Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Ausarbeitung Anwendungen 1 (AI)

Fatih Keles

Privacy in Location-based Services

Fakultät Technik und Informatik
Studiendepartment Informatik

Hamburg, 11. Juli 2006

Inhaltsverzeichnis

1 Einleitung

Mit der Verbreitung von mobilen Geräten und der Verfügbarkeit verschiedener Positionierungssysteme wie GPS steigt heutzutage das Interesse an Location-based Services (LBS). Auf der einen Seite besteht die Möglichkeit für Dienstanbieter mit LBS Geld zu verdienen, auf der anderen Seite verspricht die Technologie den Nutzern in vielen Bereichen das Leben zu vereinfachen. Bereits heute erfreuen sich beispielsweise Autonavigationsgeräte großer Beliebtheit. Bei all der Euphorie darf aber nicht außer Acht gelassen werden, dass LBS möglicher Weise ernsthafte Privacy-Risiken mit sich bringen können (Myles u. a., 2003, S. 56). Mit dieser Thematik wird sich die vorliegende Ausarbeitung auseinandersetzen.

Zu Beginn wird es eine Einführung in das Thema Privacy geben. Nach einer Begriffsdefinition werden die Privacy-Risiken erörtert, um dem Leser die besondere Bedeutung des Themas nahezubringen. Anschließend folgt eine Übersicht über die Grundprinzipien von Privacy und ein kurzer Blick in die deutsche Gesetzgebung.

Im darauf folgenden Abschnitt werden LBS thematisiert. Dort wird erörtert, was LBS sind und in welche Kategorien sie sich einteilen lassen.

In Abschnitt 4 werden die beiden Themen Privacy und LBS in Zusammenhang gebracht. Es wird erklärt, weshalb das Thema Privacy in LBS eine besondere Rolle spielt und welche Privacy-Bedrohungen es in LBS gibt. Anschließend folgt eine Einführung in die Privacy-Konzepte in LBS.

Die Ausarbeitung schließt in Abschnitt 5 mit einem Ausblick auf das nächste Semester ab.

Nicht unerwähnt bleiben soll, dass diese Ausarbeitung aufgrund des begrenzten Umfangs nur eine kurze Übersicht über die Thematik geben kann. Der Leser wird deshalb an verschiedenen Stellen auf weiterführende Literatur verwiesen.

2 Privacy

Der Begriff „Privacy“ wird im Deutschen häufig mit „Privatsphäre“ oder „Datenschutz“ übersetzt. Gemeint ist damit der Schutz der Menschen vor der Verarbeitung der persönlichen Daten (Garstka, 2003, S. 49). Hierzu findet man eine häufig zitierte Definition in (Westin, 1970).

> *Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.*

Aus dieser Definition geht hervor, dass Menschen den Anspruch haben, die Weitergabe persönlicher Informationen zu kontrollieren. Nicht umsonst gibt es große Bestrebungen, den Datenschutz mit technischen und juristischen Mitteln zu gewährleisten. Um die Sensibilität vieler Menschen bezüglich ihrer persönlichen Daten zu verstehen wird im folgenden Abschnitt auf Privacy-Risiken eingegangen.

2.1 Privacy-Risiken

Menschen sehen es als eine Bedrohung an, wenn Informationen über sie selbst ohne ihr Wissen an die Öffentlichkeit gelangen. An dieser Stelle spielt die Angst vor der Veröffentlichung intimer Kenntnisse ohne die Einwilligung des Betroffenen eine wichtige Rolle. Dies kann durch die Verzerrung des Persönlichkeitsbildes, aber auch durch das Weglassen wichtiger Details geschehen (Garstka, 2003, S.50f).

Einen potentiellen Arbeitgeber etwa könnten Informationen über Krankheiten dazu bewegen, jemanden nicht einzustellen. Durch fehlerhafte Informationen könnte man irrtümlicher Weise in das Visier staatlicher Strafverfolgungsorgane gelangen. Diese zwei Beispiele zeigen, dass die Ängste der Menschen vor dem Missbrauch persönlicher Daten durchaus berechtigt sind.

Darüber hinaus besteht die Möglichkeit verschiedene personenbezogene Daten, die unabhängig voneinander gespeichert werden, zu Verknüpfen um damit an zusätzliche Informationen zu gelangen. Diese Art des Datenmissbrauchs ist heutzutage einfacher denn je. Aufgrund der weltweiten Vernetzung über das Internet gibt es im Vergleich zu früher kaum noch örtliche und zeitliche Beschränkungen zur Nutzung und Verknüpfung von Daten (Garstka, 2003, S. 51f).

