Designing for Privacy:
Theorie und Praxis datenschutzfördernder Technik

Abschlussdiskussion:

Welche Wege führen zu datenschutzfördernden Systemen?

Jörg
pohle@informatik.hu-berlin.de
http://waste.informatik.hu-berlin.de/Lehre/ws0910/pet/

20.01.2010

Tagesordnung und Zeitplan

1. Inhaltliche Fragen zu „Engineering Privacy“ (10 min)
2. Sammlung der bisher betrachteten Methoden (20 min)
3. Kritik (10 min)
4. Diskussion (30 min)
5. Seminarrückschau (10 min)
6. Fragen zu Seminararbeiten (10 min)

Inhaltliche Fragen zu „Engineering Privacy“

Sammlung der bisher betrachteten Methoden

- PriS – Privacy Safeguard
- PRIME – Privacy and Identity Management for Europe
- MOQARE – Misuse-Oriented QuAlity Requirements Engineering
- UMLsec
- „Engineering Privacy“

PriS – Privacy Safeguard

- Vorbedingung: Es existiert ein Modell des Systems mit *Organisationszielen*, die durch *Prozesse* realisiert werden, die von *technischen Systemen* unterstützt werden.
- Vorgehen:
  1. *Datenschutzziele* definieren/finden
  2. *Einfluss* der Datenschutzziele *auf die Prozesse* bestimmen
  3. *Techniken* identifizieren, durch die die dann datenschützenden Prozesse implementiert und/oder unterstützt werden
- Ziel: ?

PRIME – Privacy and Identity Management for Europe

Das PRIME-Projekt hat kein konsistentes Vorgehensmodell für die Ableitung von technischen Datenschutzanforderungen anzubieten.

MOQARE – Misuse-Oriented QuAlity Requirements Engineering

- Vorbedingung: Es existiert eine Liste der *funktionalen Anforderungen*.
- Vorgehen:
  1. Finden der *Qualitätsziele* (nichtfunktionale Anforderungen)
  2. Beschreiben der *Misuse-Fälle*
  3. Definition der *Gegenmaßnahmen*
  4. für Gegenmaßnahmen, die Qualitätsziele sind, bei 2. neu starten
- Ziel: *Misuse Tree*

UMLsec

- Vorbedingung: Es existiert ein *UML-Modell* des Systems.
- Vorgehen:
  1. Binden von *Sicherheitsanforderungen* an UML-Elemente
  2. *Konsistenzprüfung* des Modells
  3. im Fehlerfall fehlende Anforderungen nachtragen und bei 2. neu starten
- Ziel: Modell mit *garantierten Sicherheits- bzw. Datenschutz-eigenschaften*

„Engineering Privacy“

- Vorbedingungen: *Domänenmodell* (user/recipient/joint sphere), sensible *Prozesse* (Übermittlung, Speicherung, Verarbeitung)
- Vorgehen?:
  1. *Bedrohungsmodell*: Nutzervorstellungen und -bedenken gegenüber den Prozessen in den verschiedenen Domänen, sowie inhärente Datenschutzgefährdungen
  2. gesetzliche Anforderungen an datenschutzkonforme Datenverarbeitung in Bezug auf Domänen und Prozesse
  3. *privacy-by-architecture* vs. *privacy-by-policy*
- Ziel: *Leitfaden*, aber kein Vorgehensmodell

Kritik

- Keines der Vorgehensmodelle leitet die Anforderungen tatsächlich aus dem Gesetz ab, daher gibt es keine Garantie der Vollständigkeit.
- Ohne Modellierung der rechtlichen Anforderungen im Zusammenhang können interne Abhängigkeiten nicht dargestellt werden.
- Teilweise erscheinen die Anforderungen, die aus dem Datenschutz abgeleitet werden, entweder rein technik-bezogen oder amateurhaft.

Diskussion

Seminarrückschau

- Inhalt und Schwerpunkt
- Form
- Verbesserungspotential

Fragen zu Seminararbeiten

Formale Anforderungen:

- 12 – 15 Seiten (etwa 30.000 – 35.000 Zeichen)
- themenbezogener Fließtext
- korrekte Rechtschreibung, Grammatik und Zeichensetzung
- korrekter Umgang mit Quellen

Vielen Dank für Eure Aufmerksamkeit!