Ausarbeitung AW1

Privacy in Location-based Services

Fatih Keles

Hamburg, 08. Juni 2006

Gliederung

- Motivation
- Privacy
- Location-based Services
- Privacy-Bedrohungen in LBS
- Privacy-Konzepte für LBS
  - Sichere Kommunikation
  - Privacy-Regeln
  - Anonymisierung
- Ausblick

Motivation

- Immer mehr leistungsfähige mobile Geräte
- Interesse an LBS steigt
  - Provider: Lukrativer Markt, ...
  - Nutzer: Einfacheres Alltagsleben, Entertainment, ...
- Aber:
  - Privacy-Vorbehalte der Nutzer
  - Gesetzliche Vorgaben bzgl. Privacy
- ➔Privacy in LBS wichtiges Thema

Privacy

- „Privacy bezeichnet
  - das Anrecht von Personen, Gruppen und Institutionen,
  - selbst zu bestimmen,
  - wann, wie und in welchem Umfang
  - persönliche Informationen
  - an andere weitergegeben werden.“

Westin, 1970

- Im Deutschen: Datenschutz, Privatsphäre

Privacy

- Risiken:
  - Veröffentlichung intimer Informationen ohne Einwilligung
  - Missbrauch dieser Informationen
  - „Ich habe nichts zu Verbergen“?
  - Verknüpfung von Informationen

Privacy

- Gesetzgebung in Deutschland:
  - Bundesdatenschutzgesetz (BDSG)
    - §1 Recht auf informationelle Selbstbestimmung
    - §3a Datenvermeidung und Datensparsamkeit
    - §4 Zulässigkeit der Datenerhebung
    - §28 Zweckbindung
    - ...

Location-based Services

- Im Wesentlichen von Thomas eingeführt
- „Dienste, die den Standort eines Nutzers oder Objektes verwenden, um den Nutzen des Dienstes zu steigern.“

Schiller und Voisard, 2004
Küpper, 2005

- Kategorisierung:
  - Reaktive Dienste vs. Proaktive Dienste

  - Genauigkeit der Ortsinformationen
  - Anonym nutzbar?

Privacy-Bedrohungen in LBS

- Dilemma:
  - LBS ohne Ortsinformationen nicht möglich, aber
  - Ortsinformationen potentielles Privacy-Risiko

- Ortsinformationen → weitere persönliche Informationen
  - z. B.
    - Hobbies,
    - Freundeskreis,
    - politische Einstellungen,
    - ...

Privacy-Bedrohungen in LBS

- Interessenten an persönlichen Ortsinformationen
  - Einzelpersonen
    - z. B. Freunde, Verwandte, Einbrecher
  - Böswillige Unternehmen
    - z. B. Arbeitgeber, Banken
  - Staatliche Einrichtungen
    - z. B. Justizbehörden

Privacy-Bedrohungen in LBS

- Möglichkeiten an persönliche Ortsinform. anderer zu gelangen
  - Durchsickern von Ortsinformationen
  - Durchsickern von Zeitinformationen
  - Durchsickern der Identität
  - Geheime Absprachen
  - Unerlaubtes abhören

Privacy-Konzepte für LBS

- Sichere Kommunikation
- Privacy-Regeln
- Anonymisierung

Sichere Kommunikation

- Ziel: Sichern der Leitung zwischen Anbieter und Nutzer
- Mechanismen:
  - Authentifikation
  - Integrität
  - Vertraulichkeit
- Realisierung:
  - Verschlüsselung der Verbindung
  - Authentifikationstechniken

Privacy-Regeln

- Fragestellung:
  - Wer
  - darf wann
  - in welchem Umfang
  - auf welche Ortsdaten zugreifen?
- Beispiel:
  - Mein Arbeitgeber
  - darf montags bis freitags
  - wenn ich bei der Arbeitsstelle bin
  - meine genaue Position verfolgen.

