Towards a Framework for Engineering Smart-Grid-Specific Privacy Requriements

Christian Neureiter, Günther Eibl, Armin Veichtlbauer und Dominik Engel

Josef Ressel Center for
User-Centric Smart Grid Privacy, Security and Control
Urstein Sued 1 | 5412 Puch/Salzburg | Austria

web: www.en-trust.at | www.fh-salzburg.ac.at

Projekt Kontext

- Projekt „SGMS – INTEGRA“
  - Re-Engineering und Integration implementierter Smart Grid Projekte
  - Basis: M/490 Smart Grid Architecture Model (SGAM)
  - → SGAM-Toolbox (*www.en-trust.at/SGAM-Toolbox*)

- Erkenntnisse
  - Integration nicht-funktionaler Requiremens (z.B. Privacy)
  - Requirements-Engineering für Privacy Requirements

- State of the Art
  - Privacy Requirements Engineering (Software Engineering)
  - Smart Grid Privacy

Ziele & Ansatz

- Ziel: Privacy by Design

- Ansatz
  - Integration in Entwicklungsprozess
    - Model Driven Architecture (MDA) Process
    - Privacy im Kontext von Dependability
  - Conceptual Framework
    - Strukturierte Integration in Domain-Specific Language
  - Initiales Set an „High Level Privacy Requirements“
    - Analog zu M/490 „High Level Use Cases“
  - Evaluierung an umgesetzten Real-Life Projekten
    - Konkretisierung der Requirements
    - Integration in Engineering Prozess

Privacy im Kontext von Dependability

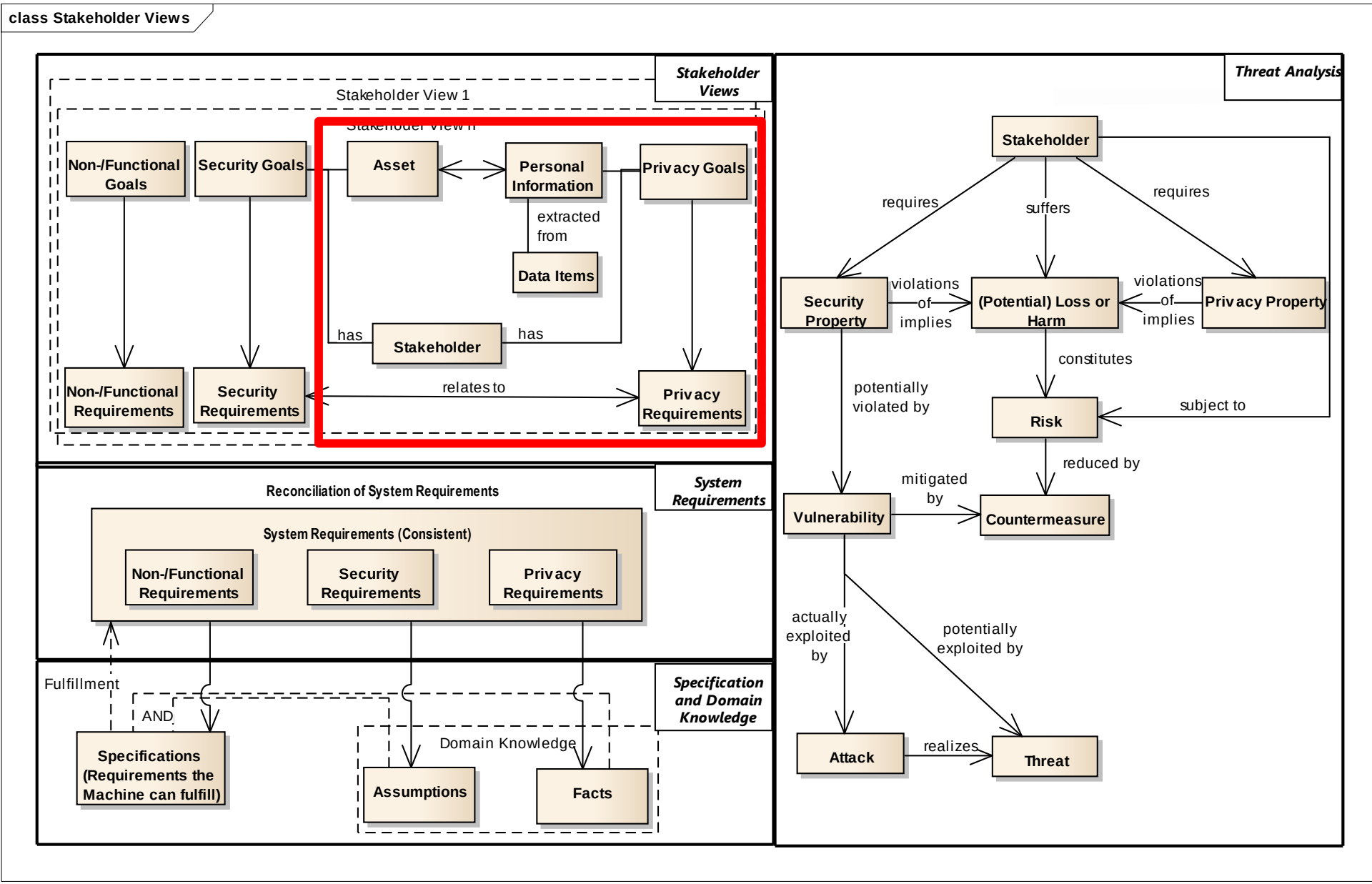
- „Verletzung von Privacy stellt eine Gefährdung dar“
  - Schwächere Gefährdung als Verletzung der funktionalen Sicherheit

