U-City 환경에서의 개인정보보호 향상을 위한 상황인지기반 보안 기법 연구

이준규*, 이창훈*, 김지호*, 송오영*
*중앙대학교 전자전기공학부
e-mail : jk3546@hanmail.net

A Study on Security Association Based on Context-Aware for Privacy Protection in U-City

Jun-Gyu Lee*, Chang-Hun Lee*, Ji-Ho Kim*, Oh-Young Song*
*School of Electrical and Electronics Engineering, Chung-Ang University

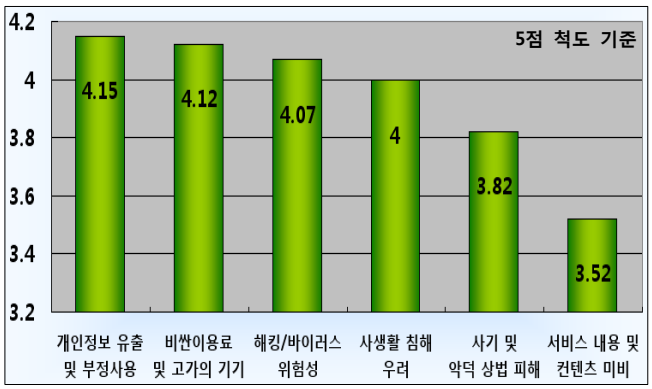
요 약

현재 우리나라는 미래형 첨단도시, U-City구현을 현실화 하고 있다. 유비쿼터스 기반기술이 총망라되는 U-City의 건설은 우리에게 편리하고 윤택한 삶을 약속하지만 U-City속의 수많은 유·무선 단말을 통해 수집되는 개인이나 사물, 환경에 대한 정보는 전자감시에 대한 우려와 이용자 프라이버시 침해를 유발하는 원인이 될 수 있으며 그에 심각성은 작금의 정보화 사회에 비할 수 없이 클 것으로 예상된다. 이에 본 논문에서는 U-City에서 발생할 수 있는 개인정보 침해위협을 통합적으로 살펴보고 개인정보보호 향상을 위한 보안 기법을 연구하였다.

1. 서론

수년전만 하더라도 낯설기만 했던 '유비쿼터스'란 용어는 이제 실생활 곳곳에서 흔히 쓰이는 보통명사가 되었다. 더욱이 우리나라는 세계 최고의 IT인프라를 기반으로 유비쿼터스 컴퓨팅 기술이 하루가 다르게 발전하고 있으며, 유비쿼터스에 관해선 우리나라의 확산 속도를 어느 나라도 따라오지 못한다. 이제 우리나라는 미래형 첨단도시, U-City(Ubiquitous-City)구현을 현실화 하고 있다. 광대역 통합망(BcN), 전자태그(RFID), 위치기반서비스(LBS), WiBro, 위성위치추적시스템(GPS), 유사광가입자망(FTTP), 홈네트워크 등 다양한 유비쿼터스 기반기술이 U-City에 총망라된다. 인공지능에 의해 도로와 교통상태가 관리되고, 공장 유해가스 배출, 소음정도 등을 실시간으로 점검하며, 주변지역의 각종 치안 범죄를 실시간으로 모니터링해 안전한 도시환경을 보장하는 U-City의 구현은 우리에게 장밋빛 미래를 약속하면서 동시에 정보화 사회에서 유비쿼터스 사회로의 변화를 예고하고 있다.

하지만 이러한 U-City환경은 산업 및 사회에 미칠 순기능 외에 개인정보의 침해에 관련된 역기능도 클 것으로 예상되고 있다. U-City환경에서는 필연적으로 개인에 관한 정보를 필요로 한다. U-City에서 요구되는 정보는 현재의 정보화 사회에서 요구되는 단순한 개인의 신상정보가 아니라 생체 인식을 통해 획득되는 바이오 정보, 실시간 추적을 가능케 하는 위치정보 등의 새로운 정보이고, 또한 어떤 개인의 행동과 성향 전반에 대해 끊임없이 수집되는 민감한 정보이기 때문에 정보 주체의 프라이버시 침해 위협이 지금보다 훨씬 높아질 것이다. 게다가 일반국민은 유비쿼터스 사회에 대해 개인정보 유출, 해킹·바이러스 사고, 사생활 침해 등 역기능에 대한 불안감을 느끼고 있는 것으로 조사되었다.