2.2 Grundprinzipien des Datenschutzes

Viele Staaten und internationale Organisationen beschlossen ab den frühen 1970er Jahren Gesetze zum Schutz der Privatspähe. Die Grundlage für alle modernen Datenschutzgesetze bildet die *„Richtlinie betreffend personenbezogene Daten in automatisierten Dateien“*, die am 14. Dezember 1990 von den Vereinten Nationen beschlossen wurde (UN1990). Sie legt im Wesentlichen folgende Grundsätze fest:

- Daten dürfen nicht verarbeitet werden, wenn sie gegen Menschenrechte verstoßen oder unter Täuschung erhoben wurden.
- Datenverarbeiter sind verpflichtet die Richtigkeit von Daten regelmäßig zu überprüfen.
- Jeder hat das Recht zu entscheiden und zu erfahren, welche Daten über ihn erhoben werden.
- Daten dürfen nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden.
- Daten, die zu einer Diskriminierung von Betroffenen führen könnten, dürfen nur unter sehr beschränkten Voraussetzungen verarbeitet werden.

2.3 Gesetzgebung in Deutschland

In Deutschland regelt das Bundesdatenschutzgesetz (BDSG) die Bestimmungen für den Datenschutz (BDSG). In § 1 des BDSG wird das Recht auf informationelle Selbstbestimmung festgelegt. Dieses Recht räumt jedem Bürger ein, selbst über die Weitergabe und Verwendung persönlicher Daten zu entscheiden. Die Verarbeitung personenbezogener Daten ist laut § 4 BDSG nur dann zulässig, wenn der Betroffene einwilligt oder ein gesetzlicher Erlaubnistatbestand vorliegt. Weiterhin regelt § 3a BDSG, dass personenbezogene Daten nur in dem tatsächlich notwendigen Umfang verarbeitet werden dürfen. § 28 BDSG legt außerdem fest, dass personenbezogene Daten nur für den Zweck verarbeitet werden dürfen, für den sie rechtmäßig erhoben wurden.

Im Rahmen dieser Ausarbeitung soll dieser kurze Einblick in die Privacy-Prinzipien und das BDSG genügen. Er sollte deutlich machen, dass sowohl die persönlichen Ängste der Menschen, als auch gesetzliche Vorgaben das Thema Privacy zu einem wichtigen Thema der Informatik machen.

Eine Einführung zum Thema Privacy kann z. B. im Aufsatz *„Informationelle Selbstbestimmung und Datenschutz: Das Recht auf Privatsphäre“* von Hansjürgen Garstka (Garstka, 2003) nachgelesen werden.

3 Location-based Services

In der Literatur gibt es bislang keine einheitliche Definition für LBS (Küpper, 2005, S. 2). Häufig werden diese jedoch als eine Untermenge der *Context-aware Services* betrachtet (Roth, 2005, S. 270). (Dey und Abowd, 2000, Kap. 3.2) beschreiben Kontextbezogenheit folgendermaßen:

> *A system is context-aware if it uses context to provide relevant information and / or services to the user, where relevancy depends on the user's task.*

Neben dem Ort nennen (Dey und Abowd, 2000, Kap. 2.3) die Zeit und die Identität und Aktivität des Benutzers als weitere Attribute der Kontextbezogenheit. Ändert sich der Ort des Benutzers hat dies oftmals Auswirkungen auf den gesamten Kontext. Beispielsweise ändern sich Faktoren, wie Temperatur, Luftverschmutzung und Lautstärke mit der Veränderung des Ortes. Aus diesem Grund spielt der Ort bei Context-aware Services eine besondere Rolle.

Oft werden LBS als Dienste beschrieben, die den Ort des Benutzers oder eines Objektes verwenden (und diesen mit weiteren Informationen verknüpfen), um den Nutzen des Dienstes zu steigern (Küpper, 2005, S. 1) und (Schiller und Voisard, 2004, S. 10). Der gesteigerte Nutzen kann z. B. darin bestehen Informationen abhängig vom Ort des Nutzers zu Filtern oder die aktuelle Position eines Zielobjektes auf einer Landkarte anzuzeigen.

Man unterscheidet zwischen reaktiven und proaktiven LBS (Lehner, 2003, S. 148). Reaktive Dienste (auch Pull-Dienste genannt) werden durch den Benutzer bewusst und explizit aufgerufen. Als Beispiel kann man sich einen Dienst vorstellen, der auf Anfrage Orte von Interesse, die sich in der Nähe des Nutzers befinden, auflistet.

