Contributions to SmartGrid Security Centre

by NR

Idea for SGSC:
1) Risk-based Security Design

Idea: A comprehensive, risk-based development process for smart grid and AMR

Security measures need to be developed and maintained within a structured framework.

Scope: Organisation wide (governance, *construction* and operations)

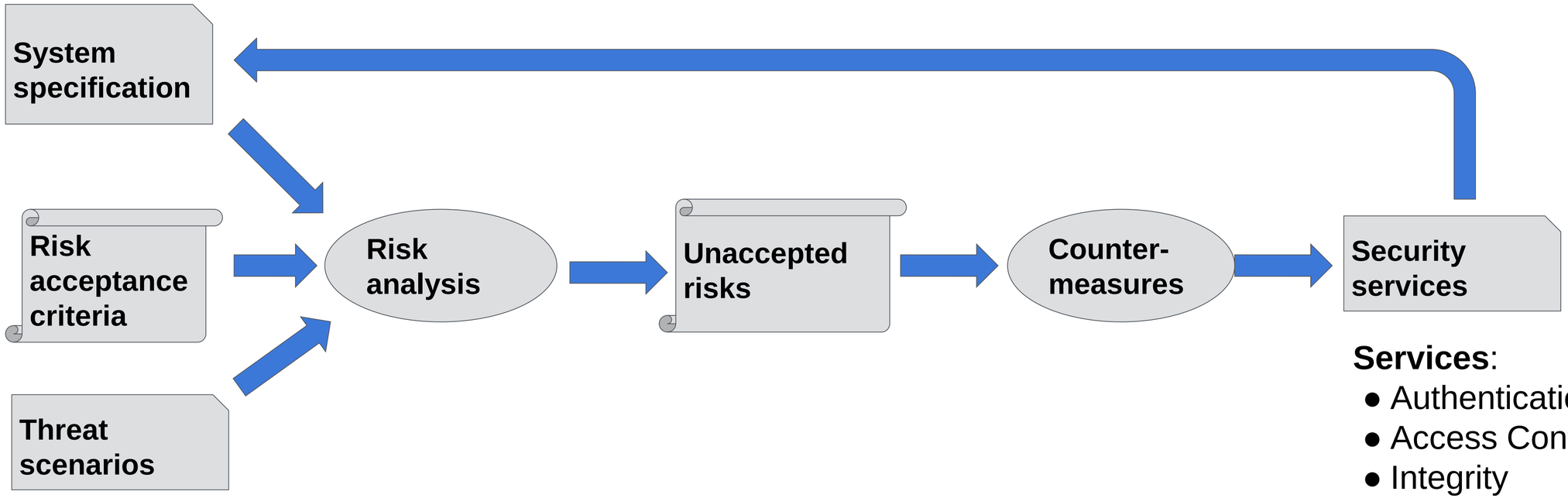
- Framework: OpenSAMM and BSIMM
- Methodology: Adapted from NIST Special Pub. 800-30 & 800-39
  Threat scenarios, risk assessment, risk acceptance criteria and countermeasures
- Design level: applying security protection mechanisms to each node and communication
  - Security protocols and mechanisms in detail (e.g. PROSA precise spec and analysis)
  - Test to verify security behaviour

Relevant work: PCAS (Personalized Centralized Authentication System), HighTrustWallet

Applicability to the SGSC and interest for external partners:

The Security Centre can recommend and guide appropriate security assurance processes.
This should be highly relevant for DSOs and the smart grid industry.

Idea for SGSC:
1) Risk-based Security Design



Services:

- Authentication
- Access Control
- Integrity
- Confidentiality
- Non-repudiation
- Support:
  - Audit
  - Log

Idea for SGSC:
2) Smart Grid Security Services

Idea: Design and analysis of security services for AMR and smart grid

Scope:

- Adaptive security – detect and adjust to changes in the environment
- Security protocols – design, specification and verification
- Cryptographic mechanisms – geared towards the smart grid / AMR use case
- Automatic testing – verify that the actual implementation follows the spec

Relevant work:

- ASSET – Adaptive Security for Smart Internet of Things in eHealth
- PROSA – precise specification and analysis
- “Compromise-protection of smart meters in the smart grid using co-dependent authentication”

Applicability to the SGSC and interest for external partners:

The Security Centre can recommend and guide appropriate security assurance processes.
This should be highly relevant for DSOs and the smart grid industry.

Idea for SGSC:
3) User-centric security

Idea: holistic model of smart grid systems and their users

A smart grid is a complicated distributed system where users form part of the system.
To avoid surprising/undesirable properties/behaviors one must consider the system as a whole.

Scope:

- Analyse the ux of smart grid management systems – with emphasis on security
- Train users and build user awareness – use tools that provide on-the-job training via smartphones or PCs

Relevant work:

- uTRUSTit – Usable TRUST in the Internet of Things
- PLA – Personlig (mobil) læringsarena

Applicability:

System security and good UX is crucial for the customers of the Security Centre
Media presentation: video, simulation, audience participation via gamification and e-learning

External interest:

This should be highly relevant for DSOs and the smart grid industry.

Idea for SGSC:
4) Scenario-based security analysis

Idea: scenario-based evaluation framework for planned smart grid solutions

Toolkit consisting of scenarios, threats, metrics, and simulations

Scope:

- Scenario creation using narrative technologies
- Catalogue of threat scenarios – for risk evaluation
- Complex security metrics – take privacy and usability into account
- Analyse results from simulations

Relevant work: "An Evaluation Framework for Adaptive Security for the IoT in eHealth"
(and an unpublished risk-based extension)

Applicability:

There is a need for practical and easily applicable analysis methods for smart grid evaluations.

External interest:

This is a practical method to analyse key security features of complex systems.