PICS Seminar — Thu 1 Feb 2018 at 10:00 – 11:30 — P401 (note room change)
Sten F Andler: Vulnerabilities and Countermeasures in Smart Grids

We present two KTH papers on 1) a study of software vulnerabilities and weaknesses of cyber components in smart grids, and 2) an analysis of the effectiveness of attack countermeasures in such a system. The focus of both papers is on embedded devices in power substations and generation plants, typically controlled by a SCADA system (for Supervisory Control And Data Acquisition). The vulnerabilities study is on actual systems with intelligent components from major manufacturers. The study uses publicly available data on the types of systems and identified vulnerabilities and weaknesses from publicly available databases and the manufacturer's websites. The study summarizes the types and severity of common vulnerabilities and shows that they mostly result from a small number of fairly simple weaknesses. It is also apparent that not all manufacturers are keen on disclosing their vulnerabilities and weaknesses. The analysis of countermeasures, on the other hand, constructs abstract models of typical electric power systems, based on publicly available information as well as expert elicitation and certain assumptions. The models are used to evaluate the overall cyber security posture and the effectiveness of protection strategies, using attack graph evaluation (securiCAD). In summary, the most effective measures are network securement (including passwords) and network segmentation (firewalls). Frequent patching is prohibitively expensive and running intrusion detection systems is not usually possible on the heterogeneous hardware. Our own approach in Elvira proposes to perform such intrusion analysis on a common operational picture, separate from the operational system, obtained by extracting data from the operational system itself.

--- Reference materials ---

This is a presentation of two KTH papers that were given in the CPSR-SG 2017 workshop at CPS Week 2017, Pittsburgh, PA, USA, with kind permission of the authors. The slides have only slight modifications from the original slides.
Paper #1: https://drive.google.com/open?id=1EO8qHD-fTS6O9FkXQdezYhUeE5lcYV8x
Presentation #1: https://drive.google.com/open?id=1spCRNBepIbVlff_ybMI2JBNaa8dvENse

Study on Software Vulnerabilities and Weaknesses of Embedded Systems in Power Networks (Margus Välja, Matus Korman, Robert Lagerström)

Abstract: ”In this paper we conduct an empirical study with the purpose of identifying common software weaknesses of embedded devices used as part of industrial control systems in power grids. The data is gathered about the devices and software of 6 companies, ABB, General Electric, Schneider Electric, Schweitzer Engineering Laboratories, Siemens and Wind River. The study uses data from the manufacturers online databases, NVD, CWE and ICS CERT. We identified that the most common problems that were reported are related to the improper input validation, cryptographic issues, and programming errors.”

Paper #2: https://drive.google.com/open?id=11bU9w0C58DMJUHh2y1jbKLFYrORVoKFD
Presentation #2: https://drive.google.com/open?id=1oth4UtVE-J-Qi99vRYhhrPsdyixBAgTy

Analyzing the Effectiveness of Attack Countermeasures in a SCADA System (Matus Korman, Margus Välja, Gunnar Björkman, Mathias Ekstedt, Alexandre Vernotte, Robert Lagerström)

Abstract: ”The SCADA infrastructure is a key component for power grid operations. Securing the SCADA infrastructure against cyber intrusions is thus vital for a well-functioning power grid. However, the task remains a particular challenge, not the least since not all available security mechanisms are easily deployable in these reliability-critical and complex, multi-vendor environments that host modern systems alongside legacy ones, to support a range of sensitive power grid operations. this paper examines how effective a few countermeasures are likely to be in SCADA environments, including those that are commonly considered out of bounds. The results show that granular network segmentation is a particularly effective countermeasure, followed by frequent patching of systems (which is unfortunately still difficult to date). The results also show that the enforcement of a password policy and restrictive network configuration including whitelisting of devices contributes to increased security, though best in combination with granular network segmentation.”