Institut für Nachrichtenübermittlung

Prof. Dr. Christoph Ruland

Vortrag

Sicherheitsanalyse der Übertragung von Energiedaten über offene Netze

anlässlich des

1. SELMA-Workshops

Übertragung von Energiemessdaten über offene Kommunikationssysteme

am 5./6. Juni 2002
bei der Physikalisch-Technischen Bundesanstalt
in Berlin-Charlottenburg

Dipl.-Inform. Melanie Angele
Prof. Dr. Christoph Ruland

Uni Siegen

Institut für Nachrichtenübermittlung

Prof. Dr. Christoph Ruland

Sicherheitsanalyse der Übertragung von Energiedaten über offene Netze

Vorgehensweise am Beispiel
des Projektes SELMA

Dipl.-Inform. Melanie Angele
Prof. Dr. Christoph Ruland

Uni Siegen

Institut für Nachrichtenübermittlung
Prof. Dr. Christoph Ruland

Agenda

- Einbettung der Sicherheitsanalyse in den Projekt-Ablauf von SELMA
- Vorstellung der bei SELMA eingesetzten Methodik der Sicherheitsanalyse
- Voraussetzungen und Besonderheiten im Fall von SELMA
- Exemplarischer Ablauf der Sicherheitsanalyse mit Beispielen