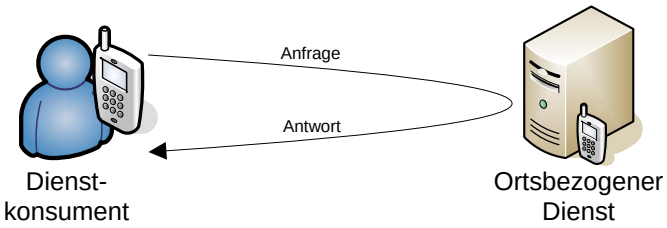

Abbildung 1: Reaktiver Dienst

Proaktive Dienste (Push-Dienste) dagegen erfordern keine explizite Anforderung durch den Benutzer. Sie werden automatisch ausgeführt sobald ein vorher definiertes Ortsereignis eintritt. Als Beispiel sei ein Informationssystem genannt, dass Touristen über eine SMS mit Informationen versorgt, wenn sie bestimmte Orte betreten. Im Gegensatz zu den reaktiven Diensten muss bei proaktiven Diensten der Nutzer permanent beobachtet werden, um das Eintreten von Ortsereignissen feststellen zu können.

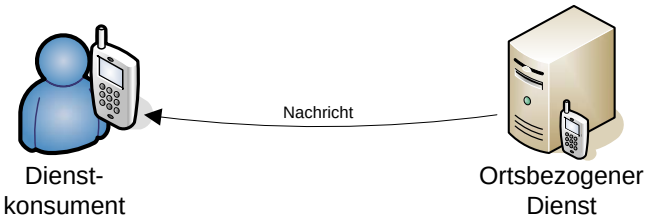

Abbildung 2: Proaktiver Dienst

Ein weiteres Unterscheidungsmerkmal stellt die Genauigkeit der Ortsinformationen dar, die ein LBS benötigt. Während einige Dienste auf wenige Meter genaue Ortsinformationen voraussetzen, reichen für andere Dienste wesentlich ungenauere Daten. Weiterhin kann man LBS daran unterscheiden, ob sie anonym nutzbar sind oder nicht.

Weitergehende Informationen zu LBS können in dem Buch *„Location-based Services: Fundamentals und Operation“* von Axel Küpper (Küpper, 2005) nachgelesen werden.

4 Privacy und Location-based Services

Aufgrund der wachsenden Verbreitung und Nutzung von LBS gewinnt die Frage nach dem Schutz persönlicher Ortsdaten immer mehr an Bedeutung. Schließlich kann ein ungenügender Schutz der persönlichen Daten zu Akzeptanzproblemen bei den Nutzern von LBS führen (Küpper, 2005, S. 257).

Die Brisanz des sog. Location-privacy liegt vor allem darin, dass man über die Kenntnis des Aufenthaltsortes einer Person auf viele weitere persönliche Daten schließen kann (Langheinrich, 2005, S. 208). Zum Beispiel ist es denkbar, über die Analyse von häufigen Aufenthaltspunkten einer Person an Informationen über Hobbies, Freunde oder politische Einstellungen zu gelangen.

Neben den persönlichen vorbehalten der Nutzer sind es die in Abschnitt 2 angesprochenen gesetzlichen Regelungen zum Datenschutz, die bei der Entwicklung und beim Einsatz von LBS nicht außer Acht gelassen werden dürfen.

4.1 Privacy-Bedrohungen in Location-based Services

Positionsinformationen sind Schlüsseldaten, ohne die LBS nicht funktionieren können und außerdem gar keinen Sinn machen. Andererseits stellen genau diese Daten ein Privacy-Risiko dar und sind zudem eine potentielle Quelle für den Missbrauch. Dieses Dilemma zeigt, dass die Anforderungen an den Schutz persönlicher Daten bei LBS noch höher anzusiedeln sind als bei herkömmlichen IT-Anwendungen (Küpper, 2005, S. 258). Vor diesem Hintergrund werden im Folgende einige Gefahren erläutert, die speziell bei LBS auftreten.

Besonders deutlich werden die Privacy-Risiken, wenn man die potentiellen Interessenten an persönlichen Ortsdaten anderer genauer betrachtet (Langheinrich, 2005, S. 210).

- *Einzelpersonen:* Dabei kann es sich z. B. um Nachbarn, Freunde oder Familienmitglieder handeln. Eine misstrauische Ehefrau etwa könnte anhand von Ortsinformationen herausfinden wollen, ob ihr Ehemann wirklich geschäftlich unterwegs war oder ein privates Date hatte. Auch kriminelle Personen, wie z. B. Einbrecher fallen in diese Kategorie.
- *Böswillige Unternehmen:* Sie könnten die Ortsdaten für vertraglich nicht vereinbarte Zwecke verwenden oder unerlaubt an andere Unternehmen weitergeben. Arbeitgeber könnten Interesse an den Freizeitaktivitäten ihrer Mitarbeiter haben. Für Banken wäre es sicherlich interessant zu wissen, in welchen Kreisen ein potentieller Kreditnehmer verkehrt.
- *Staatliche Einrichtungen:* Beispielsweise könnten Justizbehörden Straftäter aufspüren und verfolgen wollen. Genaue Ortsinformationen mit zeitlichem Bezug könnten den Behörden bei der Aufklärung von Straftaten behilflich sein. Auch ein Missbrauch der Ortsdaten durch staatliche Organe kann nicht gänzlich ausgeschlossen werden.