(그림 1) 유비쿼터스 사회의 국민 불안요소

그러나 유비쿼터스 컴퓨팅 기술이 서양에서는 이처럼 감시사회에 대한 사생활 침해와 관련하여 매우 논쟁이 심한데 반해 우리나라를 포함한 아시아에서는 주로 생활편의와 복지수준향상, 경제성장과 같은 긍정적인 측면만 집중적으로 부각되고 있는 것이 현실이다. U-City구현의 세계 선두에 서있는 우리나라도 아직 개인의 프라이버시와 정보보호, 정보통제와 관련한 부분에 있어서는 충분한 기술적·법제도적인 준비가 이루어지지 않은 상황이다. 따라서 개인정보유출에 대한 국민의 불안감을 해소하고, 이용자에게 신뢰도 높은 U-City서비스를 제공하기 위해 U-City의 건설은 그 장점뿐만 아니라 역효과에 관하여도

심도 있는 검토와 기술적, 법·정책적인 준비가 뒤따라야 할 것이다. 이하에서는 U-City에서 발생할 수 있는 개인정보 침해위협을 통합적으로 살펴보고 이를 대처하기 위한 방법을 모색해 본다.

2. U-City 환경에서 나타날 수 있는 개인정보 침해 유형

현재의 정보화 사회에서도 개인정보는 인터넷, 각종 마케팅, 다양한 커뮤니티에 저장된 개인정보, 설문조사 등의 방법으로 각 개인이 원하지 않음에도 불구하고 각종 저장매체에 기록되고 유통되고 있다. 현행에서 일반적으로 문제가 되는 개인정보의 침해유형은 (1)부적절한 정보의 접근과 수집, (2)부적절한 모니터링, (3)부적절한 분석, (4)부적절한 이전, (5)원하지 않는 영업행위, (6)부적절한 저장 등 6가지로 나누어볼 수 있다. 부적절한 정보의 접근과 수집은 정보주체의 동의 없는 개인정보의 수집, 개인정보 수집시 고지 또는 명시의무를 이행하지 않는 행위, 과도한 개인정보수집 등을 의미하며, 부적절한 모니터링이란 정보주체의 동의 없는 개인의 인터넷 활동 모니터링, 몰래카메라, CCTV를 통한 감시를 의미한다. 또 부적절한 분석은 소비자들이나 노동자들에게 알려주지 않고 그들의 사적인 정보를 분석하는 행위를 말한다. 부적절한 분석을 통해 소비자의 구매나 소비패턴을 파악할 수 있으며, 분석결과를 지불능력에 따른 차별적인 서비스제공 혹은 노동자에 대한 통제 강화에 이용할 수 있다. 부적절한 이전은 고객에게 알리지 않고 고객의 개인정보를 다른 기업들에게 넘겨주는 행위를 의미하며, 고지·명시한 범위를 넘어선 이용 또는 제3자 제공, 영업의 양수 등의 통지의무 불이행도 여기에 포함된다. 원하지 않는 영업행위라 함은 주로 인터넷 사용자의 동의나 허가 없이 상품광고 메일, 즉 스팸(spam)메일을 보내는 행위를 말한다. 이 유형의 프라이버시 침해에는 정크메일, 대량 DM, 정크 인터넷 푸시 채널 등 영리목적의 광고성 정보 전송이 포함된다. 끝으로 부적절한 저장은 개인정보를 안전하지 못한 방식으로 보관하여 저장된 정보의 신뢰성을 떨어뜨리고 정보접근에 대한 인증을 수행하지 못하는 행위를 말한다. 예컨대, 데이터베이스 시스템 관리를 잘못하여 개인 사용자가 다른 사용자의 정보를 훔쳐볼 수 있다. 개인정보 취급자에 의한 훼손이나 침해, 그리고 수집 또는 제공받은 목적 달성 후 개인정보를 파기하지 않은 행위도 여기에 속한다.

이와 같은 현행의 일반적인 개인정보침해의 유형은 유비쿼터스 컴퓨팅환경에서도 그대로 적용할 수 있을 것이다. 다만 침해유형에 큰 변화가 없다는 것이 개인정보 침해에 대한 변화가 없을 것이란 것과는 다른 문제이다. 적어도 유비쿼터스 컴퓨팅 환경 하에서 개인정보 침해의 비중이나 그 형태적 변화는 큰 차이를 가지고 나타날 것으로 예상된다. 즉 유비쿼터스 사회에서는 개인정보가 단순히 개별적으로 수집되는 것에 그치지 않고, 모든 사람이 자신의 의지와 상관없이 실시간으로 네트워크에 의해 정보를 수집 당하는 것을 의미하게 되는 것이므로 개인정보 침해의 소지가 급격히 커질 수 있다는 것이다.