Institut für Nachrichtenübermittlung
Prof. Dr. Christoph Ruland

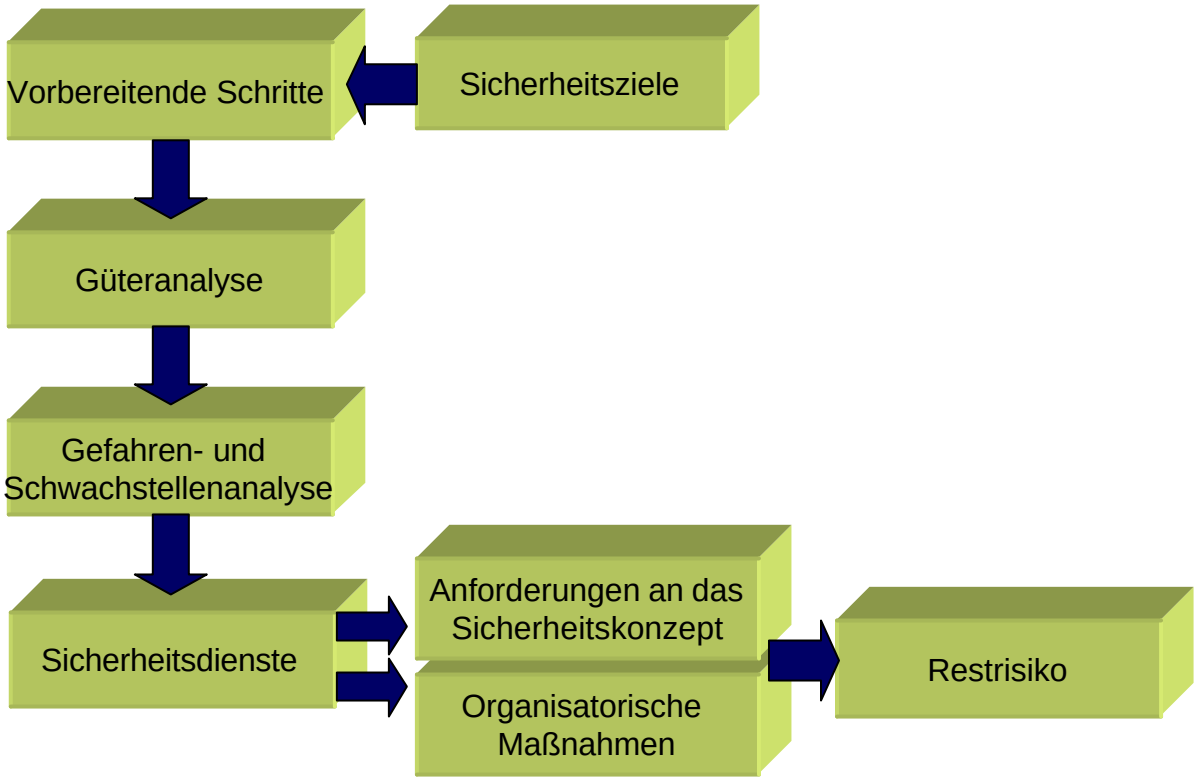
Sicherheitsanalyse bei SELMA

- Voraussetzungen
  - Das System, das analysiert werden soll, muss bekannt sein
  - Sicherheitspolitik muss vorhanden sein
  - Bei SELMA: System unbekannt, Sicherheitspolitik nicht definiert, daher: Analyse des Status Quo und der möglichen Anforderungen im liberalisierten Energiemarkt
- Aufgaben
  - Definition der Sicherheitsziele
  - Methodische Analyse von Angriffsszenarien
  - Definition der benötigten Sicherheitsdienste
  - Restrisikoanalyse Sicherheitsdienste/Sicherheitsziele
- Auswirkungen
  - Anforderungen an das Sicherheitskonzept
  - Im Sicherheitskonzept: Restrisikoanalyse Sicherheitskonzept/Sicherheitsziele

Institut für Nachrichtenübermittlung
Prof. Dr. Christoph Ruland

Methodik Sicherheitsanalyse

- Schematische Darstellung der bei SELMA verwendeten Methodik:



Grundlagen

- Sicherheitsziele wurden von den SELMA Projektteilnehmern definiert
- Definition eines abstrakten rollen-basierten Modells als Basis für die Analyse
- Verallgemeinertes Konzept
  - Nicht speziell für Energieübergabe zwischen Energieerzeuger und Endabnehmer, sondern
  - beliebig einsetzbar bei jeder Energieübergabe zwischen Energielieferant und -abnehmer
- Annahme: Im privatisierten Energiemarkt sind alle Marktteilnehmer potentielle Angreifer und Angriffsziele

Angreifer-Koalitionen

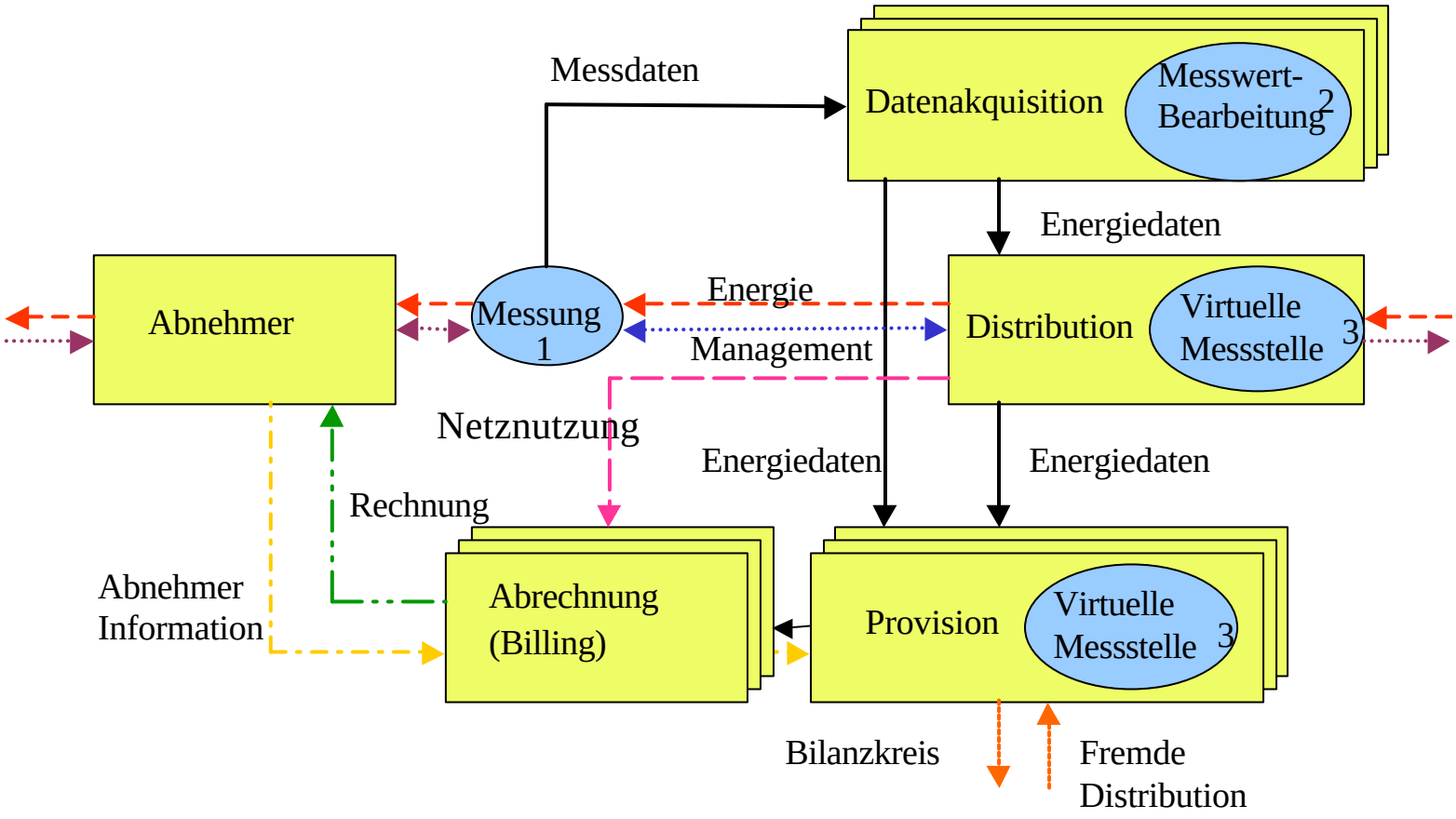
- Neue Angriffsformen durch gemeinsame Angriffe gleicher oder unterschiedlicher Marktteilnehmer
- Beispiele
  - **Veränderung der Daten in Absprache zwischen Abnehmer und Akquisitionsstelle**
    - Die Akquisitionsstelle verändert die gemessenen Daten (Messwert oder Uhrzeit) so, dass ein Abnehmer auf Kosten anderer Energie bezieht
  - **Austausch der Messgeräte zwischen zwei Abnehmern**
    - Ein Abnehmer wählt einen günstigen Tagtarif, ein anderer einen günstigen Nachttarif. Durch Austausch wird Tag und Nacht Energie zum günstigen Tarif bezogen.