(Langheinrich, 2005, S. 211) beschreibt weiterhin die Möglichkeiten für Andere an persönliche Ortsinformationen zu gelangen, die nicht für sie selbst vorgesehen sind.

- *Das Durchsickern von Ortsinformationen:* Dies ist dann der Fall, wenn ein Dienst detailliertere Informationen über den Aufenthaltsort erhält, als nötig. Für einen Restaurantfinder könnte z. B. die Postleizahl des Nutzers ausreichen, um eine Liste von Restaurants in der Nähe zu ermitteln. Die Kenntnis der exakten Position des Nutzers ist nicht unbedingt notwendig.
- *Das Durchsickern von Zeitinformationen:* Häufig ist es nicht zwangsläufig nötig zusätzlich zum Ort auch die Zeit des genutzten Dienstes zu speichern. Für ein Mautsystem könnte es ausreichen, den Eintritts- und Austrittsort eines Fahrzeuges zu ermitteln, um die Maut abrechnen zu können. Werden aber zusätzlich genaue Eintritts- und Austrittszeiten ermittelt, könnte die Polizei diese Daten nutzen um Strafzettel zu schreiben, falls die betroffene Strecke in zu kurzer Zeit abgefahren wurde.
- *Das Durchsickern der Identität:* Nicht alle Dienste müssen die genaue Identität einer Person kennen. Oft ist eine anonyme Nutzung möglich. Ein Kinobetreiber z. B. braucht nicht zwangsläufig die Identität einer Person zu kennen, um sie beim Vorbeigehen an einem Kino über aktuelle Filme zu informieren.
- *Geheime Absprachen:* Wenn Ortsdaten von verschiedenen Diensten zusammengeführt werden, könnten daraus detailliertere Informationen abgeleitet werden, als vom Nutzer der Dienste gewünscht ist.
- *Unerlaubtes Abhören* Ein Angreifer könnte die Kommunikation zwischen einem Nutzer und einem Dienst abhören um so die Ortsdaten des Nutzers zu erspähen.

Die oben beschriebenen Risiken machen deutlich, dass es vielfältige Interessen und Möglichkeiten für die Nutzung persönliche Ortsinformationen anderer gibt. Die folgenden Abschnitte beschäftigen sich daher mit Konzepten, die versuchen, den Missbrauch persönlicher Ortsdaten zu verhindern.

4.2 Privacy-Konzepte in Location-based Services

In der Literatur werden folgende drei Ansätze für den Schutz von persönlichen Daten in LBS diskutiert (Küpper, 2005, S. 261).

- *Sichere Kommunikation*
- *Privacy-Regeln*
- *Anonymisierung*

Es folgt eine detaillierte Beschreibung der genannten Punkte.

4.2.1 Sichere Kommunikation

Bei diesem Ansatz geht es um die Absicherung der Kommunikationsleitung zwischen dem Dienstanbieter und dem Dienstkonsumenten. Dabei wünscht man die Gewährleistung von *Authentifikation*, *Integrität* und *Vertraulichkeit*. Vertraulichkeit bedeutet, dass auf die übertragenen Informationen nicht von Dritten zugegriffen werden kann. Die Integrität soll gewährleisten, dass der Empfänger genau die Informationen erhält, die der Sender abschickt. Authentifikation schließlich

bedeutet, dass die Teilnehmer der Kommunikation tatsächlich diejenigen sind, als die sie sich ausgeben. Die genannten Mechanismen können z. B. über eine verschlüsselte Verbindung und gängige Authentifikationstechniken[1] sichergestellt werden (Eckert, 2004).

4.2.2 Privacy-Regeln

Über eine sichere Kommunikationsleitung kann gewährleistet werden, dass keine Unbefugten auf die übertragenen Informationen zugreifen oder sie verändern. Jedoch wird nicht geregelt, in welchem Umfang einzelne Dienstanbieter auf die Ortsdaten zugreifen dürfen (Küpper, 2005, S. 262). An dieser Stelle kommen die Privacy-Regeln ins Spiel. Sie sollen regeln, wer, wann, in welchem Umfang auf welche Ortsdaten zugreifen darf.

Im einfachsten Fall könnte man den LBS-Nutzer bei jeder Dienstanfrage um eine Bestätigung bitten (Myles u. a., 2003, S. 56). Dadurch würde der Nutzer des Dienstes jedoch zu häufig gestört werden. Aus diesem Grund versucht man durch die Einführung von Privacy-Regeln den Bestätigungsprozess zu automatisieren.

