한국항행학회 논문지 제13권 제2호 2009년 4월

위치기반 서비스의 프라이버시 위협 요소 분석 및 보안 대책에 관한 연구

Analysis of Privacy threats and Security mechanisms on Location-based Service

오수현*, 곽진**

Soo-Hyun Oh*, Jin Kwak**

요 약

위치기반 서비스에서 활용되는 위치정보는 사용자에게 편의성을 제공한다는 취지와는 다르게 서비스 제공자의 의지에 따라 얼마든지 악용될 수 있다는 위험성을 가지고 있다. 위치정보가 악용될 경우에는 개인의 위치추적이 가능하기 때문에 개인의 프라이버시를 침해할 수 있으며 위치정보의 오용으로 인해 사용자에게 큰 피해를 가져올 수도 있다. 본 논문에서는 위치정보가 수집되고 활용되는 과정을 위치정보의 수집, 이용, 제공, 보관, 파기 등과 같이 생명주기별로 분류하고, 이에 따른 프라이버시 침해 요인을 분석한다. 그리고 위치정보 프라이버시 보호를 위한 정보보호 기술을 운영기술과 정책 및 관리 기술로 분류하여 분석하고, 분석 결과를 바탕으로 생명주기별 침해 요인에 따른 프라이버시 보호 방안을 제시하고자 한다.

Abstract

A location information used in LBS provides convenience to the user, but service provider can be exploited depending on how much risk you have. Location information can be exploited to track the location of the personal privacy of individuals because of the misuse of location information may violate the user can import a lot of damage. In this paper, we classify the life cycle of location information as collection, use, delivery, storage and destroy and analyze the factors the privacy is violated. Furthermore, we analyze information security mechanism is classified as operation mechanism and policy/management mechanism and propose a security solutions of all phase in life cycle.

Key words : Location-based Service, Location Information, , Privacy, Life Cycle, Security Mechanisms

I. 서 론

최근 들어 이동통신 기술의 발전과 함께 위치정보는 개인, 기업 및 공공분야에 이르기까지 다양한 형태로 활용되고 있다. 휴대폰을 이용하여 친구의 위치를 찾아주는 서비스, 관광지의 정보를 찾아 길안내를 해주는 서비스, 기업의 물류 및 차량관리 서비스, 그리고 긴급구조를 위한 재난·재해 구조 서비스 등을

* 호서대학교 정보보호학과(Department of Information Security, Hoseo University)
** 순천향대학교 정보보호학과(Department of Information Security Engineering, Soonchunhyang University)
· 교신저자(Corresponding Auther) : 곽진
· 투고일자 : 2009년 3월 20일
· 심사(수정)일자 : 2009년 3월 23일 (수정일자 : 2009년 4월 8일)
· 게재일자 : 2009년 4월 30일

대표적인 예라 할 수 있다[1][2].

위치기반 서비스에서 활용되는 위치정보는 특별한 개인정보로, 이름이나 주민등록번호와 같이 이용자가 직접 입력한 일반적인 개인정보와는 다른 특성을 가지고 있다. 따라서 위치기반 서비스에서 활용되는 위치정보는 사용자에게 편의성을 제공한다는 취지와는 다르게 서비스 제공자의 의지에 따라 얼마든지 악용될 수 있다는 위험성을 가지고 있다. 위치정보가 악용될 경우에는 개인의 위치추적이 가능하기 때문에 개인의 프라이버시를 침해할 수 있으며, 위치정보의 오용으로 인해 사용자에게 큰 피해를 가져올 수도 있다. 그러므로 위치기반 서비스가 보다 활성화되기 위해서는 위치정보의 보호를 통한 사용자의 프라이버시 보호가 선결되어야 한다[3].

따라서 본 논문에서는 위치정보가 수집되고 활용되는 과정을 위치정보의 수집, 이용, 제공, 보관, 파기 등과 같이 생명주기별로 분류하고, 이에 따른 프라이버시 침해 요인을 분석한다. 그리고 위치정보 프라이버시 보호를 위한 정보보호 기술을 운영기술과 정책 및 관리 기술로 분류하여 분석하고, 분석한 결과를 바탕으로 위치정보의 생명주기별 침해 요인에 따른 프라이버시 보호 방안을 제시하고자 한다.

