Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

NR Contributions to the overall Goal of the IoTSec Project

Norwegian Computing Center

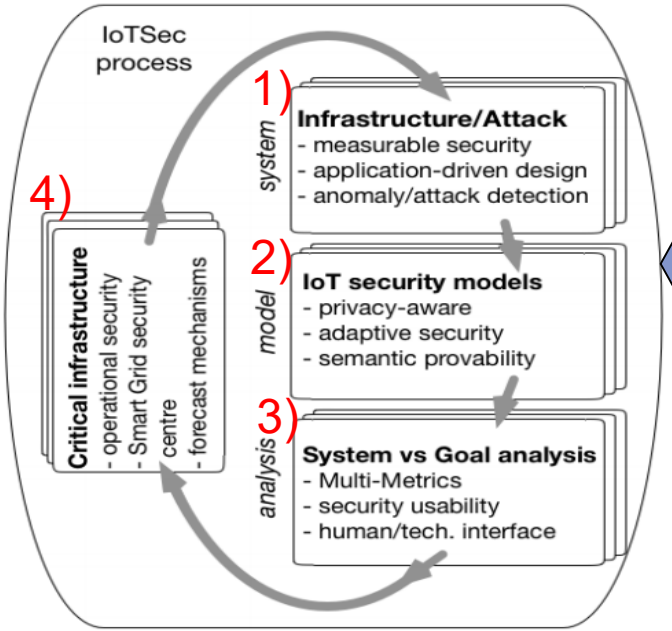
Habtamu Abie

Gjøvik

24/10-2019

Goal: Safe and secure IoT-enabled smart power grid infrastructure

IoTSec process



5) General

NR's contributions: Anticipatory intelligence

1) - Measuring security & attack detection – EGT
2) - Privacy aware & adaptive security
- adaptive authentication, semantic description of IoT
- communication-efficient privacy-preserving, temporal anonymity, compromise-protection
- EGT (Integrity & confidentiality)
- adaptive data collection

3) - Security evaluation and analysis
- white paper and presentation at sikkerthetfestival 2019

4) - Adaptive data collection & analytics

5) - 2 Master students & 4 services to smart grid security center

Case Studies

- Smart home
- Smart meters
- AMI (advanced metering Infrastructure)
- Smart Grid Security Center
- Education & internationalization

Case studies

- Smart home
  - Adaptive authentication, semantic description, data collection, adaptive cybersecurity framework
- Smart meters
  - privacy-preserving, temporal anonymity, compromise-protection
  - EGT
- AMI (Advance Metering Infrastructure)
  - EGT (integrity and confidentiality) attack-defense
- Smart Grid Security Center
  - Risk-based security design, adaptive security, scenario-based security analysis, user-centric security

Contributions to Smart Grid Security Centre

- Risk-based security design
  - organization wide: governance, construction and operations
- Adaptive security
  - detect and adjust to changes in the environment
- Scenario-based security analysis
  - design and analysis of security services, toolkit consisting of scenarios, threats, metrics, and simulations
- User-centric security
  - holistic model of smart grid systems and their users

Benefits of IoT based smart grid [1]

- Advanced metering infrastructure (AMI)
  - Easily implementing the advanced metering infrastructure
- Improved reliability of the power system
  - intelligent grid that has the ability to quickly self-healing, in the event of any external or internal disturbances or threats
- Enhanced functions of SCADA
  - a large number of sensors, actuators and smart meters deployed to monitor the whole power grid infrastructure

