Master's Thesis at Siemens
Topic: Security Attack Detection in Automation and Control Systems

SIEMENS
Ingenuity for life

Master's Thesis at Siemens

Master's Thesis Topic: Security Attack Detection in Automation and Control Systems

Location: The Master's work will be carried out at and financed by Siemens Corporate Technology in Munich

Working conditions:

- This opening is only for TUM students, preferably from Electrical Engineering or Computer Science
- The selected student will conduct the work at Siemens Corporate Technology in Munich (last stop of U5 in Neuperlach Süd)
- From the TUM side, this work will be supervised by the Chair of Real-Time Computer Systems
- The duration of the work will be 6 months
- The selected student will be paid by Siemens according to its regulations for financing Master's students
- The student will have an opportunity to interact with different Siemens internal groups working on IT Security and Industrial Automation
- The work will be carried out and the thesis written in English
- Starting date: as soon as possible

Contact person at Siemens: Dr. Dragan Obradovic

The application documents should be sent to: dragan.obradovic@siemens.com. They should include a CV and copies of transcripts / grades.

Master's Thesis at Siemens
Topic: Security Attack Detection in Automation and Control Systems

SIEMENS
Ingenuity for life

Topic Description:

Classical Internet security methods such as access control, firewalls and encryption are applied to a variety of applications including automation and control systems. But in contrast to other applications, automation systems are typically used in a very well planned and optimized manner, where the knowledge about their dynamics and underlying communication links are stored in different engineering tools. Having access to this knowledge enables planning very sophisticated cyber-attacks such as Stuxnet, but it also enables the development of mechanisms for early detection and stopping of these attacks.

Exploiting the available system knowledge in detection of possible malicious attacks can be illustrated on the detection methods based on identifying deviations in the observed underlying communication traffic. If no knowledge about the application is available, observing its communication traffic would only lead to the network topology identification and to a black-box statistical model of packet exchanges between network elements. Any deviation from "typical" communication patterns would then be seen as a sign of a cyber-attack.

Although in the above approach the network topology will be detected, there will be no semantic understanding of the network elements and the generated traffic. On the other hand, with the application system knowledge the underlaying communication elements will be clearly related to control system elements such controllers, sensors and actuators. In addition, by knowing the controller sampling rate, the frequency of the information (i.e., packet) exchange will also be a priori known. Hence, the communication traffic model would be much more accurate and reliable.

The goal of this Master's thesis work is to first analyze the state-of-the-art in cyber-attack detection and mitigation measures relying on the a priori knowledge about the application. Second, it is expected that this work will investigate and develop different attack detection mechanisms relying on diverse levels of the control application knowledge, from knowing the close-loop communication topology all the way to having dynamic models of the controller and the controlled plant.

Reference:

Peter Waszecki, Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Ramesh Karri, Samarjit Chakraborty: *Automotive Electrical and Electronic Architecture Security via Distributed In-Vehicle Traffic Monitoring*. IEEE Trans. on CAD of Integrated Circuits and Systems 36(11): 1790-1803 (2017)

This paper proposes security attacks in cars using in-vehicle traffic monitoring schemes. Similar ideas could be extended to automation systems in this thesis work.