Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc.

Traffic Causality Graphs for Industrial Networks

Motivation

Industrial Control Systems are complex systems that manage physical processes [1]. They consist of sensors and actuators and are controlled via a network. To be able to analyze root causes to faults and errors, it is crucial to understand the dependencies of services in such networks. Therefore, there are several approaches to put network flows into context, e.g. Traffic Causality Graphs [2]. So far, these have been used in several works to analyze the causation of network flows in consumer networks [3][4].

Topic

The goal of this thesis is to explore the applicability of TCGs for industrial networks. Therefore, the differences between consumer and industrial networks need to be analyzed. Further, properties of TCGs should be identified. Based on these insights, TCGs should be implemented and used to analyze a traffic capture from an ICS testbed [5] The evaluation should then analyze the applicability of TCGs in industrial netwoks.

Your Task

- Analysis of TCGs
- Development and implementation of a TCG pipeline from data-set to graph
- Identification of TCG shortcomings
- Evaluate methodology on provided network captures

Requirements

- Basic network knowledge
- Ability to write maintainable code

Sources

- [1] Knapp, Eric D., and Joel Thomas Langill. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress, 2014.
- [2] Asai, Hirochika, Kensuke Fukuda, and Hiroshi Esaki. "Traffic causality graphs: profiling network applications through temporal and spatial causality of flows." 2011 23rd International Teletraffic Congress (ITC). IEEE, 2011.
- [3] Zhang, Hao, et al. "Visualizing traffic causality for analyzing network anomalies." Proceedings of the 2015 ACM International Workshop on International Workshop on Security and Privacy Analytics. 2015.
- [4] Asai, Hirochika, et al. "Network application profiling with traffic causality graphs." International Journal of Network Management 24.4 (2014): 289-303.
- [5] iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design

Contact

Lars Wüstrich wuestrich@net.in.tum.de
Christian Lübben luebben@net.in.tum.de
Holger Kinkelin kinkelin@net.in.tum.de
http://go.tum.de/080755