3. U-City 환경에서의 개인정보보호 향상을 제안하는 보안 기법

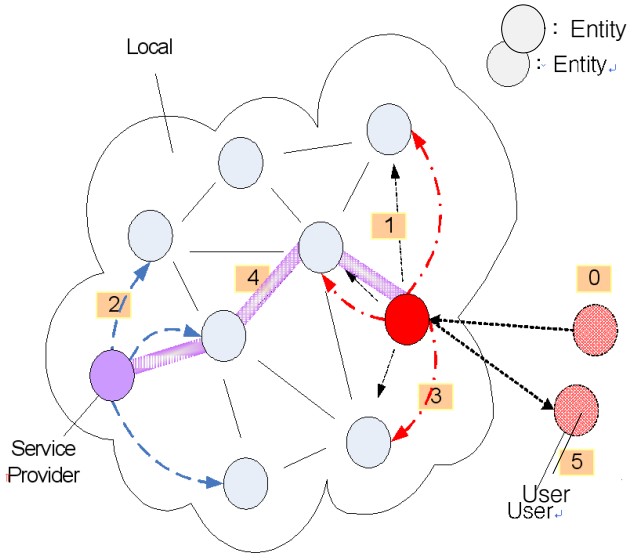
현재 수도권을 비롯한 각 지자체에서 추진되고 있는 U-City계획은 향후 제공하게 될 서비스의 많은 부분에서 개인정보침해의 문제를 간과한 채 진행되고 있다. 실제 서울시에서 시행중인 요일제 운행 RFID 부착차량에 대한 혜택부여정책 역시 RFID에 의해 운행기록이 남을 수 있다는 점은 간과된 채 운영 중이다. 그러나 향후 U-City건설이 실현되면 위와 같이 개인정보침해와 관련된 사안은 사전에 신중히 검토되어야 한다. 각 차량에 RFID장치를 부착하여 실시간으로 차량운행정보와 각 교차로에서 차량의 정보를 수집하게 되면 비록 교통운행의 원활을 도모하고 안전한 운전을 보장해 줄 수는 있겠지만 각 개인의 차량운행경로 혹은 주행 목적지 등이 고스란히 수집되어서 심각한 개인정보침해의 문제를 발생시킬 수 있기 때문이다.

항목 / 권한등급	조 회 등 급 (Service Provider's View Point)		서비스 항목
Level 0 (Guest Mode)	Personal	• Name, Age, Gender	• 기본적인 안내 서비스
	Device	• Mobile Type, Power Management Type,	
Level 1 (Single Mode)	Personal	• Guest Mode Information • E-mail Address, Preferred Service Type, Preferred Role Type, Preferred Protocol Type	• 위치 안내 서비스 - 주차장 위치
	Device	• Defined Max Data Rate, Memory size, Computation Ability	
Level 2 (Intermediate Mode)	Personal	• Guest & Single Mode Information • Birth-day, Cellular Phone Number, Interest, Blood Type, Friend List	• 친구 찾기 서비스 • 광고 서비스
	Device	• Minimum Latency and Throughput, Device Address (Ad-Hoc Address)	
Level 3 (Master Mode)	Personal	• Guest & Single & Intermediate Mode Information • Home Address, Home Phone Number, Schedule, 생활반경	• 성생활 정보 서비스
	Device	• Power Status Information, Mac Address	

<표 1> 개인정보 레벨 및 서비스 등급

U-City환경에서는 수많은 유·무선의 단말을 통해 갖가지 정보들이 실시간으로 수집, 이동, 저장, 처리된다. 여러 경로를 거치며 오고 가는 정보는 개인의 바이오정보, 위치정보 등 민감한 정보가 있을 것이고 반면에 나이와 같은 통계나 연구목적의 상대적으로 그 민감성이 적은 정보도 있다. 따라서 사용자 프라이버시침해를 최소화하기 위해서는 개인정보의 등급화와 그에 따른 적절한 관리가 필요하다. 어떤 개인정보는 공개적 접근이 허용되어야 하고, 어

떤 개인정보는 보다 철저하게 보호되어야 할 것이다. 예컨대 개인정보에는 의료, 성적 취향과 같이 수집이나 공개가 절대적으로 제한되는 정보가 있을 것이고, 수집과 이용 및 공개에 반드시 당사자의 동의 또는 통지를 요하는 정보도 있을 것이다. 개인정보의 등급화는 그러한 판단을 내리는데 없어서는 안 될 것이다. 또한 개인정보의 수명 관리에도 개인정보의 등급화는 필수적이 될 것이다. 개인정보는 그것이 지닌 민감성에 따라 <표 1>과 같이 4등급으로 분류할 수 있다.