Laut (Cuellar, 2002, S. 188) sind Privacy-Regeln Zusicherungen dafür, dass eine bestimmte Menge von Informationen an bestimmte Personen oder Dienste nur unter bestimmten Bedingungen freigegeben werden. Das folgende Beispiel stellt Privacy-Regeln für den Studenten, Stefan, in natürlichsprachlicher Form auf:

Stefan ist Informatik-Student und übt gleichzeitig eine Arbeit als studentische Hilfskraft aus. Er ist manchmal beruflich unterwegs um Kunden zu besuchen und erlaubt seiner Freundin die Stadt zu erfahren, in der er sich gerade aufhält. Sein Arbeitgeber soll sogar auf genaue Positionsinformationen von Stefan zugreifen dürfen, aber nur wenn Stefan gerade bei der Arbeitsstelle ist oder einen Kunden besucht und nur während der Arbeitszeiten. Stefans Kommilitonen dürfen über einen Buddy-Finder-Dienst seinen genauen Aufenthaltsort erfahren, weil er sich häufig mit ihnen zum Lernen trifft, jedoch nur wenn Stefan an der Uni ist. Stefans Freunde dürfen die Stadt erfahren, in der er sich befindet, aber nur, wenn Stefans Freundin nicht in der Nähe ist.

Diese Regeln zeigen, dass es eine Reihe von Bedingungen gibt, die bei Privacy-Regeln berücksichtigt werden müssen. (Myles u. a., 2003, S. 57) nennen folgende Typen von Bedingungen:

- *Aktoren:* Die Aktoren können z. B. Unternehmen oder Personen sein. Stefan erlaubt beispielsweise seiner Freundin, seinem Arbeitgeber und seinen Kommilitonen den Zugriff auf seine Ortsdaten.
- *Dienstarten:* Dienstarten können z. B. Navigationsdienste oder Buddy-Finder-Dienste sein. Beispielsweise nutzt Stefan einen Buddy-Finder-Dienst um sich mit Kommilitonen zum Lernen zu verabreden.
- *Zeitliche Beschränkung:* Oft wird der Zugriff auf Ortsdaten zeitlich begrenzt. Stefans Arbeitgeber z. B. darf auf seine Positionsinformationen nur während der Arbeitszeiten zugreifen.
- *Örtliche Beschränkung:* Auch eine örtliche Beschränkung ist denkbar. Stefans Kommilitonen etwa dürfen über den Buddy-Finder-Dienst seinen Aufenthaltsort nur dann erfahren, wenn Stefan an der Uni ist.

[1] Gängige Authentifikationstechniken sind z. B. das Challenge-response-Verfahren oder die Authentifikation durch Benutzerzertifikate.

- *Genauigkeit der Ortsinformationen:* Während Stefan seinem Arbeitgeber den Zugriff auf seine exakte Position erlaubt, darf seine Freundin nur die Stadt kennen, in der er sich befindet.
- *Bedingungen in Abhängigkeit vom Kontext:* Der Kontext kann z. B. der Gesundheitszustand einer Person, das aktuelle Wetter oder die An- bzw. Abwesenheit von anderen Personen sein. Im obigen Beispiel erlaubt Stefan seinen Freunden den Zugriff auf seine Ortsinformationen nur, wenn seine Freundin nicht in seiner Nähe ist.

Bei den genannten Bedingungstypen handelt es sich nicht um eine vollständige Auflistung. Vielmehr soll ein Eindruck darüber vermittelt werden, dass es viele unterschiedliche Arten von Bedingungstypen gibt. Zusätzlich kann man sich z. B. Regeln vorstellen, die die Einhaltung von gesetzlichen Vorgaben überprüfen.

Wie auch am obigen Beispiel zu erkennen ist, werden die genannten Regeln häufig miteinander verknüpft. Stefans Arbeitgeber darf auf seine Ortsinformationen nur dann zugreifen, wenn er sich in seiner Arbeitsstelle befindet oder bei einem Kunden ist und auch dann nur innerhalb der Arbeitszeiten. Hier gibt es demnach sowohl eine örtliche, als auch eine zeitliche Beschränkung. Solche Verknüpfungen können wesentlich komplexer sein als in dem genannten Beispiel. Passt man nicht auf sind sogar widersprüchliche Regeln möglich. Laut (Küpper, 2005, S. 263f) müssen Privacy-Regeln deshalb nach wohlgeformten Regeln organisiert werden können. Diese müssen die Festlegung von Prioritäten, Abarbeitungsreihenfolgen und Beziehungen zwischen den einzelnen Regeln ermöglichen.