- Dependability
  - Prozesse und Methoden vorhanden
  - → RAMSS (Reliability, Availability, Maintainability, Safety, Security)
  - *„By Design“*

- P-RAMSS
  - Erweiterung um Privacy
  - Anwendung erprobter und bekannter Methoden
  - *„By Design“*

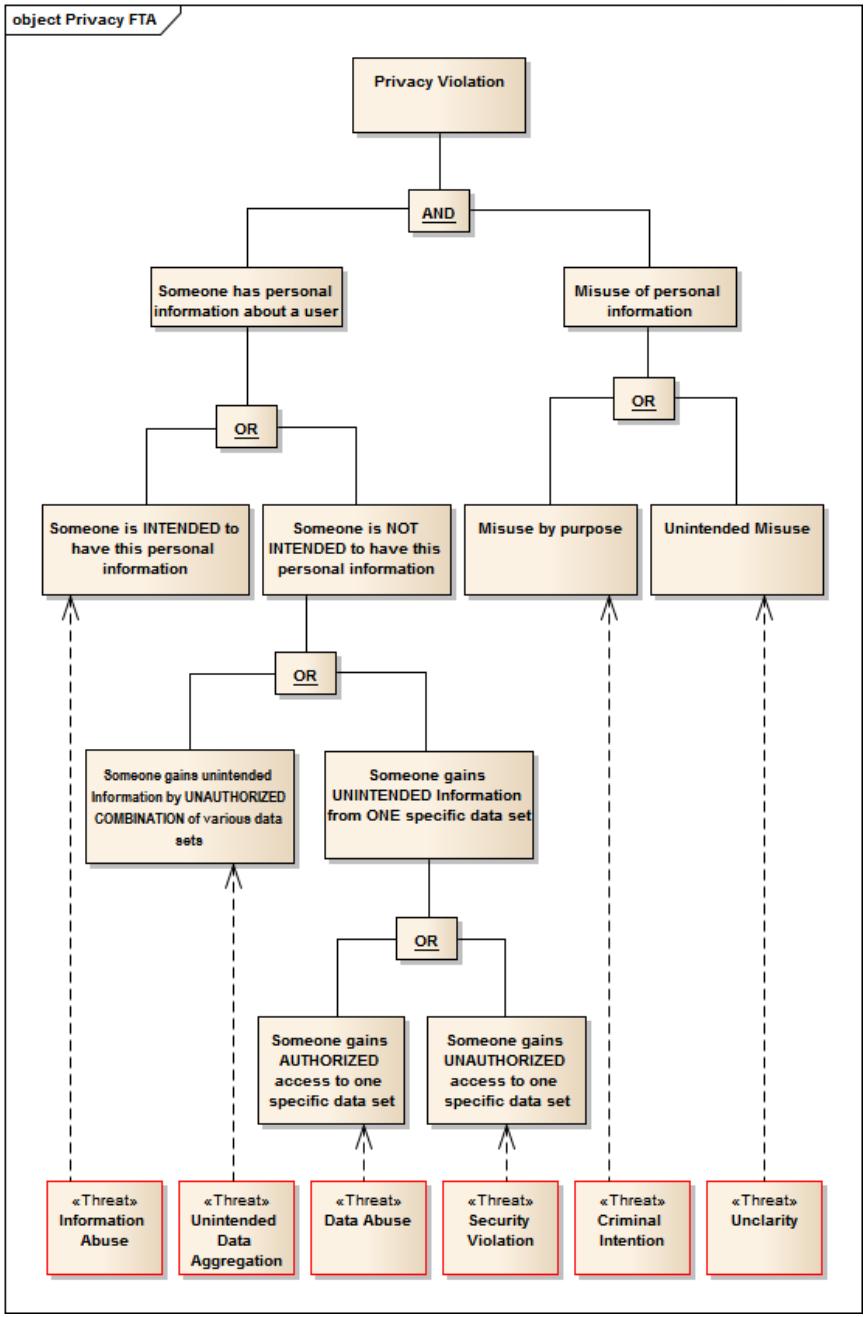
Conceptual Framework

- Integration des Conceptual Frameworks von Beckers et al. [8]
  - Minimale Adaption (Data Items)
  - Darstellung der Relation zwischen „Daten“ und „Persönlicher Information“
  - → welche persönlichen Informationen können aus Daten (Messwerten) gewonnen werden?