Association
0. Context Setting
1. Entity Discovery
2. Service Advertisement/Discovery
3. Authentication
4. Level Configuration
   - Authorization
   - Privilege Mapping
   - Negotiation
   - Location Information 노출 범위 및 Location Tracking 설정
5. Deassociation
   - History Information 및 Accounting 문제 해결

(그림 2) 프라이버시 향상을 위한 Secure Association 방법

U-City환경에서는 서비스 사용자(User)와 서비스 제공자(Service provider)가 로컬(Local)영역에 혼재해 있다. 따라서 이러한 동적인 네트워크 구성으로 인해 로컬(Local)에서의 Association이 중요한 문제로 부각되며, 초기 Association시 프라이버시 문제의 대부분을 한 번에 해결할 수 있는 인증, 보안레벨 부여 등의 방안을 제시하고자 한다. 일련의 과정은 (그림2) 와 같이 도식화 할 수 있고, 각각의 원형은 사용자의 단말이나 서비스 제공자 서버 등의 Entity이다. 새로운 사용자가 서비스 제공자로부터 서비스를 제공받기 위해 정보보호를 위한 Secure association 방법은 다음과 같다. 실제 사용자가 U-City의 어떤 서비스를 제공받기 위해 먼저 상황정보 설정(Context Setting) 단계에서는 자신의 정보에 대해 온톨로지(Ontology)화 시키고, 사용자 탐색(Entity Discovery)단계에서는 사용자가 새로운 그룹으로 들어가는 경우 메시지를 전송하여 자신이 등장했음을 통보한다. 서비스 공지/탐색(Service advertisement/discovery)단계에서는 서비스 정보를 사용자에게 알려주거나 사용자가 서비스에 대해서 요청을 한다. 다음으로 인증(Authentication)단계에서는 자신이 원하는 서비스나 정보에 대해 접근권한을 요청하고 서비스 제공자는 권한에 대한 인증을 승인하거나 제한한다. 이 단계에서 상호인증이 이루어지면 지정된 경로를 통해 서비스가 제공된다. 레벨 설정(Level Configuration)단계에서는 사용자가 요청한 서비스나 정보에 대해서 다양한 보안레벨에 따른 권한 검사(privilege matching)를 통해 서비스 및 정보에 따른 접근 권한(Access authorization)을 부여한다. 마지막으로 종료(Deassociation)단계에서는 자신의 기록 정보 삭제 요청과 자신이 가지고 있던 다른 사용자 정보(위치, 집 주소, 주민등록번호)등을 삭제 후에 서비스를 종료한다.

4. 결론

앞으로 다가올 U-City환경에서는 도시 곳곳에 유비쿼터스 컴퓨팅 디바이스들이 내재되어 다양한 정보들을 실시간으로 수집하고, 이를 기반으로 우리에게 유용한 서비스를 제공해 준다. 하지만 도시 내에서 여러 경로를 오고가는 방대한 양의 정보는 그 성격에 따라 민감한 개인정보나 위치, 환경 등의 정보일 수 있다. 따라서 사용자 프라이버시침해를 최소화하고 안전한 U-City를 건설하기 위해서는 개인정보의 등급화와 그에 따른 적절한 관리가 필요하다. 본 논문에서는 개인정보의 민감성에 따라 등급을 설정하고 그에 상응하는 서비스 레벨을 분류하였다. 또한 실제 사용자가 어떤 서비스를 제공 받고자 할 때 인증, 보안레벨 부여 등 체계적인 절차를 제안하였다.

Acknowledgement

본 연구는 서울시 산학연 협력사업(CR070019)과 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성지원사업의 연구결과로 수행되었습니다.

참고문헌

[1] 한국정보보호진흥원, 2003 개인정보보호백서, 2003
[2] 이성몽, 유비쿼터스 컴퓨팅 환경에서 개인정보보호방법
[3] 한국정보보호진흥원, 유비쿼터스 프라이버시 보호 종합대책 수립, 2006
[4] 윤수진, U-City구현에 있어서의 개인정보보호