Aufbauend auf den genannten Überlegungen machen (Myles u. a., 2003) in ihrem Aufsatz *„Preserving Privacy in Environments with Location-Based Applications“* einen Vorschlag für die Realisierung eines Konzeptes basierend auf Privacy-Regeln. Ein Wesentliches Element sind Validatoren, die die Privacy-Anforderungen der Nutzer überprüfen. Ein sehr einfacher Validator ist z. B. der *User Confirmation* Validator, der eine explizite Bestätigung durch den Nutzer fordert. Weitere Typen von Validatoren sind beispielsweise *Limit Time* oder *Limit Location* Validatoren, die die zeitlichen oder örtlichen Grenzen für die Nutzung eines Dienstes festlegen. Auf weitere Details des genannten Aufsatzes kann an dieser Stelle nicht weiter eingegangen werden. Der Leser sei auf die Originalliteratur verwiesen.

4.2.3 Anonymisierung

Privacy-Regeln sind nur dann sicher, wenn alle LBS-Teilnehmer vertrauenswürdig sind (Küpper, 2005, S. 265). Es kann nicht ausgeschlossen werden, dass einer der Beteiligten Informationen an unbefugte Dritte weitergibt. Aus diesem Grund gibt es eine Reihe von Arbeiten, die sich mit der Anonymisierung von Ortsinformationen beschäftigen. (Cuellar, 2002, S. 187ff) unterscheidet dabei zwischen der *Abstraktion vom Identifikator* und der *Abstraktion vom Inhalt*. Bei der Abstraktion vom Identifikator wird die tatsächliche Id eines LBS-Teilnehmers durch eine Anonyme Id ersetzt. Mit Abstraktion vom Inhalt meint man die Reduzierung der Genauigkeit von Zeit- und Ortsinformationen. Alastair R. Beresford und Frank Stajano stellten 2003 das Konzept der sog. *Mix Zones* vor. Anhand dieses Konzeptes wird die Idee der Anonymisierung im Folgenden beispielhaft vorgestellt.

Das Mix Zones Konzept fällt in die Kategorie der Abstraktion vom Identifikator. Die Grundidee besteht darin, Orte in *Application Zones* und *Mix Zones* zu unterteilen. Die Nutzung von LBS

findet nur in den Application Zones statt. In den Mix Zones dagegen, gibt es keinerlei LBS-Kommunikation. Jedes Mal wenn ein LBS-Nutzer eine Mix Zone betritt erhält er von einer Middleware ein neues Pseudonym. Alle Nutzer in solch einer Mix Zone sind sozusagen „gemixt“. Sie können nicht mehr ohne weiteres verfolgt werden, da sich die Nutzer bei jeder LBS-Applikation mit einem anderen Pseudonym anmelden. Die Verwendung von Pseudonymen führt außerdem dazu, dass die Nutzer von den Dienstanbietern nicht identifiziert werden können. Aus Privacy-Sicht stellt dies ebenfalls einen Vorteil dar.

Laut (Beresford und Stajano, 2004, Kap. 2) besteht das Ziel des Mix Zones Ansatzes darin, eine langfristige Verfolgung der Nutzer durch die Dienstanbieter zu verhindern und gleichzeitig die kurzfristige Nutzung von LBS zu ermöglichen. Jedoch gibt es eine Reihe von Problemen, die diesem Ziel entgegenstehen.

Anhand von zwei Szenarien werden nachfolgend mögliche Probleme des Mix Zones Ansatzes diskutiert. Abbildung 3 zeigt hierzu eine Beispielanordnung für drei Application Zones und einer Mix Zone.

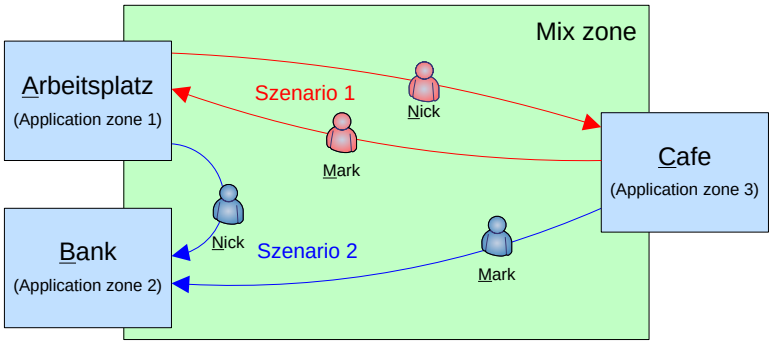

Abbildung 3: Eine Beispielanordnung für den Mix Zones Ansatz. Während der Arbeitsplatz (A) und die Bank (B) dicht beieinander liegen, liegt das Cafe (C) etwas weiter entfernt.

