Karlsruhe Institute of Technology

Security Lab

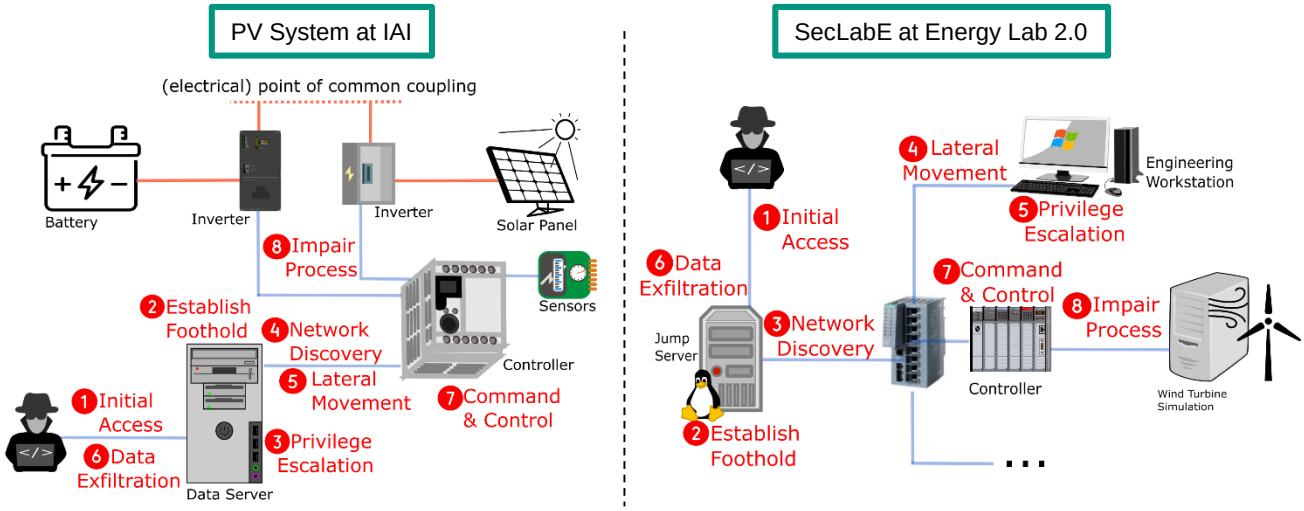
Institute for Automation and Applied Informatics (IAI)

Earliest start: now

HiWi

Attack Emulation with Caldera at Seurity Lab Energy

Background: The most dangerous attackers for critical infrastructures are the so-called Advanced Persistent Threat (APT) actors who often employ low and slow strategies with many system built-in tools[1]. For intrusion detection research, appropriate data is of critical importance. Given that we can hardly find any usable and useful public dataset that fits our application domain and with which we can evaluate and improve our detection methods, we need to resort to attack emulation. For this, we do experiments, on the one hand, on a real energy system (with minimal impact on it), i.e., a PV system in operation at our institute, and on the other hand, in a lab environment, i.e., SecLabE at Energy Lab 2.0. With Caldera, we aim to mimic common behaviors of APT actors in our test systems, for data generation.



Tasks:

- Literature review of major cyber-attacks, APT actors, MITRE ATT&CK matrix
- Get familiar with the Caldera attack emulation framework
- Implement attack steps listed in the above figures, and be creative
- Collect, process and label the generated data

Benefits: At the beginning (1-2 months), the supervisor will spend a reasonable amount of time to teach, guide and support the student with the appropriate materials. In this case, the student does not have to spend/waste lots of time for finding the appropriate literature, tutorials. At the end, the student should have a solid understanding of cyber-attacks, and practical experience in implementing attacks and using various tools etc.

Requirements: Highly motivated; basic understanding of cyber-attacks; good programming skills; adequate understanding of operating systems and network communication.

1. Q. Liu et al. 2022. Binary Exploitation in Industrial Control Systems: Past, Present and Future. *IEEE Access*, *10*, 48242 - 48273.

Contact: Qi Liu
Group: Robust Secure Automation (RSA)
Phone: +49 721 608-23973
E-mail: qi.liu@kit.edu

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