Angeglichener Informationsfluss

sozialbasierte Modellierung von Datenschutz in UbiCom

Xiaodong Jiang, Jason I. Hong, and James A. Landay
University of California, Berkeley

Hans-Jürgen Stemmer, 30.6.2004

Ungleiche Informationsverteilung

- Besitz "geheimer" Informationen, die von allgemeinem Interesse sind
- Beispiel Gebrauchtwagenmarkt
  - Der Verkäufer hat in der Regel sehr viel bessere Informationen über "sein" Auto als der Käufer
- Beispiel Fahrrad-Diebstahlversicherung
  - Unter den Fahrradfahrern gibt es welche, die das Risiko eines Diebstahls durch fehlende oder schlechte Fahrradschlösser erhöhen

Externe Einflüsse

- nicht oder unzureichend berücksichtigt
- nicht oder unzureichend berechenbar
- Kosten und Konsequenzen werden von Unbeteiligten getragen
- Beispiel Wasserverschmutzung
  - Ursache: Verschmutzung durch Industrieanlagen
  - Auswirkung: Schädigung des Fischbestandes
  - Kosten: Fischer
- Störung des Marktes / Gleichgewichtes

Ein Beispiel

- Alice besucht Paris
- Sie leiht einen TravelGuide (Palm) aus, der sie auf interessante Orte hinweist und über den sie Informationen abfragen kann

Alice (Data Owner)

Ein Beispiel

- Bob ist Geschäftsmann in Paris
- Er bietet das System TravelGuide an
- Das System bestimmt den Standort der Geräte und gibt Tips für den Aufenthalt

Ein Beispiel

Bob (Data Collector)

Alice (Data Owner)

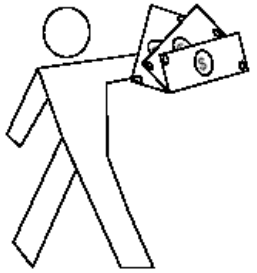
- Bob kennt Alices Aufenthaltsort
- Er erfährt, was Alice interessiert
- Alice weiß über Bob nichts

Ein Beispiel

Bob (Data Collector)

Alice (Data Owner)

Carol (Future Data User)



Die Situation ist schizophren

- Neue Möglichkeiten und
- Neue Risiken

- Hardware immer leistungsfähiger
- Speicher immer größer (Diskette, CD, DVD)
- Software immer besser (Bilderkennung, ...)
- Vernetzung flächendeckend und flexibel
- Miniaturisierung
- Gerätekosten sinken

Datenschutz ist ein Kompromiss

Absatz/Marketing

Bequemlichkeit

Nutzen

Bedienbarkeit **Datenschutz**

Haftung

Sicherheit

Gesellschaft

Gestaltung von Datenschutz

- Märkte
  - Handel mit Informationen
  - Verbraucherverhalten (Bezahlung, Sensibilität)
- Gesellschaft
  - Normen, Verursacher, Bestrafung
- Gesetzgebung
  - Eigentumsrecht an privaten Daten
  - Risikoabschätzung
- Technologie

Principle of Minimum Asymmetry

A privacy-aware system should minimize the asymmetry of information between data owners and data collectors and data users, by:

- Decreasing the flow of information from data owners to data collectors and users
- Increasing the flow of information from data collectors and users back to data owners

Approximate Information Flow

- **Information Space**
  - Speicherung, Verwaltung und Verteilung
- Qualität der Daten
  - Lebensdauer, Genauigkeit, Zuverlässigkeit
- Begrenzung von Daten
  - physikalisch, sozial (Abteilung), activity-based
- Operationen auf Daten
  - create, update, delete, grant
  - promotion, composition, inference