Szenario 1:
Angenommen ein Nutzer N befindet sich in A und ein Nutzer M in C. N verlässt A um nach C zu gelangen und gleichzeitig geht M von C nach A. Die Pseudonyme von N und M ändern sich jeweils in der Mix Zone. Ein Beobachter dürfte Aufgrund der Änderung der Pseudonyme kein Bewegungsprofil erstellen können. Er sieht nur, dass irgend jemand A und irgend jemand anderes C verlässt. Nach einer Weile betritt wieder irgend jemand A und jemand anderes C. Wer diese Personen sind ist unbekannt. Jedoch kann der Beobachter annehmen, dass derjenige, der C betreten hat wahrscheinlich derjenige sein muss, der zuvor A verlassen hat und umgekehrt. Der Grund hierfür liegt darin, dass der Beobachter davon ausgeht, dass es wahrscheinlicher ist, dass A und C aneinander vorbeigehen um zur jeweils gegenüberliegenden Application Zone zu gelangen, anstelle wieder umzukehren. Auf diese Weise wäre es einem Beobachter also möglich trotz des Wechsels der Pseudonyme in der Mix Zone ein Bewegungsprofil von N und M zu erstellen.

Szenario 2:
Es wird wieder angenommen, dass sich N in A befindet und M in C. N geht diesmal von A nach B und gleichzeitig geht M von C nach B. Weil sich die Pseudonyme von N und M jeweils in der Mix Zone ändern dürfte ein Beobachter keine Schlüsse über den zurückgelegten Weg von N und

M ziehen können. Da aber der Weg von A nach B kürzer ist als der von C nach B könnte ein Beobachter annehmen, dass N B vor M betreten hat und somit derjenige sein muss, der zuvor in A gewesen ist. Entsprechend müsste M derjenige gewesen sein, der zuvor in C war. Auch nach diesem Szenario kann ein Beobachter also ein Bewegungsprofil von N und M erstellen.

Die beiden Szenarien machen eine wesentliche Schwäche des Mix Zones Ansatzes deutlich. Das Erstellen von Bewegungsprofilen einzelner Nutzer kann nur dann wirksam verhindert werden, wenn sich immer ausreichend viele Nutzer in der Mix Zone befinden. (Beresford und Stajano, 2003, S. 50) führen deshalb den Begriff *Anonymity Set* als Qualitätsmaß ein. Der *Anonymity Set* für eine Mix Zone errechnet sich dabei aus der Summe der Nutzer, die sich in einer bestimmten Zeitspanne gleichzeitig in der Mix Zone aufhalten. LBS-Nutzer können anhand des *Anonymity Sets* entscheiden, ob sie einen LBS nutzen wollen oder nicht. Beispielsweise könnte ein Nutzer festlegen, dass er einen LBS nur dann nutzt, wenn der *Anonymity Set* der Mix Zones in der Umgebung des LBS mindestens 10 beträgt. Dies setzt natürlich voraus, dass die Middleware in der Lage ist, aus historischen Daten den durchschnittlichen *Anonymity Set* der Mix Zones zu errechnen. Ein Problem bleibt jedoch, dass niemand garantieren kann, dass der aktuelle *Anonymity Set* tatsächlich so hoch ist wie der Durchschnittliche.

Abschließend seien noch zwei weitere Einschränkungen des Mix Zones Ansatzes genannt. Zum Einen kann dieser Ansatz nur dann funktionieren, wenn eine vertrauenswürdige Middleware vorhanden ist, die die Organisation von Application Zones und Mix Zones übernimmt (Beresford und Stajano, 2004, Kap. 2). Zum Anderen gibt es LBS, die die Identifikation der Nutzer voraussetzen und daher mit Pseudonymen nicht oder nur eingeschränkt funktionieren können[2]. Dies ist ein allgemeines Problem vieler Ansätze, die im Bereich der Anonymisierung anzusiedeln sind (Beresford und Stajano, 2003, S. 49).

Wie bereits oben erwähnt kann man das Konzept der Mix Zones in die Kategorie „Abstraktion vom Identifikator“ einordnen. Ein Konzept für die Kategorie „Abstraktion vom Inhalt“ schlagen z. B. (Gruteser und Grunwald, 2003) in ihrer Ausarbeitung *„Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking“* vor. Auf dieses Konzept wird an dieser Stelle nicht eingegangen. Der interessierte Leser sei auf die genannte Ausarbeitung verwiesen.

5 Fazit & Ausblick

Die vorliegende Ausarbeitung sollte einen Überblick über die Privacy-Problematik in Location-based Services geben. Es wurden potentielle Gefahren aufgezeigt und mögliche Lösungsansätze diskutiert. Dem Leser sollte deutlich geworden sein, dass die Einbeziehung der Privacy-Problematik ein wichtiger und integraler Bestandteil bei der Entwicklung von LBS sein sollte. Privacy-Überlegungen sollten von Anfang in die Designentscheidungen einfließen und nicht nachträglich aufgesetzt werden.