Privacy-Regeln

- Regeln beschreiben:
  - Aktoren
  - Dienstarten
  - Zeitliche Beschränkungen
  - Örtliche Beschränkungen
  - Genauigkeit der Ortsinformationen
  - Kontextabhängige Bedingungen
  - ...
- Verknüpfungen von Regeln bestimmen Gesamtregel
  - Achtung: Regeln müssen Widerspruchsfrei sein

Privacy-Regeln

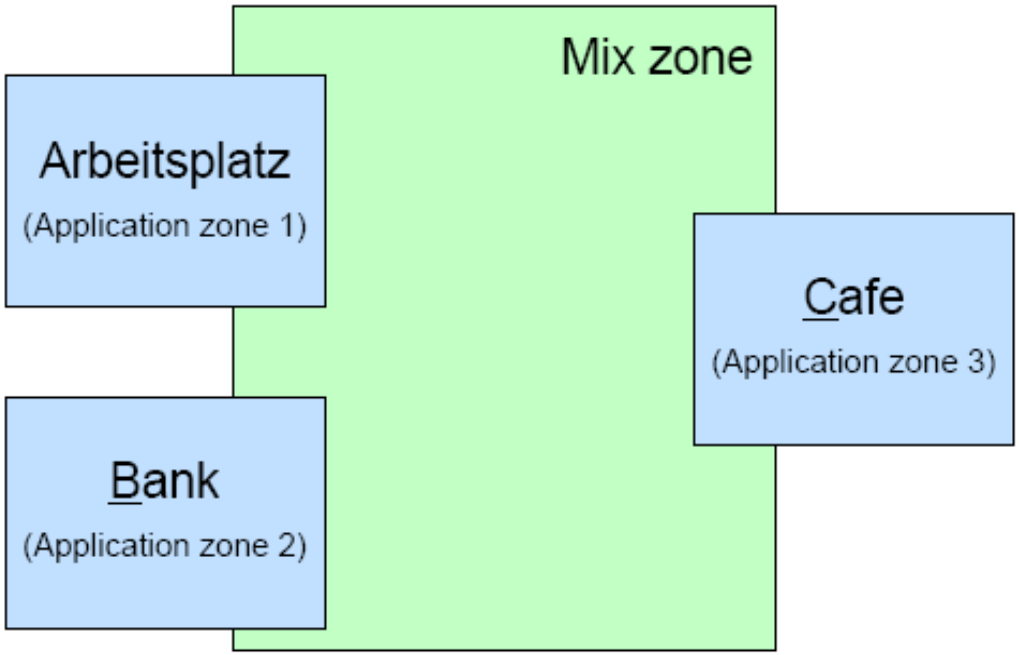
- Arbeit zu dem Thema:
  - „Preserving Privacy in Environments with Location-based Applications“ (Myles, Friday, Davies, 2003)
  - Zentrales Element: Validatoren
    - User Confirmation Validator
    - Limit Time Validator
    - Limit Location Validator
    - ...
  - Regel = Verknüpfung von Validatoren
  - Widerspruchsfreiheit: Festlegung von Prioritäten und Abarbeitungsreihenfolgen

Anonymisierung

- Idee:
  - Pseudonyme bei Nutzung von LBS
  - Konkrete Person nicht identifizierbar
- Arbeit zu dem Thema:
  - Mix Zones-Konzept (Beresford, Stajano, 2003)