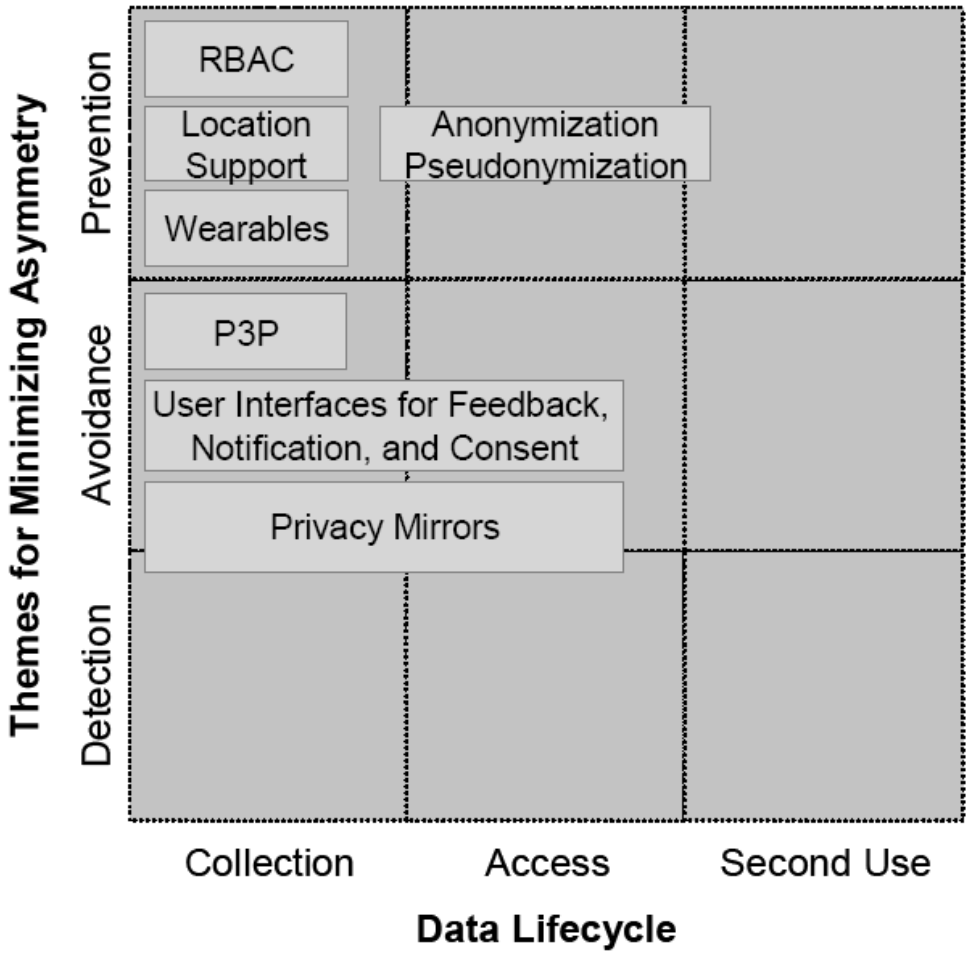
Approximate Information Flow

- **Lebenszyklus (Data Lifecycle)**
  - Sammlung, Zugriff, Verarbeitung, Weitergabe
  - Was geschieht mit Daten?
- Gewinnung von Daten
- Zugriffsschutz, Verwendungszweck, Datensicht
- Verwendung nach der Erhebung
- Verwendung durch Dritte
  - Kontrolle

Approximate Information Flow

- **Themes** (Prevention, Avoidance, Detection)
- Vorbeugung
  - Geringere Qualität, Anonymisierung, Garbage Collection, Verschlüsselung
- Vermeidung
  - Dialog mit dem Benutzer, Hinweismeldungen
- Erkennung
  - Aufspüren von Datenschutzverletzungen, Verfolgung, Notification

A Design Space for categorizing privacy protection mechanisms



Verwendungsmöglichkeiten

- Beschreibung von Themen, Produktion und Anforderungen
- Bedarf erkennen
- Merkmal zur Zertifizierung