Sicherheitsziele (Auswahl)

- Einhaltung der gesetzlichen Anforderungen
  - Eichgesetz, Eichordnung, PTB-Anforderungen, Datenschutz
- Die erzeugten Messdaten müssen nachweisbar und rechtsgültig sein
- Betrugs- und Manipulationsversuche müssen erkannt werden
- Sicherheit muss skalierbar und anpassbar sein
- Messgeräte müssen online konfigurierbar sein
- Alle Beteiligte, inkl. Presse und Öffentlichkeit müssen Vertrauen in SELMA haben
- Es darf nicht möglich sein, dass sich mehrere Marktteilnehmer erfolgreich für einen Angriff zusammen-tun

Institut für Nachrichtenübermittlung
Prof. Dr. Christoph Ruland

Rollenbasiertes abstraktes Modell



Uni Siegen

Güteranalyse

- Bestimmung der relevanten Güter (Hardware, Software, Funktionen, Informationen, etc.) und ihres Wertes
- Beispiel Messdaten:
  - Auswirkung bei Manipulation:
    - Fehlerhafte Abrechnung
    - Unter Umständen finanzieller Verlust für den Abnehmer oder andere Teilnehmer
    - Imageverlust (falls es bekannt wird)
    - Wert: hoch
  - Auswirkung bei Verlust/Zerstörung
    - Ungenaue Abrechnung
    - Verlust der Nachprüfbarkeit
    - Wert: mittel

Gefahren- und Schwachstellenanalyse

- Zufällige Gefahren
  - Naturkatastrophen, Hard- und Software, Umgebungsprobleme, Bedienungsfehler
- Passive Angriffe
  - Abhören
- Aktive Angriffe (Auswahl)
  - Nicht-autorisierter Managementzugriff
  - Modifikation während der Übertragung
  - Manipulationen, Löschen, Wiederholen von Daten
  - Maskerade als anderer Systemteilnehmer
  - Leugnen des Ursprungs der Daten
  - Angriffe von Koalitionen