class Stakeholder Views
Stakeholder Views
Stakeholder View 1
Stakeholder View II
Non-/Functional Goals
Security Goals
Asset
Personal Information
Privacy Goals
extracted from
Data Items
has
Stakeholder
has
Non-/Functional Requirements
Security Requirements
relates to
Privacy Requirements
System Requirements
Reconciliation of System Requirements
System Requirements (Consistent)
Non-/Functional Requirements
Security Requirements
Privacy Requirements
Fulfillment
AND
Specifications (Requirements the Machine can fulfill)
Specification and Domain Knowledge
Domain Knowledge
Assumptions
Facts
Threat Analysis
Stakeholder
requires
suffers
requires
Security Property
violations of
implies
(Potential) Loss or Harm
violations of
implies
Privacy Property
constitutes
potentially violated by
Risk
subject to
reduced by
mitigated by
Vulnerability
Countermeasure
actually exploited by
potentially exploited by
Attack
realizes
Threat

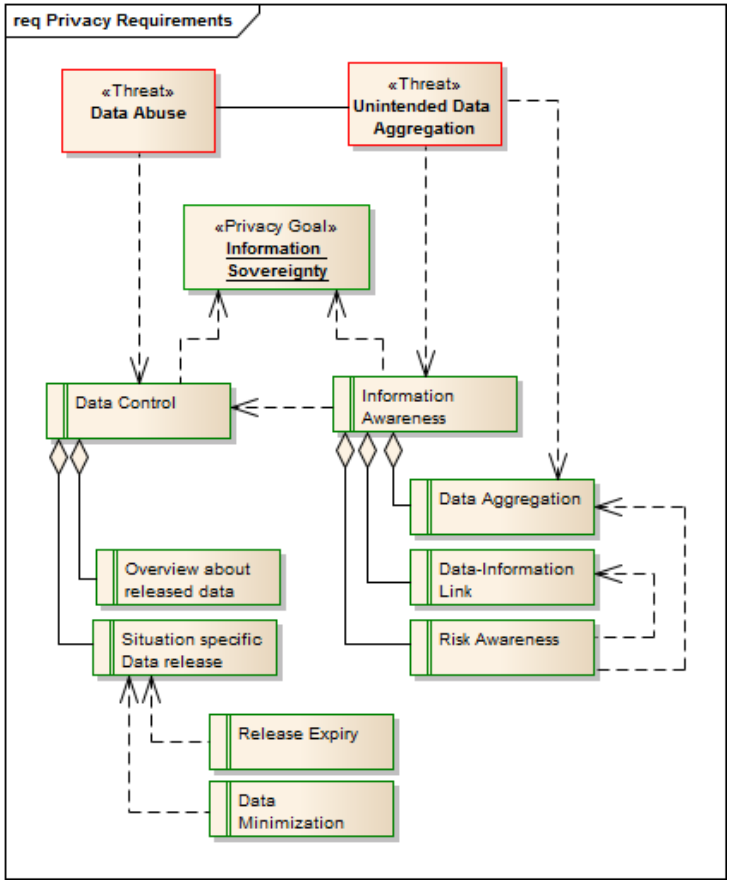
Threat Tree Analysis

- Abstrakte Threat Tree Analysis
  - „Privacy Violation“
  - *„Someone uses information about me in a way I don‘t want“*
- Expliziter Schritt
  - Informations-Gewinn aus Daten
- Fokus
  - Data Abuse
  - Unintended Data Aggregation



Requirement Elicitation

- High Level Privacy Requirements
  - Analog zu M/490 HLUC‘s
- Neues Privacy Goal
  - Information Sovereignty
- Zwei wesentliche Aspekte
  - „Information Awareness“
  - „Data Control“



Aktuelle Arbeiten

- Integration des Frameworks in SGAM-Toolbox
  - Modellbasierte Architektur
  - Domain-Specific-Language
  - Smart Grid Architecture Model (SGAM)
  - Use Case Mapping Proces

- Evaluierung an Real Life Project
  - Privacy Requirements Engineering
  - Projekt INTEGRA

Vielen Dank für Ihre Aufmerksamkeit

christian.neureiter@en-trust.at