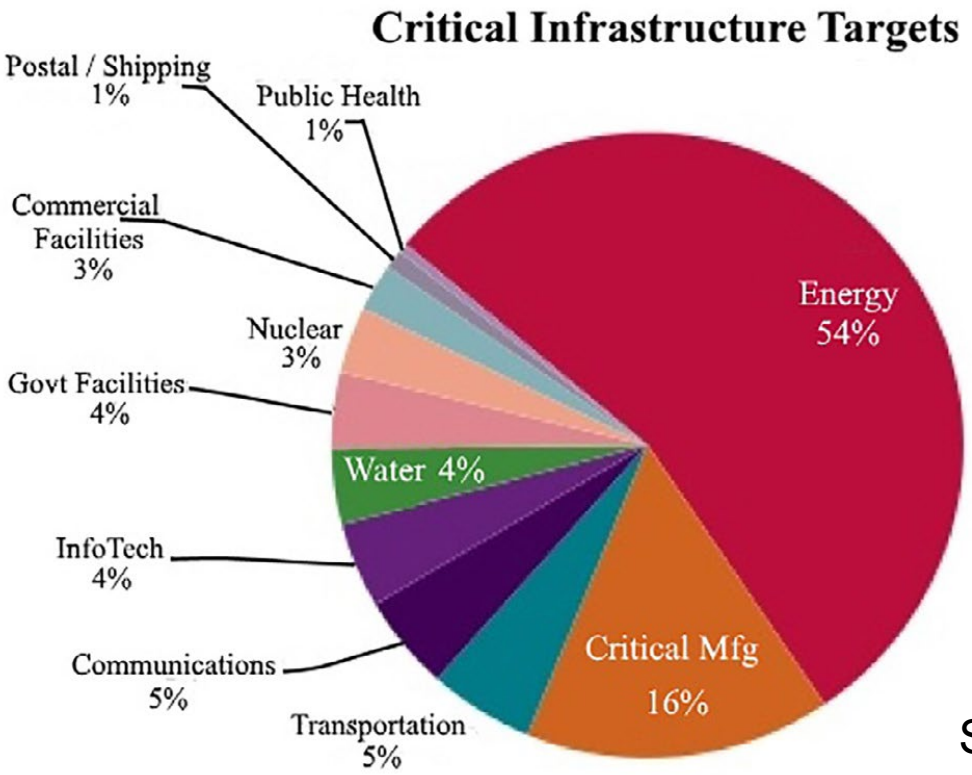
Benefits of IoT based smart grid [1] …

- Management of power in the grid
  - bidirectional electric flow where the end-customer buys and sells any excess energy
- Demand response.
  - managing load and demand response, enabling the effecting of dynamic energy pricing mechanisms.

Benefits of IoT based smart grid [1] …

- Interaction with end-customer
  - real time, fast, and bi-directional data exchange provides better interaction with energy end-users
- Monitoring the status and operation of grid assets
  - IoT helps to detect, predict and respond to emerging problems proactively

Impact of cyber-attacks on critical infrastructure, 2016

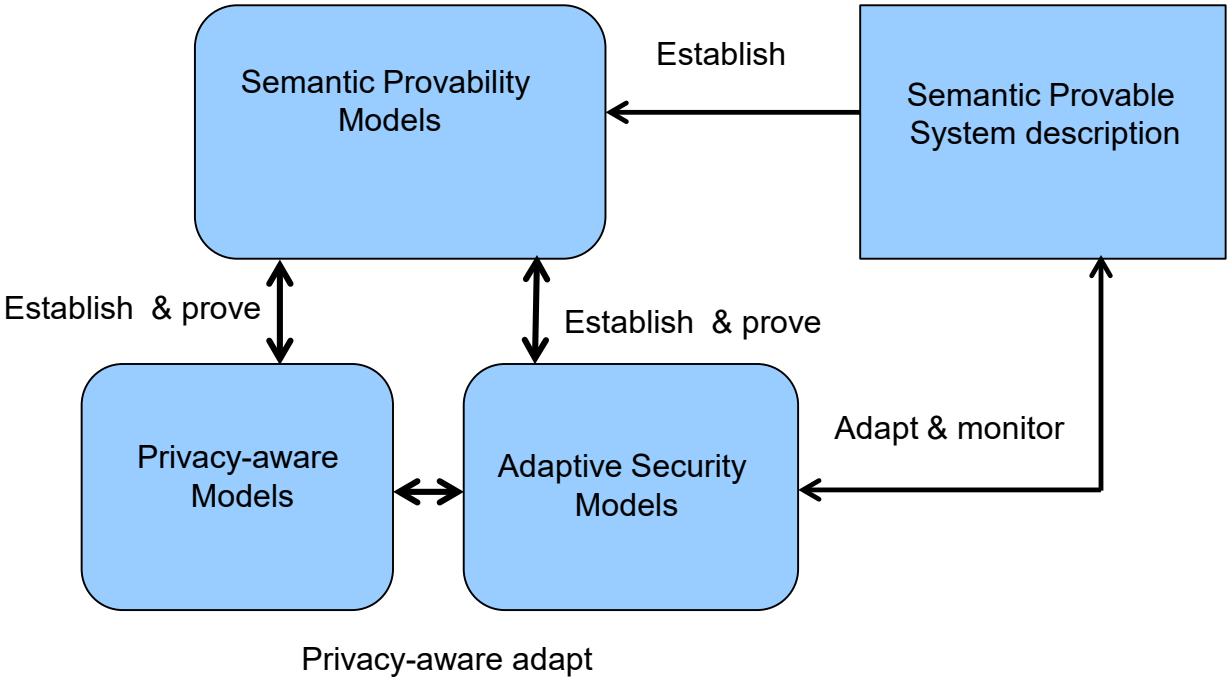


Source: [1]

Four main types of attacks

- Device attack
  - compromise and control a grid network device
- Data attack
  - illegally insert, alter, or delete data or control commands
- Privacy attack
  - learn about a users' private or personal information
- Network attack
  - denial of service (DoS)

Example - WP2 – Inter-tasks research integration



Future outlook

- Anticipatory intelligence
  - collecting and analyzing information to identify new, emerging trends, changing conditions
- Emotion AI
  - AI (replicating the way humans think) that measures, understands, simulates, and reacts to human emotions
- Explainable AI (XAI)
  - solution that can be understood by human experts, an implementation of the social right to explanation
- Cognitive Security
  - processing of increasing volume of data by interpreting, diagnosing and adapt to the environment without the need for human intervention
- SDGs (UN sustainable development goals)
  - Contributions to solving challenges to one or more of the SDGs

Seminal Reference

1. Kenneth Kimani, Vitalice Oduol, Kibet Langat, Cyber security challenges for IoT-based smart grid networks, international journal of critical infrastructure protection 25 (2019) 36–49