Institut für Nachrichtenübermittlung
Prof. Dr. Christoph Ruland

Beschreibung der Angriffe

- Beschreibung der Attacke
  (Beispiel: „Akquisitionsstelle modifiziert die Daten in Absprache mit dem Teilnehmer“)
- Motivation („finanzieller Vorteil“)
- Wahrscheinlichkeit („mittel“)
- Bestehende Gegenmaßnahmen („keine“)
- Gefährdung durch die Attacke („mittel“)

→ Attacke muss durch Sicherheitsdienste verhindert oder zumindest erkannt oder als Restrisiko akzeptiert werden.

Geforderte Sicherheitsdienste

- Vertraulichkeit
  - personenbezogene Daten
- Gewährleistung der Datenunversehrheit
  - Messdaten, Managementdaten
- Verfügbarkeit
  - Messdaten, Abrechnungsdaten
- Authentikation
  - Messdaten, Kommandos, Abrechnungsdaten
- Zugangs- und Zugriffskontrolle
  - Datenzugriff, Managementzugriff
- Nicht-Abstreitbarkeit
  - Messwerte, Quittungen
- Logbücher

Institut für Nachrichtenübermittlung
Prof. Dr. Christoph Ruland

Anforderungen an das Sicherheitskonzept (1)

- Technische Anforderungen (Auswahl)
  - Digitale Signaturen der Messwerte sollen technisch qualifizierten Signaturen entsprechen
  - Erweiterungen der Messdatensätze um digitale Signaturen, zeitvariante Parameter, zusätzliche Identifikationen, etc.
  - End-to-End Authentikation der Messwerte von der Generierung bis zur Abrechnung
  - Verifikation der Messwerte muss jedem Marktteilnehmer möglich sein
  - Transportgebundene Vertraulichkeit bei Übertragung personenbezogener oder sensibler Daten
  - Managementanforderungen (Schlüssel-, Rechte-, Parameter-Management, Software-Download)
  - Mehrfache Lieferanten mit jeweils externen Datenakquisitionsstellen

Anforderungen an das Sicherheitskonzept (2)

- Organisatorische Anforderungen (Auswahl)
  - Umgang mit (asymmetrischen) Schlüsselsystemen: Gewährleistung der Geheimhaltung privater Schlüssel, Authentizität der öffentlichen Schlüssel
  - Herstellung und Initialisierung der Messgeräte
  - Management eichtechnisch-relevanter Vorgänge
  - Management nicht-eichtechnisch-relevanter Vorgänge
  - Zusammenhang mit EDI-Konzept des VDEW zur elektronischen Verarbeitung von Messdaten

Restrisiko

- 100%ige Sicherheit ist nicht erreichbar
- Das Restrisiko wird bewusst in Kauf genommen
- Das Restrisiko wird dazu genutzt, eine günstige Kosten-Nutzen Relation zu erhalten.
- Mehrstufige Restrisikoanalyse
  - **Sicherheitsanalyse**
    - Vergleich Sicherheitsziele mit Anforderungen an Sicherheitsdienste und Sicherheitskonzept
  - **Sicherheitskonzept**
    - Vergleich Umsetzung der Sicherheitsanalyse
  - **Spezifikation**
    - Vergleich Umsetzung des Sicherheitskonzeptes
  - **Realisierung**
    - Problem fehlerhafter Implementation

Zusammenfassung

- Sicherheitsanalyse für den Messwert-Datenaus-tausch im liberalisierten Energiemarkt
- Marktteilnehmer können mehrfach auftreten, Funktionen können an externe Partner delegiert werden. Daher ist eine große Vielzahl an Möglichkeiten der Verteilung von Funktionen auf die Marktteilnehmer gegeben
- Der allgemeine Ansatz - Rollenmodell und Markteilnehmer - hat sich äußerst bewährt
- Es wurden systematisch Angriffsszenarien betrachtet
- Anforderungen an Sicherheitsdienste und die Sicherheitsarchitektur wurden definiert
- Gute Ausgangsbasis für Sicherheitskonzept und Messlatte für die Restrisikoanalyse