Ⅱ. 관련 연구

2-1 위치정보의 개요

위치정보 법에서는 개인 위치정보를 특정한 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로 전자적으로 수집된 것으로 정의하고 있다. 개인 위치정보는 특정인의 개인정보라 할 수 있으며, 개인이나 사물의 위치를 파악할 경우에는 이를 통해서 그 개인의 활동영역과 내용을 파악하거나 추측할 수 있다. 이처럼 개인의 활동영역과 내용이 파악되는 경우에는 개인의 행동에 대한 자유가 침해될 가능성이 있다. 예를 들어, 개인이 휴대하고 사용하고 있는 휴대폰과 같은 모바일 단말기나 개인휴대 정보단말기 등을 이용하여 위치정보를 파악하는 경우 축척되는 개인의 위치정보는 그 사용자의 생활패턴이나 활동영역을 포괄하는 정보가 될 수 있다[4].

특히, 위치정보만으로는 특정 개인의 위치를 알 수 없다 하더라도 다른 정보들과 결합하여 특정 개인의 위치를 알 수 있는 경우에는 개인 위치정보에 해당한다고 할 수 있다. 위치정보는 시간의 흐름에 따라 계속적으로 변화하는 동적인 특성을 가지고 있으며, 위치정보의 변경여부나 변경내용, 변경시간, 변경기록 등의 내용을 포함하게 된다.

2-2 위치기반 서비스

위치기반 서비스(LBS : Location Based Service)는 '사용자에게 부가적인 가치를 제공하기 위해 모바일 단말기의 위치 정보와 타 정보를 결합하는 네트워크 기반의 서비스'로 정의할 수 있다. 또한, 정보통신정책연구원(KISDI)은 관련 보고서를 통해 측위기술 및 응용 애플리케이션에 대해 보다 강조한 '위치확인기술을 이용해 이용자의 위치를 파악하고 이와 관련된 애플리케이션을 부가한 서비스' 라고 정의하고 있다[5]. LBS 기술은 휴대 단말의 위치를 파악하는 위치인식 기술과 핵심 기반기술을 제공하는 위치기반 서비스 플랫폼 기술, 그리고 다양한 LBS 응용을 제공하기 위한 위치기반 서비스 공통기술과 위치기반 서비스 단말 및 응용서비스 기술로 구성된다[6].

Ⅲ. 위치정보의 생명주기

3-1 위치정보 시스템 아키텍처

위치정보의 수집과 위치기반 서비스를 제공하기 위해 사용되는 위치정보 시스템은 서비스 자체를 제공하기 위한 시스템들과 프라이버시를 보호하기 위한 시스템들, 그리고 각 시스템들 간의 상호운영을 위한 프로토콜들로 구성된다. 그림 1은 위치정보 시스템을 구성하는 기본 요소들의 아키텍처를 나타낸다.

그림 1과 같이 위치정보 시스템은 위치정보 타겟, 위치 프라이버시 규칙 생성자, 위치결정 시스템과 위치정보 서버, 위치기반 서비스 제공자, 위치정보 취득자, 위치 프라이버시 규칙서버, 위치정보 제공로그

서버, 위치 스토리지 등으로 구성된다.

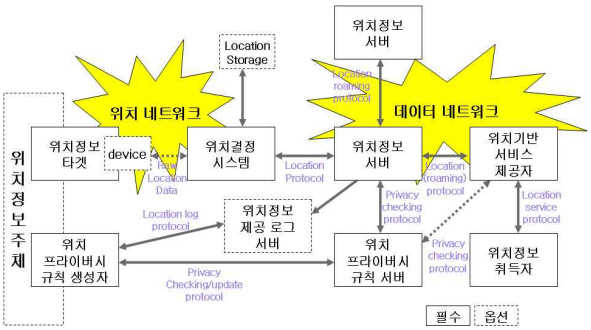

그림 1. 위치정보 시스템과 프라이버시 보호 아키텍처
Fig 1. Location information system and privacy protection archutecture

3-2 위치정보의 생명 주기

본 논문에서는 위치정보의 생명주기를 수집, 이용 및 제공, 보관 및 파기 단계로 나누어 분석한다.

(1) 수집 단계

수집단계는 서비스 제공자가 서비스 이용자의 위치정보를 수집하는 단계로, 수집되는 정보는 위치정보 서비스 가입 시 서비스 제공자가 이용자에게 요구하거나 이용자의 개인정보를 이용하여 생성하는 정보이다. 위치정보 수집의 기본 원칙은 서비스 목적을 달성하는데 필요한 최소한의 범위 내로 제한되어야 하며 반드시 정보주체의 동의를 얻어야 함을 기본 원칙으로 한다.

(2) 이용 및 제공 단계

수집 단계에서 수집된 개인정보는 서비스 이용자에 대한 인증 및 부가 서비스를 위해 이용되며, 필요에 의해 제 3자에게 제공될 수 있다. 제 3자에게 제공할 경우에는 서비스 제공자의 위치정보 보호정책에 따라야 한다. 위치정보는 정보주체의 동의가 있거나 법률의 규정에 의한 경우를 제외하고는 사전에 정보주체에게 고지한 이용목적 외의 다른 목적으로 사용되거나 타인에게 제공, 공유, 판매되어서는 안 된다.

(3) 보관 및 파기

보관 및 파기 단계는 서비스 제공자가 서비스 이용자의 개인정보 및 위치정보를 저장하고 이를 관리하는 단계이다. 이 단계에서는 수집단계에서 수집된 개인정보와 위치정보를 데이터베이스에 저장하고 허가받은 자만이 해당 개인의 개인정보와 위치정보에 접근할 수 있는 권한제어가 필요하다. 또한, 서비스 이용자가 서비스 탈퇴를 요청하였을 경우 명시되어 있는 일정기간 동안만 해당 정보를 보유하고 관리기간 종료 시 파기해야 한다.

Ⅳ. 위치기반 서비스 침해 위협

4-1 위치정보 시스템 공격의 동기

위치정보 시스템 공격자의 가장 명백한 동기는 비공개 위치 정보를 유지하기 바라는 위치정보 주체의 위치를 알아내는 것이다. 이는 비 인증된 위치정보 취득자에 한정된 것은 아니며, 위치정보를 전달받도록 인증된 위치정보 취득자에 의해서도 발생할 수 있다. 위치정보 시스템의 공격 동기를 공격자 유형별로 분류하면 표 1과 같다.

표 1. 위치정보 시스템 공격자의 동기
Table 1. Motives of attacker on LBS

공격자	공격 동기
비인증 취득자	대상 위치정보 주체의 위치를 파악
인증된 취득자	허용된 정확도 보다 높은 정확도의 위치 정보 획득 위치정보를 누출하거나 동의된 것 이상 축적
Whoever	특정 주체의 위치정보가 배포되는 것을 막는 경우 위치정보를 수정하거나 파괴하고자 하는 경우 허용되지 않은 제3자에게 redirect하고자 하는 경우 시스템 자체를 멈추게 하고자 하는 경우

4-2 위치정보 프로토콜의 위협 분석

위치정보 기반 서비스에서 발생할 수 있는 대표적인 보안 위협은 다음과 같다. 이는 RFID 기반 서비스와 같은 유비쿼터스 네트워크 환경에서 발생하는 위협들과 유사하지만, 공격 대상이 되는 정보가

위치정보와 같은 민감한 개인정보이므로 이에 대한 보안 대책이 필수적으로 요구된다[7][8].

(1) 도청 또는 가로채기

가장 일반적인 공격 방법은 위치결정 시스템과 위치정보 서버 사이의 연결이나 위치정보 서버와 위치기반 서비스 제공자 사이의 연결 중의 하나를 도청하거나 패킷을 가로채는 방법이다. 또한 공격자는 필터링되지 않은 위치 정보를 수신하기 위하여 위치정보 서버에게 중재자의 흉내를 내도록 시도할 수도 있으며, 반대로 공격자는 위치정보 주체에 의해 운반된 위치결정 시스템에게 위치정보 서버로 위장할 수 있고 위치 프라이버시 규칙 생성자로도 위장할 수 있다.

(2) 신분 위장(Identity Spoofing)

공격자는 위치결정 시스템과 위치정보 서버사이의 네트워크 연결에서 패킷 트래픽을 위장하도록 시도할 수 있다. 특히, 서비스 거부(denial-of-service) 공격과 같은 몇몇 다른 수단에 의하여 위치결정 시스템이 자신의 메시지를 위치정보 서버에게 제출할 수 없게 되었을 경우 좀 더 유효한 공격이 된다. 또한 공격자는 위치정보 서버로부터 위치기반 서비스 제공자까지 트래픽을 위장하도록 시도할 수 있다.

(3) 정보 수집(Information Gathering)

도청과 가로채기는 공격자가 시간이 흐름 따라 점점 더 많은 데이터를 수집하기 때문에 트래픽 분석 위협을 야기할 수 있다. 트래픽 분석 위협은 네트워크를 통해 전송되는 데이터 패킷들로부터 위치정보 주체와 관련된 다양한 프라이버시 정보를 침해할 수 있다. 여기에는 위치기반 서비스 참여자들 사이에 위치정보를 주고받는 관계 또는 특정 위치의 빈발성 분석에 의한 장소의 특성 파악 등이 포함된다.

(4) 서비스 거부(Denial of Service)

위치정보 시스템의 공격자들은 단지 특정한 사용자들을 목표로 하기 보다는 오히려 위치정보 서버에 대한 서비스 거부 공격을 시도할 것이다. 많은 위치기반 서비스 시나리오에서 위치정보 서버가 많은 디바이스들을 위해 위치 정보에 대한 접근을 관리하는 핵심적인 역할을 하기 때문에 위치정보 서버에 대한 공격은 위치기반 서비스에 전반적인 영향을 끼칠 수

표 2. 위치정보의 프라이버시 침해 유형 및 요인
Table 2. Privacy infringement types and factors of location information

생명주기	프라이버시 침해 유형	프라이버시 침해 요인
수집단계	부적절한 접근 및 수집	- 목적에 명시되어 있지 않은 개인정보와 위치정보의 수집 - 목적에 명시되어 있다 하더라도 이용자의 사전 동의없는 수집
이용 및 제공단계	악의적인 위치정보 분석(악의적 모니터링)	- 악의적인 목적으로 서비스 이용자의 위치정보 수집을 통한 이용자의 이동 경로 분석 - 부적절한 모니터링을 통한 개인정보 침해에 대한 위협
	부적절한 위치정보의 제공	- 개인정보보호 정책에 명시되지 않은 위탁사업자나 제 3서비스 제공자에게 개인정보 제공 - 개인정보보호정책에 명시되지 않은 개인정보 항목 제공 - on/off line으로 개인정보를 제 3자에게 양도하는 등 불법적 거래 - 이용자의 동의없이 특정 이용자의 위치 정보를 제 3자에게 제공
	원하지 않는 마케팅 수단으로의 활용	- 보유한 개인정보와 위치정보를 바탕으로 사전 동의를 거치지 않고 상품 광고나 광고성 정보를 제공하는 경우
보관 및 파기단계	부적절한 저장	- 안전성이 보장되지 않은 시스템에 개인정보 및 위치정보가 저장 - 법에서 명시한 보유 기간 이후에도 개인정보 및 위치정보를 보존
	개인정보와 위치정보의 노출	- 이용자의 동의없이 개인정보와 위치정보를 노출하는 경우 - 권한관리 또는 시스템/서비스 오류로 인해 정보가 노출되는 경우 - 관리자 및 이용자의 실수로 정보를 노출하는 경우 - 이용자의 위치정보가 권한이 없는 제 3자에게 노출이 되는 경우
	관리기간 이후 저장	- 보유기간이 경과한 후에도 개인정보 및 위치정보가 파기되지 않는 경우
	부적절한 위치정보 파기	- 관리 기간이 만료되거나 이용자가 서비스를 더 이상 원하지 않는데도 정보를 파기하지 않은 경우 - 개인정보가 저장된 하드디스크의 저장 정보를 삭제하지 않고 그대로 방치하는 경우 - 자석식 소거기나 소각기 등을 이용하지 않고 포맷하는 경우

있다. 위치 정보의 생명주기의 각 단계별 프라이버시 침해 유형 및 주요 요인은 표 2와 같다.

Ⅴ. 위치정보 프라이버시 보호 방안

5-1 프라이버시 보호를 위한 정보보호 기술

(1) 운영 기술

운영기술은 위치기반 서비스 제공을 위해 수집한 개인정보와 위치정보가 실제 운영되는 동안 즉, 위치정보 및 개인정보의 송·수신, 제공 등의 과정에서 사용되는 정보보호 기술을 말한다. 운영기술은 프라이버시 필터링 기술, 프라이버시 스캐닝 기술, 개인정보보호 통신기술, 개인정보보호 저장기술 등을 통해서 제공할 수 있다. 위치정보 프라이버시 보호를 위한 운영 기술은 표 3과 같다.

(2) 정책/관리 기술

정책/관리기술은 서비스 제공자의 개인 정보보호 정책을 효과적으로 표현하여 이를 서비스 이용자와 커뮤니케이션 하고 서비스 제공자 및 서비스 이용자 내부에서 개인정보보호 정책에 따라 운영되도록 관리하는 기술을 의미한다. 개인 정보보호 정책기술은 XML 기반의 P3P 정책과 HTML 기반 기술이 있고, 개인정보보호 관리기술은 개인정보보호가 정책 등에 맞춰 운영되는지 관리 하는 기술과 사용자 스스로가 개인정보를 제어하여 관리 하는 기술로 분류할 수 있다[9].

표 3. 위치정보 프라이버시 보호를 위한 운영 기술
Table 3. Operation technique for protection of Privacy on location information

운영 기술	세부 기술
프라이버시 필터링	네트워크 필터링 기술 : 방화벽, IDS, IPS, 위협관리 시스템
	개인정보 노출 차단 기술 : 기밀문서 유출방지 기술, 홈페이지 노출차단 기술, 이메일 개인정보 필터링 기술
	프라이버시 침해 차단 기술 : 애드브로커, 스파이웨어 필터, 안티 스팸 솔루션
프라이버시 스캐닝	개인정보 검색 기술
	개인정보 취약성 점검 기술
개인 정보보호 통신 기술	개인정보 은닉 기술 : 리메일러, 경로제거기, 익명화 기술
	개인정보 암호화 기술 : VPN
	개인정보 인증 기술 : 주민번호대체수단
개인 정보보호 저장 기술	Secure OS 기반 개인정보 DB
	개인정보 DB 암호화 기술
	개인정보 DB 관제 시스템

5-2 위치정보 생명주기별 프라이버시 보호 방안

(1) 수집단계

수집단계에서 발생할 수 있는 프라이버시 침해 요인은 불필요한 개인정보의 수집, 개인 정보보호 정책에 명시되지 않은 개인정보의 수집, 이용자의 동의없는 개인정보의 수집, 이용자의 동의없는 개인의 위치정보 모니터링 등이 있다. 이러한 프라이버시 침해 요인을 해결하기 위한 보안 요구사항은 다음과 같다.

① 위치정보 서비스 제공자는 반드시 수집 목적이 분명한 정보만을 사용자의 동의하에 수집해야 한다.

② 위치정보 서비스 제공자는 관리 편의성이나 상업적 목적을 위해 서비스와 관련성이 없는 개인정보를 수집해서는 안 된다.

③ 위치기반 서비스 제공자는 서비스 이용자의 프라이버시 정책을 정확히 공지하고, 이에 적합한 서비스를 제공하여야 한다.

④ 위치기반 서비스 제공자가 정보를 수집할 때, 서비스 이용자가 인증을 요구하는 경우에는 적절한 절차에 의해 인증을 제공해야 한다.

⑤ 위치기반 서비스 제공자는 서비스 이용자가 인지하지 못하는 동안에 위치정보를 수집해서는 안 된다.

⑥ 서비스 제공자가 위치정보를 수집 단계에서 이용자 동의 없이 제 3자에게 정보가 유출되지 않도록 해야 한다.

⑦ 이용자의 위치정보를 저장하고 있는 시스템은 안전한 보안 대책에 의해 보호되어야 한다.

이와 같은 위치정보 수집 단계의 보안 요구사항을 만족하기 위한 보안 대책은 표 4와 같다.

표 4. 수집단계에서의 보안 대책
Table 4. Security measures on collection phase

요구사항	보안 대책	
	기술적 측면	정책/관리적 측면
①	▪ 사용자 동의획득을 위한 안전한 본인확인 수단 필요 (예) 주민번호 대체수단	▪ XML/HTML 기반 보안 정책 ▪ 개인정보보호정책 및 관리 방침 공지 및 동의 확인
②	▪ P3P(Platform for Privacy Preferences)	▪ 추가 정보 수집 시우, 사용자의 동의 획득하는 절차 필요
③	▪ P3P(Platform for Privacy Preferences)	▪ 사용자 프라이버시 보호방안 공지
④	▪ 안전한 서버인증 수단 확보 (예) 공개키 인증서, TLS	▪ 사용자가 서버 인증을 요구할 수 있는 절차 필요
⑤	▪ 사용자 동의획득을 위한 안전한 본인확인 수단 필요	▪ 위치정보 수집에 대한 명시적인 공지 ▪ 위치정보 수집 범위, 기간, 방법에 대한 공지
⑥	▪ DB 암호화 ▪ DB 접근 권한 관리 ▪ 개인정보 노출차단 시스템	▪ 이용자 정보 제공에 대한 명시적인 동의를 획득하는 절차 필요
⑦	▪ Secure OS ▪ DB 암호화 ▪ 네트워크 보안 시스템 (예) 방화벽, IDS 등	▪ 서버 및 DB 관리자들의 접근권한 설정 및 문서화 ▪ 시스템 접근에 대한 감사 및 로그 보관

(2) 이용 및 제공 단계

위치정보를 이용 및 제공하는 단계에서 발생할 수 있는 프라이버시 침해 요인은 서비스 이용자의 동의없는 개인정보 및 위치정보의 분석이나 개인정보보호 정책에 명시되지 않은 위탁사업자나 제 3 서비스 제공자에게 위치정보 제공, 서비스 이용자의 개인정보 및 위치정보를 제 3자에게 양도하는 등 불법적 거래 등이 있다. 이용 및 제공 단계의 프라이버시 침해 요인을 해결하기 위한 보안 요구사항은 다음과 같다.

① 위치정보를 분석하는 경우에는 개인정보보호 정책에 명시된 목적과 정확히 일치하는 정보만을 분석하여야 하며, 명시하지 않은 정보를 결합하여 분석할 수 없다.
② 이용자의 동의없이 위치정보를 모니터링하거나 추적할 수 없어야 한다.
③ 이용자의 허가없이 광고성 스팸메일이나 문자, 전화 등을 시도해서는 안 된다.
④ 이용자 정보보호정책에 명시되지 않은 위탁 사업자나 제3자에게 DB가 공개되어서는 안된다.
⑤ 관리자의 오류 및 권한 남용에 의해 이용자의 정보가 노출되어서는 안 된다.
⑥ 악의적인 사용자가 불법적인 권한 획득을 통해 이용자의 정보가 노출되어서는 안 된다.

표 5. 이용 및 제공 단계에서의 보안 대책
Table 5. Security measures on use and providing phase

요구사항	보안 대책	
	기술적 측면	정책/관리적 측면
①	▪ XML/HTML 기반 보안 기술 ▪ P3P	▪ 위치정보 분석을 위한 목적, 범위, 절차 등을 명시 ▪ 위치정보 분석 로그 보관
②	▪ 안전한 사용자 동의획득 수단 ▪ 프라이버시 제어 수단	▪ 위치정보 모니터링, 수집, 범위, 방법, 동의절차에 대한 명시적인 공지
③	▪ 프라이버시 침해 차단 기술 ▪ 사용자 동의획득 수단 확보	▪ 스팸 발송 금지에 관한 규정
④	▪ Secure OS ▪ DB 암호화 ▪ 네트워크 보안 시스템 ▪ 네트워크 모니터링	▪ 시스템 및 DB 접근 권한 명시 및 문서화 ▪ 시스템 및 DB 접근에 대한 감사 및 로그 보관
⑤	▪ 인증/접근제어 시스템 ▪ 네트워크 모니터링 ▪ DB취약성 점검시스템	▪ 관리자의 권한 관리 방침 명시 ▪ 감사 및 로그 기록 보관
⑥	▪ 인증/접근제어 시스템 ▪ 네트워크 보안 시스템 ▪ 개인정보 노출 차단 시스템	▪ 불법적인 침입에 대비할 수 있는 정보보호관리체계 수립

이와 같은 위치정보 이용 및 제공 단계의 보안 요구사항을 만족하기 위한 보안 대책은 표 5와 같다.

(3) 보관 및 파기 단계

보관 및 파기 단계에서 발생할 수 있는 프라이버시 침해 요인은 수집된 개인정보를 불법적인 유출 위협이 있는 상태로 저장하거나 개인정보보호 정책에

위배되는 보관 기관 및 파기 절차, 관리자 또는 이용자의 실수나 오류로 인한 정보 노출 등이 있다.

보관 및 파기 단계의 프라이버시 침해 요인을 해결하기 위한 보안 요구사항은 다음과 같다.

① 이용자 정보를 저장하고 있는 데이터베이스와 시스템은 적절한 보안 대책에 의해 관리되어야 한다.

② 이용자 정보보호정책에 명시한 보유기간이 경과한 정보는 DB, 백업 DB, 관련 파일 등에서 즉시 파기해야 한다.

③ 보유 기간이 지나지 않은 정보의 손상에 대비하여 보안 대책을 구축해야 한다.

④ 이용자 정보가 저장된 파일이나 문서 등을 파기할 때에는 복구가 불가능한 형태로 처리해야 한다.

표 6. 보관 및 파기 단계에서의 보안 대책
Table 6. Security measures on keeping and destruction phase

요구사항	보안 대책	
	기술적 측면	정책/관리적 측면
①	▪ 접근제어 시스템 ▪ Secure OS ▪ 네트워크 보안 시스템	▪ 관리자 접근 권한 및 DB 보안 정책 설정
②	▪ XML/HTML 기반 보안 기술 ▪ 개인정보보호	▪ 이용자 정보의 파기절차 및 관리 방침 문서화
③	▪ 침해사고 대응 시스템 ▪ 네트워크 모니터링시스템 ▪ 정보 이중화(백업 DB)	▪ 침해 사고 대응체계 구축 및 절차 문서화
④	▪ 개인정보노출차단 시스템 ▪ 안전한 문서 관리 시스템	▪ 이용자 정보의 파기절차 및 관리 방침 문서화
⑤	▪ 권한 관리/접근 제어 ▪ 개인정보노출차단 시스템	▪ DB와 시스템에 대한 접근 제어 정책 수립
⑥	▪ 권한 관리/접근 제어 ▪ 정보 이중화(백업 DB)	▪ 정보의 저장, 복구에 대한 절차 문서화
⑦	▪ 권한 관리/접근 제어 ▪ 개인정보노출차단 시스템 ▪ DB 보안	▪ 관리자 및 이용자의 접근 권한 문서화

⑤ 이용자 정보 파기 권한을 가지지 않은 자가 정보를 임의로 파기할 수 없도록 해야 한다.

⑥ 관리자의 실수에 의해 이용자 정보가 파기되는 경우에 대한 보안 대책을 마련해야 한다.

⑦ 관리자나 이용자의 실수로 인해 이용자 정보가 노출되지 않도록 해야 한다.

위와 같은 프라이버시 침해 요인을 해결하기 위한 보안 대책은 표 6과 같다.

Ⅵ. 결 론

유비쿼터스 환경에서의 위치정보 활용서비스는 개인, 기업 및 공공분야에 이르기까지 다양한 형태로 활용되고 있다. 위치기반 서비스에서 활용되는 위치정보는 사용자에게 편의성을 제공한다는 취지와는 다르게 서비스 제공자의 의지에 따라 얼마든지 악용될 수 있다는 문제점을 가지고 있다.

이처럼 위치정보가 악용될 경우에는 개인의 위치추적이 가능하기 때문에 개인의 프라이버시를 침해할 수 있으며 위치정보의 오용으로 인해 사용자에게 큰 피해를 가져올 수도 있다. 그러므로 위치기반 서비스가 보다 활성화되기 위해서는 위치정보의 보호를 통한 사용자의 프라이버시 보호가 선결되어야 한다.

따라서 본 논문에서는 위치정보가 수집되고 활용되는 과정을 위치정보의 수집-이용-제공-보관-파기 등과 같이 생명주기별로 분류하고, 이에 따른 프라이버시 침해 요인을 분석하였다. 그리고 위치정보 프라이버시 보호를 위한 정보보호 기술을 운영기술과 정책 및 관리 기술로 분류하여 분석하고, 그 결과를 바탕으로 생명주기별 침해 요인에 따른 프라이버시 보호 방안을 제시하였다.

본 논문의 연구결과는 향후 개인정보보호를 위한 위치정보보호 프라이버시 침해 방지 가이드라인을 작성하는데 기반 자료로 활용할 수 있으며, 위치정보 프라이버시 침해 방지를 위한 기술 개발 등의 연구분야에서 기반 자료로 활용될 수 있을 것이다.

감사의 글

본 논문은 2007년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임(20070-0382)

참 고 문 헌

[1] 박용우, “위치기반 서비스.의 기술동향 및 활성화 전망”, KISDI IT FOCUS, 2001
[2] 윤미영, 김선아, “Safeguard of u-Society, LBS", 한국 *정보사회진흥원*., 2007
[3] 오태원, “개인위치정보의 법적 문제와 위치기반 서비스의 전망”, *정보통신정책*, 2002
[4] 한국전자통신연구원, “LBS 기술 및 산업현황 연구 보고서”, 2006
[5] 전자부품 연구원, “위치기반 서비스 동향”, 2004
[6] 와이즈인포, “LBS 주요 기술 및 서비스 현황”, 2007
[7] 곽 진, 여상수, “RFID 프라이버시 보호 프로토콜들에 대한 안전성 및 성능 비교 분석”, *Journal of the Korean Data Analysis Society*, Vol. 9, No. 4, 2007
[8] 오수현, “프라이버시 보호 가능한 RFID 인증 시스템의 비교·분석” *Journal of The Korean Data Analysis Society,* Vol. 7, No. 1, 283-296, 2005
[9] ㈜위너다임, "P3P 개인정보보호정책생성기 최종보고서", 한국정보보호진흥원 최종보고서, 2005

오 수 현(吳秀賢)

1998년 2월 : 성균관대학교 정보공학과(공학사)
2000년 2월 : 성균관대학교 전기전자 및컴퓨터공학부(공학석사)
2003년 8월 : 성균관대학교 전기전자 및컴퓨터공학부(공학박사)
2004년 3월~현재 : 호서대학교 정보보호학과 조교수
관심분야 : 암호 프로토콜, 유/무선 네트워크 보안, 정보보호제품 평가/인증

곽 진

2000년 8월 : 성균관대학교 정보공학과(공학사)
2003년 2월 : 성균관대학교 전기전자 및컴퓨터공학부(공학석사)
2006년 2월 : 성균관대학교 전기전자 및컴퓨터공학부(공학박사)
2006년 4월-2006년 11월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월-2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년-2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 3월~현재 : 순천향대학교 정보보호학과 조교수
관심분야 : 암호프로토콜, RFID 시스템 보안, 개인정보보호, 정보보호제품 평가 등