Master assignment / Internship

Improving the security of the industrial control traffic – traffic analysis and classification.

This is an external assignment to be carried on in collaboration with Stedin Netbeheer BV, Rotterdam / Utrecht / Delft (http://www.stedin.nl), and ENCS - European Network for Cyber Security, The Hague (https://www.encs.eu)

Objective:
Critical infrastructures, such as the power distribution, depend on SCADA (Supervisory Control and Data Acquisition) system for their operation. SCADA systems provide the operator with a real time view of the controlled process and allow a remote execution of supervisory commands. However, many of the existing networks were designed with other priorities than their security. Meanwhile, SCADA networks are vulnerable to cyber attacks due to many factors: the increasing tendency to connect the control networks and corporate networks of these systems; allowing remote connections to the unmanned premises; connecting part of these networks to the Internet. Since the attacks are evolving, the networks are never entirely secure. Nevertheless, there is a possibility to detect malicious behaviours in a network by monitoring the traffic, and observing patterns or anomalies, which indicate an intrusion.

Stedin Netbeheer is a power distributor operating mostly in the Randstad conurbation, managing 250 substations of 10kV and higher, and more than 20 000 medium voltage substations. These substations are used to transform the voltage and distribute the electrical power, and are mostly monitored and operated using SCADA networks.

Current network monitoring methods are not tailored to SCADA networks – commonly we see an attempt to use the techniques from IT networks in SCADA networks. The goal of this assignment is to classify the type of traffic observed on the premises of a power distributor, that is, in a substation, and propose a method (or tool) to identify malicious connections, or traffic patterns.

We are looking for someone, who:
- Is doing a Master program in Computer Science, Telematics or Electrical Engineering
- Has good programming skills (e.g. Python, Java)
- Is interested in network traffic monitoring, and intrusion detection.

Assignment:
The goal of this assignment is to classify the type of traffic observed in a premise of power distributor and propose a method to identify malicious connections, or traffic patterns. With the outcome of your project we would like to be able to answer the following questions:
- What are the appropriate tools for investigating the IP connectivity within a substation (e.g. libpcap, Snort, Bro)?
- What devices are communicating within substation? What devices are communicating from outside the substation?
- Is whitelisting a feasible security measure of a substation?
- Remote connection to a substation: what should be avoided and what is recommended?
- What topology is observed in a substation? Can you visualise it from the traffic?

Your tool or method will be verified using traffic collected from a real power grid substation.
If you are interested and have an additional or different idea, contact us. Maybe we also think it's interesting.

For more information about this assignment, please contact:

- Anne Remke: a.k.i.remke@utwente.nl
- Boudewijn Haverkort: b.r.h.m.haverkort@utwente.nl
- Justyna Chromik: j.j.chromik@utwente.nl