of IDS, a system which provides near real-time detection is still very useful. This is shown by the 290 reported ICS-CERT incidents in

Email addresses: d2.myers@qut.edu.au (David Myers), s.suriadi@qut.edu.au (Suriadi Suriadi), k.radke@qut.edu.au (Kenneth Radke), e.foo@qut.edu.au (Ernest Foo)