Challenges of Cyber Security in Smart Grids

Gothenburg, 2010-10-11

Jens Zerbst

VATTENFALL

Cyber Security perceptions of a ’Smart Grid’

- Introduction and expansion of a communication network for the current and upcoming electricity network
- Introduction of new technology and connectivity approach
- Long term usage of legacy assets in the domains operation, bulk generation, transmission and distribution
- Introduction of intelligent control and connectivity between different domains; e.g. customer, markets, service provider, operation, bulk generation, transmission and distribution
- In some parts usage of large scale homogeneous technical environmental
- **…**

Multi-layered risk discussion in ‘Smart Grid’

- Vulnerabilities
  - Legacy systems
  - Introduction of connectivity (even to un-trusted partners)
  - Increasing technical complexity (e.g. protocols)
  - "Security by obscurity" security culture background
  - Lacking physical access restriction
  - …

Multi-layered risk discussion in ‘Smart Grid’

- Likelihood
  - High grade of connectivity
  - Huge amount of devices with homogeneous technology
  - Partly exposed infrastructure
  - Processing of increasing amount of data (e.g. customer data)
  - Potential larger scale communication network
  - …

Multi-layered risk discussion in ‘Smart Grid’

- Impact
  - Fraud
  - Privacy
  - Compliance
  - Availability, Reliability
  - Safety
  - …

Threat vector as an example

	Intentional	Un-intentional
Malicious	e.g. dedicated attack from criminal individuals, groups, terrorists or nations	e.g. un-directed attack from a ‘common’ Botnet virus
Non-malicious	e.g. a disgruntled employee or outsourcing vendor intentionally manipulates sensor data	e.g. malfunction of software or procedures

VATTENFALL

Questions

VATTENFALL