Es ist geplant, im nächsten Semester in einer Gruppe von sechs Masterstudenten ein Framework für Spiele im LBS-Umfeld zu entwickeln. Unter dem Arbeitstitel „Pervasive Gaming Framework“ soll eine Software entstehen, die die Entwicklung von LBS-Spielen unterstützt und vereinfacht. Es ist vorgesehen, Softwarekomponenten, die bei der Entwicklung von LBS-Spielen häufig benötigt werden, zu identifizieren und diese in dem genannten Framework zur Verfügung zu stellen.

[2] Ein Beispiel sind Community-Dienste, die für jeden Nutzer Profile anlegen und diese den Nutzern bei jeder Anmeldung wieder zuordnen können müssen.

Prototypisch soll ein konkretes Spiel auf Grundlage des entwickelten Frameworks implementiert und getestet werden.

In die Entwicklung des Frameworks werden die speziellen Interessensgebiete der Mitglieder der Entwicklergruppe einfließen. Dabei möchte ich mich schwerpunktmäßig mit der hier diskutierten Privacy-Problematik und dem Thema Location-based Services im Allgemeinen befassen. Die oben angesprochene Integration von Privacy-Überlegungen in die Architektur des Frameworks sind mir dabei ein besonderes Anliegen.

Literatur

[BDSG] *Bundesdatenschutzgesetz (BDSG)*. – URL http://www.gesetze-im-internet.de/bdsg_1990/. – Überprüft am 08.05.2006

[UN1990] *United Nations guidelines concerning computerized personal data files*. – URL http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm. – Überprüft am 08.05.2006

[Beresford und Stajano 2004] BERESFORD, Alastair ; STAJANO, Frank: Mix Zones: User Privacy in Location-aware Services. In: *Proceedings of the Second IEEE Annual Conference On Pervasive Computing and Communications Workshops* IEEE (Veranst.), 2004, S. 127–131

[Beresford und Stajano 2003] BERESFORD, Alastair R. ; STAJANO, Frank: Location Privacy in Pervasive Computing. In: *Pervasive Computing, IEEE* 2 (2003), S. 46–55

[Cuellar 2002] CUELLAR, Jorge R.: *Geographic Location in the Internet*. Kap. Location Information Privacy, S. 179–208, Kluwer Academic Publishers, 2002. – ISBN 1-4020-7097-7

[Dey und Abowd 2000] DEY, Anind K. ; ABOWD, Gregory D.: Towards a Better Understanding of Context and Context-Awareness. In: *Workshop on The What, Who, Where, When, and How of Context-Awareness, as part of the 2000 Conference on Human Factors in Computing Systems (CHI 2000)*, April 2000

[Eckert 2004] ECKERT, Claudia: *IT-Sicherheit: Konzepte, Verfahren, Protokolle*. München : Oldenbourg Wissenschaftsverlag GmbH, 2004. – ISBN 3-486-20000-3

[Garstka 2003] GARSTKA, Hansjürgen: Informationelle Selbstbestimmung und Datenschutz: Das Recht auf Privatsphäre. In: SCHULZKI-HADDOUTI, Christiane (Hrsg.): *Bürgerrechte im Netz* Bd. 382. Bundeszentrale für politische Bildung, 2003, S. 48–70

[Gruteser und Grunwald 2003] GRUTESER, Marco ; GRUNWALD, Dirk: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: *International Conference on Mobile Systems, Applications and Services* ACM/USENIX (Veranst.), 2003

[Küpper 2005] KÜPPER, Axel: *Location-Based Services: Fundamentals and Operation*. West Sussex : John Wiley & Sons Ltd., 2005. – ISBN 0-47009-231-9

[Langheinrich 2005] LANGHEINRICH, Marc: *Personal Privacy in Ubiquitous Computing: Tools and System Support*, Swiss Federal Institute of Technology Zurich, Dissertation, 2005

[Lehner 2003] LEHNER, Franz: *Mobile und drahtlose Informationssysteme: Technologien, Anwendungen, Märkte*. Berlin, Heidelberg : Springer-Verlag, 2003. – ISBN 3-540-43981-1

[Myles u. a. 2003] MYLES, Ginger ; FRIDAY, Adrian ; DAVIES, Nigel: Preserving Privacy in Environments with Location-Based Applications. In: *Pervasive Computing, IEEE* 2 (2003), S. 56–64

[Roth 2005] ROTH, Jörg: *Mobile Computing: Grundlagen, Technik, Konzepte*. Heidelberg : dpunkt.verlag GmbH, 2005. – ISBN 3-89864-366-2

[Schiller und Voisard 2004] SCHILLER, Jochen H. (Hrsg.) ; VOISARD, Agnès (Hrsg.): *Location-Based Services*. Morgan Kaufmann, 2004. – ISBN 1-55860-929-6

[Westin 1970] WESTIN, Alan F.: *Privacy and Freedom*. New York : Atheneum, 1970. – ISBN 0-370-01325-5