

Smart Energy Management Program (SEMP)

“innovative security mechanisms in smart grids”

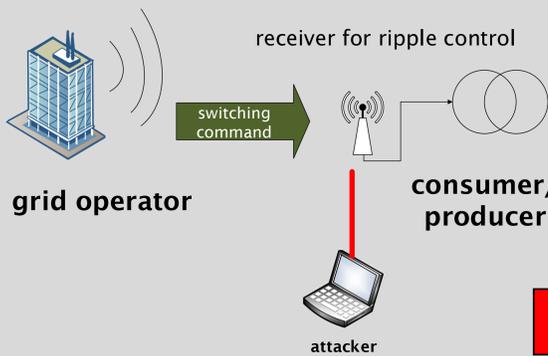
Starting point:

- ◆ hardly/no security-mechanisms in ripple control
- ◆ upcoming Smart Meter Gateways don't cover all security concerns

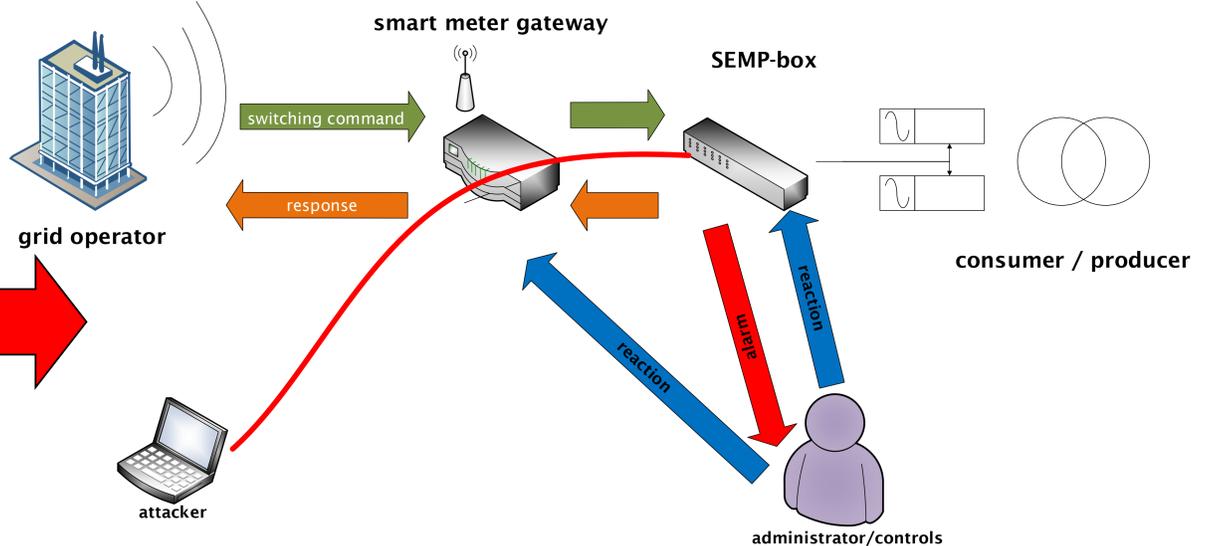
Project idea:

- ◆ active management for energy-producers and consumers
- ◆ based on the “MessSystem 2020” (FNN)
- ◆ innovative security mechanisms (HoneyNet, IDS)
- ◆ classic IT-concepts are transferred to the smart grid
- ◆ auditable transfer and execution of switching commands

State of the art (1):

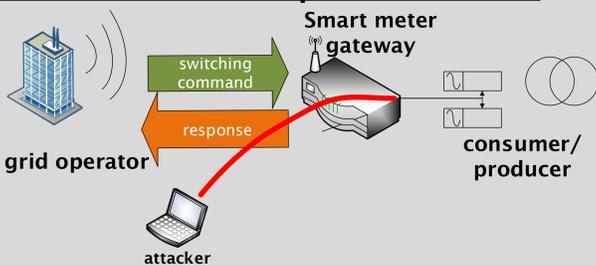


Projectgoal SEMP (3):



- ◆ SEMP-box used as an additional security gateway
- ◆ via hash-chains validated, bi-directional communication
- ◆ automated alarm-functions in case of anomalies >>> fast reaction possible

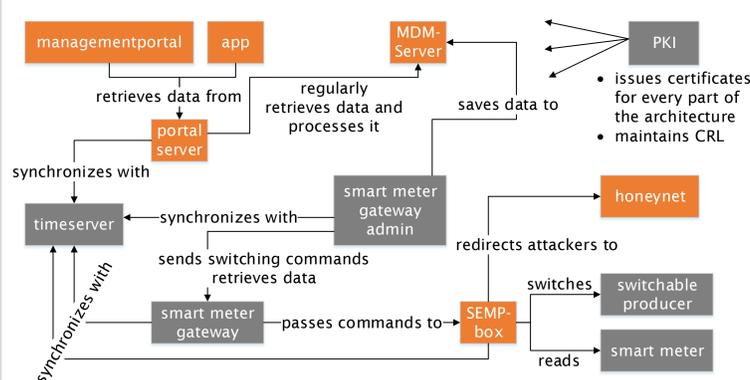
Current developments (2):



Necessary steps:

- ◆ analysis of actual systems
- ◆ compliance to technical guidelines by BSI (Federal Office for Information Security)
- ◆ definition of an architecture
- ◆ definition of security requirements for every part of the architecture
- ◆ development of an intrusion detection system running on the SEMP-box
- ◆ development of a HoneyNet (Gen III)

SEMP-architecture (4):



- ◆ every communication is secured via TLS
- ◆ certificate-based authentication, where possible
- ◆ SEMP-box used as central point for security and execution of switching commands

HoneyNet development:

- ◆ development of a new honeywall with new Web-UI
- ◆ development of a method to monitor encrypted communication
- ◆ virtualization of SMGW and SEMP-boxes
- ◆ best possible cover up of virtualization

HoneyNet (5):

- ◆ used for research in new attack methods
- ◆ used for distraction from the productive system
- ◆ honeywall as central, invisible monitoring point
- ◆ SEMP-Box's intrusion detection system detects attack and initiates redirection of the attacker

