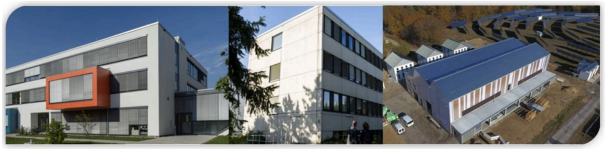
Karlsruhe Institute of Technology



Institute for Automation and Applied Informatics (IAI)

Master's Thesis

Structured analysis of Photovoltaics Inverter Communication

Photovoltaic Inverters perform the DC/AC conversion in PV Systems. They are often digitally connected and remotely controllable. Due to the growing amount of installed systems and the small amount of manufacturers in the market, identical points of influence for large amounts of PV-Inverters exist. This makes them a critical component for the power grid [1].

Knowledge of the control influences of these devices is only available on a theoretical level, this work closes the gap by practically analyzing the actually implemented influences.

Research Questions:

- Which commands does a typical PV inverter accept and from which origin?
- Are power-dimming commands accepted and for which purpose?
- Which endpoints does an inverter connect to and what data is being transmitted?
- How are these connections secured against attacks?
- What protection mechanisms are implemented against Load-Altering-Attacks?

Main Tasks:

- Get an overview over the functionality of the selected PV inverters
- Set up an evaluation plan that allows a structured analysis of the PV inverters
- Perform technical analysis on up to five PV inverters
- Document the results and, if relevant, together with the supervisors report possible

vulnerabilities to the manufactures

Required Skills and Experience:

- Masters Student in Computer Science or related
- Technical knowledge on most of the following topics: Basic Knowledge of Photovoltaic Systems, IT-Security for IoT devices, basic networking, machine-in-the-middle attacks, firmware reverse engineering, scripting in any language, authentication and X.509 certificates

References:

[1]: Goerke et al. „Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability “ 2024, doi:10.1145/3632775.3661943

Contact
Nils Goerke
goerke@fzi.de
Richard Rudolph
richard.rudolph@kit.edu

Skills

- PV Systems
- IT-Security for IoT
- Networking
- Mitm attacks
- Firmware reverse engineering
- Scripting in any language
- Authentication and X.509 certificates

Studies

- Computer Science / Informatics

Languages

German or English

Institute for Automation and Applied Informatics (IAI)
Karlsruhe Institute of Technology
Campus North
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen