프라이버시 보호를 위한 개인 위치 정보 관리 프로토콜

황영식° 남택용
한국전자통신연구원
{yshwang°, tynam}@etri.re.kr

A Protocol of Personal Location Information Control for Privacy

Youngsik Hwang° Taekyong Nam
Privacy Protection Research Team, Electronics and Telecommunications Research Institute

요 약

본 논문에서는 프라이버시 보호를 위한 개인 위치 정보 접근에 대한 통보 유무, 동의와 같은 차별화 된 정책 설정과 특정 장소나 시간에 대해 위치 정보 제공을 차단 할 수 있는 프로토콜을 제안 하려고 한다. 제안하는 프로토콜은 모바일 상의 프라이버시 설정을 위해 응용 레벨에서 동적으로 발생하는 개인의 위치 정보에 대해 유저가 설정한 특정 장소와 시간에 따라 차단하는 기능 설정할 수 있다. 또한 서비스 제공자와 요청자 별로 개인 위치 정보 접근에 대한 통보 유무, 동의와 같은 차별화된 정책을 설정 할 수 있다. 제안하는 프로토콜은 이들 설정된 정책들의 리스트들을 요청자 별로 나누어서 사용자 프라이버시 리스트 서버(UPLS)에서 관리하며, 서비스 요청 시 설정된 정책에 맞는 서비스를 서비스 제공자들이 제공하게 되므로 개인 위치 정보에 대해 프라이버시를 제공하게 된다.

1. 서 론

유비쿼터스 사회의 도래와 함께 많은 양의 정보들이 제공되어 지고 또한 정보들을 제공 받을 수 있게 되었다. 특히 다양한 모바일 기기들의 발달은 많은 개인들의 위치 관련 정보 발생하게 되었고 이들 정보는 개인 위치 정보 관련한 많은 서비스를 창출 하고 있다. 하지만 기술과 정보의 발달과 함께 대두되는 많은 문제점이 발생 하듯이 개인 위치 정보는 개인의 위치 정보의 실시간 노출, 추적 이라는 프라이버시 문제를 발생시키고 있다.

하지만 현재 이루어지는 위치 관련 서비스들은 제공 대상에 따른 서비스 제한 정도의 단순한 정책을 적용한 정도로 기능은 맞춤화된 서비스(Houdini[1])와 같은 적정 수준의 개인 프라이버시를 제공 하지 않고 있다. 이는 곧 한 개인의 위치 정보가 실시간으로 노출 되어 이를 이용한 범죄 발생 가능성이 큰 것을 의미한다.

따라서 본 논문에서는 이를 위해 모바일 상의 프라이버시 설정을 위해 응용 레벨에서 제공되는 PCP[2]와 같은 프로토콜의 제공을 위해 세 가지 방법을 제시한다. 첫째, 특정인의 위치 정보 요청 시 맞춤형 서비스 제공을 위해 대상자가 설정한 임시 전면 차단, 특정 장소 차단, 특정 시간 차단과 같은 맞춤 조건들을 검사 후 조건을 만족할 경우에만 정보 제공을 한다. 둘째, 첫째 조건을 만족 시 사용자 프라이버시 리스트 서버의 개인 위치 정보 접근에 대한 통보 유무, 동의의 유무[3]와 같은 차별화된 정책들의 리스트에 맞게 정보를 제공하며, 또한 동의 과정을 통해 자신의 정보에 대한 접근을 알 수 있게 하는 프로토콜을 제시 한다. 셋째, 로그 데이터베이스(LDB)에 개인 위치 정보에 접근 시도와 정보 제공에 대한 기록을 남기게 함으로써 이 정보를 통해 자신의 정보의 오용 등을 예상하고 방지 할 수 있게 한다.

본 논문은 이후 2장에서 전체 시스템 구조와 관련된 정의들에 대해 얘기하며, 3장에서는 세부 프로토콜을 단계별로 분석한다. 그리고 끝으로 4장에서 결론을 맺는다.

2. 정의 (Definition)

- 개인 위치 정보 (PLI : Personal Location Information) :
개인 위치 정보(PLI)는 시간에 따라 동적으로 변경되는 특정인의 위치 정보들로 모바일 기기를 통해 서비스 공급자들에게 전달되어 관리, 제공 되어진다.

- 사용자 (User) :
사용자(User)는 크게 두 종류로 분류 되어진다. 첫째, 특정 유저의 개인 위치 정보(PLI)를 요청하는 유저인 Requester와 둘째, 요청 유저의 대상이 되어지는 유저로 정보 제공의 동의 요청이나 고지를 받는 Requestee이다.

- 서비스 공급자 (SPn : Service Provider) :
특정 위치 관련 서비스 공급자(SP)로 가입된 유저에게 실시간 개인 위치 정보(PLI)를 받아 관련된 서비스를 관리, 제공하는 주체로 사용자 프라이버시 리스트 서버에서 설정 메시지(CM)를 받아 그에 맞는 서비스를 제공한다.

- 사용자 프라이버시 리스트 서버 (UPLS : User Privacy List Server) :
개인 위치 정보(PLI)에 대해 차단 설정 조건 판별 및 서비스 공급자(SP)의 종류에 따라 Requester에 대해 정보의 고지의 유무, 고지 후 동의 유무 등의 설정 정보를 가지고 있다.

- 로그 데이터베이스 (LDB : Log DataBase) :
개인 위치 정보(PLI)의 민감성과 기밀성 때문에 사용자 프라이버시 리스트 서버(UPLS)에 대한 요청과 서비스 공급자(SP)의 전송에 대한 로그(Log)를 기록하기 위한 데이터베이스이다.

- 설정 메세지 (CM : Configuration Message) :
개인 위치 정보(PLI)의 설정의 유무, 요청자(Rquester)에 대해서 정보 제공에 대한 통보의 유무, 통보 후 동의 유무에 대한

설정된 정책의 정보를 포함 하고 있는 메시지이다. 서비스 공급자(SP)에 요청에 의해 사용자 프라이버시 리스트 서버(UPLS)에서 제공 한다.

3. 개인 위치 정보 제공 프로토콜

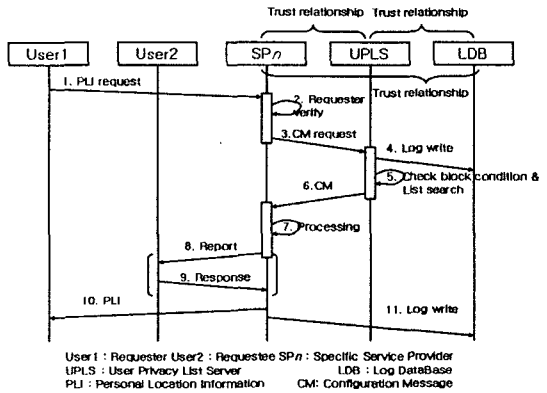

그림 1. Protocol structure flow

그림 1.에 나타난 프로토콜 구조의 흐름에 나타난 단계들에서 전송되는 데이터의 형식, 데이터의 의미, 데이터 처리 과정 등의 세부 과정별로 살펴보면 다음과 같은 형식과 동작을 하는 세부 과정들로 이루어져 있다.

3.1 PLI request (개인 위치 정보의 요청)

개인 위치 정보의 요청으로 Requester 식별 정보(ID_{U1}), Requestee 식별 정보(ID_{U2}), *Timestamp*의 정보를 전송하는 과정이다. 정보들은 *HMAC(n)*을 이용하여 디지털 서명을 추가해서 전송된다.

$$(ID_{U1},\ ID_{U2},\ Timestamp) \mid S_{KU1}(HMAC(ID_{U1},\ ID_{U2},\ Timestamp))$$
$$= (ID_{U1},\ ID_{U2},\ Timestamp) \mid Sig(M)$$

ID_{U1} : Requester(User1)의 식별 정보, ID_{U2} : Requestee(User2)의 식별 정보, *Timestamp* : 시간 관련 정보 $S_{KU1}(M)$: Requester(User1)의 private-key로 암호화(서명)

3.2. Requester verify (요청자의 인증)

서비스 공급자가 requester를 인증하는 단계이다. User1의 서명을 이용하여 PLI 요청에 대해 검증을 함으로써 User1의 요청을 처리하게 된다. *Timestamp* 변수는 replay attack에 대한 안전을 보장하는 역할을 하게 되며, 요청자의 인증 후 서비스 공급자는 서비스에 관련된 Requester와 Requestee의 정보를 가지게 된다.

3.3. CM request (설정 정보에 대한 요청)

서비스 공급자가 PLI request의 정보를 이용 UPLS에 CM를 요청하는 단계이다. 이때 서비스 공급자 식별 정보, Requester의 아이디, Requestee의 아이디, 현재 위치, 시간 정보와 함께 freshness를 위한 Nonce 값을 인자로 가진다.

$$SP_{id} \mid ID_{U1} \mid ID_{U2} \mid Area(Zip\ Code) \mid time \mid N$$

SP_{id} : 서비스 공급자(SP)의 식별 정보, N : Nonce value

Area(Zip Code) : Requestee(User2)의 현재 위치 정보, *time* : 요청 시간

3.4. Log write (로그 남기기)

UPLS에서 요청에 대한 로그(Log)를 LDB에 기록한다. 특히, 처리 과정[3.7)단계] 이전에 로그(Log)를 남기게 함으로써 공격 사도자의 정보를 저장하며 사후 감사(Audit)용으로 쓰일 수 있다.

3.5. Check block condition & List search (차단 조건 검사와 설정의 검색)

이번 단계에서는 크게 두 가지 과정을 이루고 있다. 첫째, 요청 대상자가 설정해 놓은 차단 조건의 검사와 둘째, 프라이버시 리스트 서버(UPLS)에 CM에 대한 정보의 검색이다.

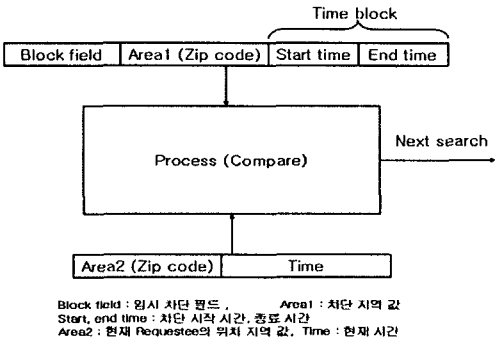

그림 2. Block Condition Check

우선 요청 대상자가 설정해 놓은 차단 조건에 대한 검사이다. 이 경우 서비스 공급자(SP)가 전송한 요청 대상자의 아이디와 현재 위치 정보, 현재 시간 값을 사용자 프라이버시 리스트 서버(UPLS)에 해당 유저가 설정한 차단 조건 블록 값과 비교를 한다. 차단 조건의 블록 값은 임시 전면 차단 값을 가지는 Block 필드, 차단 위치 정보를 값을 가지는 Area 블록, 차단 시간을 가지는 Time 블록으로 이루어져 있다. Block 필드의 경우 요청 대상자가 임시로 자신의 위치 정보 차단 시 설정하는 값으로 설정 시 위치 정보가 전면 차단된다. Area 블록의 경우 위치 정보 차단 지역에 대한 정보이며 우편 번호 체계가 가지는 지역 코드의 값을 이용한다. 이 값들과 서비스 제공자(SP)가 전송된 위치 정보가 같을 경우 요청 대상자가 차단 설정 지역에 있기 때문에 위치 정보가 차단되게 한다. 마지막 값인 Time 블록의 경우 차단 시작 시간 값과 종료 시간 값을 가지고 있으며, 전송된 시간 정보와 비교 후 차단 시간에 해당하면 역시 위치 정보가 차단되게 된다.

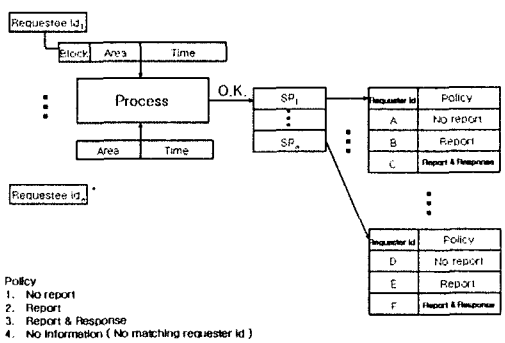

그림 3. UPLS List structure and search process

위의 차단 조건 검사가 성공하면 해당 SP의 검색 → Requestee의 검색 → Requester 검색이 이루어지게 된다. 검색 결과가 있을 시 최종적으로 해당 검색 결과인 정책(*policy*) 정보를 얻게 되며 이 정보는 차별화된 프라이버시 제공을 위해 이용된다.

3.6. CM (설정 메시지)

List search 결과 후 얻은 정보(Policy field)를 CM 형태로 전송한다. 이때 이전에 받은 Nonce 값을 같이 보내게 됨으로써 freshness를 보장한다.

$$N \mid policy$$

N : Nonce value, *policy* : UPLS List structure의 policy의 값

3.7. Processing (처리)

서비스 공급자는 CM의 정책(*policy*)값에 맞는 메시지를 생성하여 적절한 Requester(User1)에게 PLI request의 응답 정보로 넘겨준다. PLI request 응답 정보는 다음과 같다.

i. Requestee에게 통보 하지 않고 Requester에게 제공.
ii. Requestee에게 통보는 하나 동의 응답 없이 제공.
iii. Requestee에게 통보 후 동의 결과에 따라 제공.
iv. 제공 거부.

3.8. Report (통보)

통보 미설정시 3.8), 3.9) 과정은 생략되며, 통보 설정 시에는 Requester에 대한 정보를 Requestee에게 전송하게 된다. 동의 설정 시에는 추가적으로 Nonce 값을 덧붙여 보내게 된다.

i. Requestee의 통보 설정 시

$$E_{KS}(ID_{U1}) \mid P_{KU2}(K_S) \mid Sig(M)$$

K_S : 서비스 공급자에서 정한 세션키, E_{KS} : 서비스 공급자에서 정한 세션키로 대칭키 방식의 암호화, $P_{KU2}(K_S)$: Requestee의 public-key로 세션키를 암호화, $Sig(M)$: $M(=E_{KS}(ID_{U1}) \mid P_{KU2}(K_S))$ 에 전자 서명함

ii. 통보 & 동의 설정 시

$$E_{KS}(ID_{U1}, N) \mid P_{KU2}(K_S) \mid Sig(M)$$

3.9. Response (응답)

동의에 대한 응답을 전송하다. 통보 시 받은 Nonce 값과 동의의 결과를 서비스 공급자에서 정한 세션키로 암호화 하여 전송한다.

$$E_{KS}(N, response)$$

response : Requestee의 동의 정보 값

3.10. PLI (개인 위치 정보)

최종적으로 서비스 공급자가 Requester에게 개인 위치 정보 제공 서비스가 이 단계에서 이루어진다. 한번 연결된 서비스는 서비스 공급자가 정해준 세션키로 정보 및 서비스가 암호 되어 제공된다.

$$E_{KS}(PLI) \mid P_{KU1}(K_S) \mid Sig(M)$$

PLI : Requester가 요청한 Requestee의 개인 위치 정보 값으로 서비스 공급자(SP)가 제공함

3.11. Log write

SP에서 정보 제공에 대한 로그(Log)를 LDB에 기록한다. 이는 정보 접근 시도를 기록하는 3.4)단계와 달리 정보 제공에 대해 기록을 남기는 과정이다. 이 로그 정보는 개인 위치 정보의 제공 주체 유저가 사후 자신에 위치 정보에 제공에 대한 로그(Log)를 확인 할 수 있게 한다.

4. 결 론

본 논문에서는 개인 위치 정보의 중요성을 인식하고 이에 맞는 프로토콜을 제시 하였다. 제안된 방법에서는 첫째, 자신의 위치 정보를 임시 전면 차단, 특정 장소나 시간에 대한 차단을 제시 하였다. 특히, 특정 장소에 대한 차단은 우편 번호의 지역 정보 값을 응용 하였다. 또한 다양한 서비스와 사용자에 대해 통보의 유무, 동의 유무와 같은 차별화 되게 설정된 정책을 통해서 개인의 위치 정보의 프라이버시를 보장하였다. 더불어 이를 위해 유저 프라이버시 서버(UPLS)와 설정 메시지(CM), 로그 데이터베이스(LDB) 등의 시스템적인 요소를 추가된 시스템을 제안 하였다. 이렇게 제시된 프로토콜은 자신의 위치 정보에 대해 컨트롤 할 수 있으며, 또한 통보와 동의를 통해 자신 위치 정보의 사용 여부를 알 수 있게 하여 위치 정보에 대한 프라이버시를 해결 하였다. 그리고 이들 정보를 전달하는 프로토콜에 현재 널리 이용되고 있는 유무선 PKI 기반 기술을 적용하였기 때문에 프로토콜의 간결화와 함께 동시에 검증된 안전성을 제공하였다.

끝으로 본 논문이 제시한 프로토콜의 차후 진행 되어야 할 연구 방향을 짚어 보면 개인 위치 정보의 무선 단말기로 모바일 기기를 가정 하고 있지만 모바일기기 뿐만 아니라 각종 센서들을 통해서도 개인 위치 정보가 발생할 수 있다. 따라서 무선 단말기의 범위를 센서의 수준까지 확대할 필요가 있다. 하지만 센서의 경우 전력과 컴퓨팅 파워, 메모리 등의 제한으로 인해 현재 PKI기반 기술의 적용이 불가능하다. 이에 따라 PKI를 대체할 적은 컴퓨팅을 제공하는 암호 방식 예를 들면 해쉬 체인(Hash Chain)을 응용한 방식[4] 등의 적용을 고려해야겠다.

[참고문헌]

[1] http://www2003.org/cdrom/papers/poster/p299/p299-hull.html
[2] http://member.openmobilealliance.org/ftp/Public-documents/TP/Permanent_documents/OMA-WID_0042-LocPCP-V1_0_1-20041022-A.zip
[3] 박남제, "위치정보 프라이버시 보호기술", ETRI RFID/USN 보안 기술 소식지", 1호, pp. 13-16, 2005.
[4] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen and David E. Culler, "SPINS: Security Protocols for Sensor Networks", Proceedings of the 7th annual international conference on Mobile computing and networking, pp.189-199, 2001