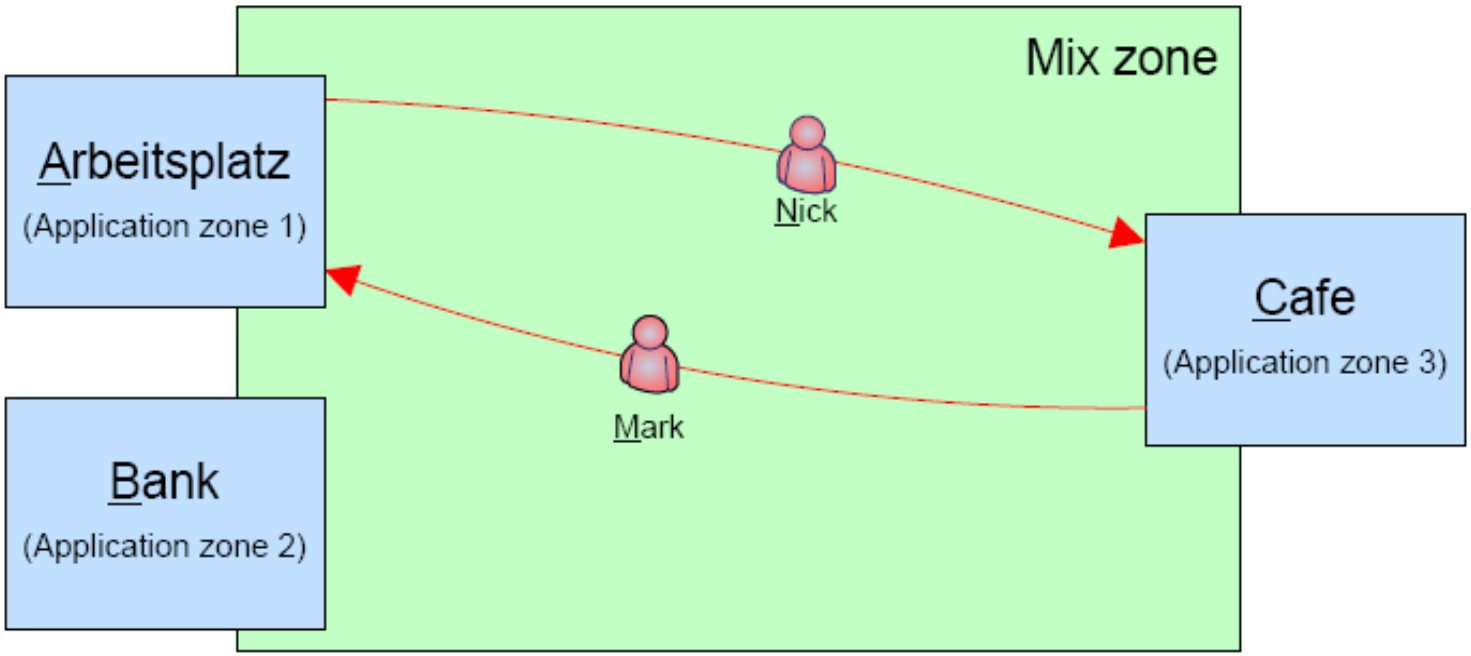
Anonymisierung

- Mix Zones
  - Orte werden unterteilt in
    - Application Zones und
    - Mix Zones
  - LBS nur in Application Zones
  - Neues Pseudonym bei betreten der Mix-Zones
  - Kein Tracking möglich
  - Nutzer nicht identifizierbar



