Karlsruher Institut für Technologie

Earliest start: Now!

KASTEL

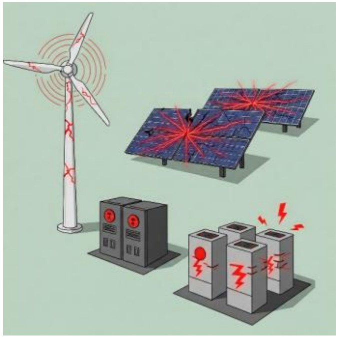
Bachelor's Thesis / Master's Thesis
Data Modification Attack on protection relays in the Smart Grid
Cyberattack on power plants at KASTEL Security Lab Energy

The Secure Energy Systems (SES) research group focuses on the cyber-physical security of energy systems. We operate the KASTEL Security Lab Energy to conduct cybersecurity experiments on the smart grid in a safe environment.

In the distributed generation part of our lab, we use a hardware-in-the-loop approach to simulate a photovoltaic power plant, wind turbine and battery power plant. The real-time simulation is connected to protection relays via analog amplifiers. Each power plant uses a Remote Terminal Unit (RTU) as a gateway between field level and the control center.

An attacker with insider access to the power plant could install a malicious device in the network. With this backdoor in place, the attacker can modify data sent between the RTU and protection relay. Using this capability, the attacker can launch a data modification attack on the control commands that are relayed by the RTU.

The goal of this project is to develop a data modification attack for the Manufacturing Message Specification (MMS) protocol from the IEC 61850 standard. The attack should be evaluated using the connection between the RTU and the protection relay. Due to a firmware bug, the password protection of MMS can be bypassed. Therefore, the attack can assume knowledge of the password for the protection relay.



We offer:

- Realistic lab environment with industrial hardware
- Possibility of contributing to scientific publications
- Close supervision

Requirements:

- Student in Computer Science or electrical engineering
- Basic understanding of network protocols
- Good Python programming skills

The proposed thesis consists of the following **main tasks:**

- Familiarization with RTUs, protection relays and the MMS protocol
- Define conditions for unsafe states and their potential impact for PV/Wind/Battery power plants
- Implementation of the MMS data modification attack in the KASTEL Security Lab Energy
- Extend the data modification attack to achieve a greater impact by targeting the unsafe states
- Master Thesis: Coordinated Attack on multiple power plants

We are happy to answer any questions you might have. If you are interested, contact me via email to nicolai.kellerer@kit.edu including current transcript of records and a resume/CV.
A prior HiWi time can be arranged to get more familiarization with the topic.

Contact Data

Karlsruher Institut für Technologie (KIT)
Automation and Applied Informatics (IAI)
Location: Campus North

Name: Nicolai Kellerer
Secure Energy Systems (SES)
Phone: +49 721 608-24913
E-Mail: nicolai.kellerer@kit.edu