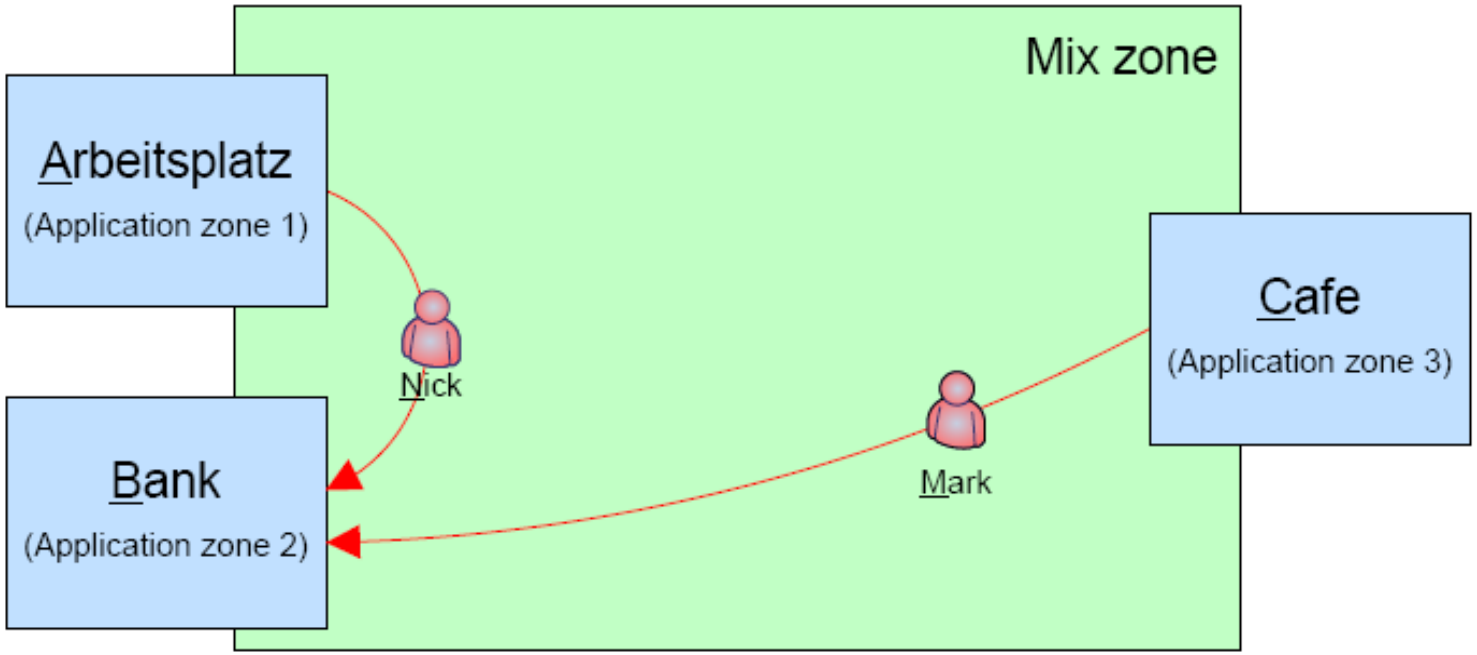
Anonymisierung

- Mix Zones - Szenario 1



Anonymisierung

- Mix Zones - Szenario 2



Anonymisierung

- Mix Zones - Diskussion:
  - Funktioniert nur, wenn sich viele Nutzer in den Mix Zones aufhalten
  - „Anonymity Set“ als Qualitätsmaß
  - „Anonymity Set“ = Anzahl Nutzer in Mix Zone pro Zeiteinheit
  - Nutzer können Mindestwert für „Anonymity Set“ bestimmen

Zusammenfassung

	Sichere Kommunikation	Privacy-Regeln	Anonymisierung Mix Zones
Ziele:	Sichere Kommunikation zwischen LBS-Anbieter und Nutzer.	Festlegen, wer, wann, in welchem Umfang, auf welche Ortsdaten zugreifen darf.	Langfristige Verfolgung der Nutzer verhindern. Gleichzeitig kurzfristige Nutzung der Dienste ermöglichen.
Probleme:	- LBS-Anbieter können personenbezogene Informationen an Dritte weitergeben	- Middleware notwendig - LBS-Anbieter können personenbezogene Informationen an Dritte weitergeben	- Middleware notwendig - Anonyme Nutzung von LBS nicht immer möglich - „Anonymity Set“ nicht zuverlässig

Ausblick

- Projekt im 3. Semester
  - „Mobiles mehrbenutzerfähiges tolles Spiel“
  - Vorläufiger Projektname: „Pervasive Gaming Framework“
  - Spielidee: Schnitzeljagd
- Was hat das mit Privacy zu tun?
  - (erstmal) wenig ☹
- Was hat das mit LBS zu tun?
  - viel ☺
- Kompromiss aus verschiedenen Themenschwerpunkten

Literatur

- Küpper, A. - Location-Based Services: Fundamentals and Operation - John Wiley & Sons Ltd., 2005
- Beresford, A. & Stajano, F. - Mix Zones: User Privacy in Location-aware Services - Proceedings of the Second IEEE Annual Conference On Pervasive Computing and Communications Workshops, 2004, 127-131
- Myles, G.; Friday, A. & Davies, N. - Preserving Privacy in Environments with Location-Based Applications - Pervasive Computing, IEEE, 2003, 2, 56-64
- Eckert, C. - IT-Sicherheit: Konzepte, Verfahren, Protokolle - Oldenbourg Wissenschaftsverlag GmbH, 2004
- ...

Diskussion

Vielen Dank!

Fragen?