유비쿼터스 환경에서의 개인 프라이버시 보호

김정훈*, 홍만표*, 예홍진**
*아주대학교 정보통신전문대학원 디지털백신 및 인터넷면역시스템연구실
**아주대학교 정보통신전문대학원 인터넷보안연구실
e-mail:kjh3684@ajou.ac.kr

Personal Privacy Protection in Ubiquitous Environment

Jung-Hun Kim*, Man-pyo Hong*, Hong-Jin Yeh**
*Graduate School of Information and Communication, Ajou University
**Graduate School of Information and Communication, Ajou University

요 약

유비쿼터스 컴퓨팅 환경이 우리 생활에 밀접하게 다가오면서 결국에는 헤아릴 수 없을 정도의 엄청난 가치를 발생 시킬 것이다. 그러나 문제는 이와 같은 긍정적 영향 이면에는 이를 이용한 사회적 역기능 및 그로 인한 부정적 영향 또한 존재할 것이다. 개인 프라이버시 침해는 수많은 부정적 영향 중 가장 심각한 문제가 될 것이다. 본 논문에서는 이러한 개인 프라이버시 침해 중 매우 현실성 있고 실현 가능성이 있는 시나리오를 설정하여 기본적인 개인 프라이버시 보호 모델을 제안한다. 유비쿼터스 환경이 실현되면서 구현 가능성이 있는 전자명함 전달을 기반으로 개인 프라이버시 보호 모델을 설계하였다. 본 논문에서 제안한 모델은 유비쿼터스 환경에서 전자 명함을 전달할 때 개인의 프라이버시를 최대한 보장하면서 자신의 정보, 즉 전자명함을 안전하게 전달하는 방법이다. 향후 유비쿼터스 컴퓨팅 시대가 실현되어 전자명함 서비스가 우리의 생활 속 깊숙이 자리하고 있을 때 본 논문에서 제안하는 모델을 적용하면 개인 프라이버시 보호에 있어서 많은 문제들이 해결될 것으로 기대된다.

1. 서론

최근 유비쿼터스라는 단어로 함축되는 새로운 환경이 그 성장잠재력과 필요성을 인정받으며 산업 전반과 실생활에 걸쳐 다양하게 접목하기 위해 활발히 연구 되고 있다. 유비쿼터스는 단순한 정보기술이 아닌 철학적 변화이며 사회 구조의 변혁이다. 따라서 산업 전반의 생산·유통·기반뿐 아니라 개인 실생활의 행태까지도 변화시킬 것으로 예측되고 있다. 이를 반영하듯 국내에서는 지난 2003년 유비쿼터스 컴퓨팅 사업단이 출범하여 유비쿼터스 노드들이 주변 환경의 상황을 자율적으로 인지하여 사람에게 최적의 서비스를 제공할 수 있는 유비쿼터스 컴퓨팅 응용기술과 이를 위한 네트워크 기반 원천 기술의 개발을 목표로 활발한 연구를 진행하고 있으며, 대표적인 정보통신 선진국인 미국[1]·유럽·일본에서도 국가적인 지원을 바탕으로 유비쿼터스 컴퓨팅의 원천 기술 및 서비스 모델 개발을 위한 각종 프로젝트가 기관·기업·대학 등을 중심으로 수행되고 있다.

이와 같은 추세로 볼 때 유비쿼터스 컴퓨팅 환경은 머지않은 미래에 우리가 인지하지 못할 정도로 우리 생활 속에 파고들 것이다. 이런 변화는 분명 우리에게 큰 편의를 가져다 줄 것이며, 우리는 이러한 편의에 빠르게 적응하고 의존하게 될 것이다.

이러한 긍정적인 영향 이면에 이를 이용한 사회적 역기능 및 그로 인한 부정적인 영향 또한 존재할 것이라는 점이다. 그 중 유비쿼터스 컴퓨팅 환경에서 각 개인의 정보가 자신도 모르게 유출되는 개인 프라이버시 침해는 매우 심각할 것이다[2]. 개인 프라이버시 침해는 기존 환경에서도 많은 문제가 되고 있는 가운데 유비쿼터스 컴퓨팅 환경이 도래되었을 때 더욱 심각해 질 것이다[3].

본 논문에서는 개인 프라이버시를 보호하기 위한 모델을 제안하려고 한다. 제안하는 모델은 유비쿼터스 컴퓨팅 환경의 실현을 비추어 보았을 때 현실성

이 있고, 실현가능성이 있는 전자명함 서비스를 기반으로 하여 설계하였다. 기존 전자명함 서비스의 경우 종이 명함을 전자화 시켜 이 메일이나 웹 문서 등에 첨부하여 전달하는 것을 말한다. 그러나 유비쿼터스 컴퓨팅 환경이 실현되면 장소·상황·시간 등을 고려하여 개인 정보를 제공함으로써 개인이 장소·상황·시간을 인지하지 않고도 자신의 정보를 담은 전자명함을 제공할 수 있는 서비스가 필요하다. 이러한 상황에서 개인의 정보가 자신의 의도와 다르게 너무 많은 정보가 유출될 가능성이 높다. 본 논문에서는 유비쿼터스 컴퓨팅 환경에서의 전자명함을 전달 할 때 발생할 수 있는 개인 프라이버시 문제를 고려하여 개인 프라이버시를 최대한 보호할 수 있는 모델을 제안하려고 한다.

우선 2장에서는 유비쿼터스 컴퓨팅 환경에서 존재할 수 있는 프라이버시 침해 기술과 보호 기술에 대하여 살펴볼 것이며, 제안하는 개인 프라이버시 침해를 보호하는 기본적인 개인 프라이버시 보호 모델을 3장에서 설명할 것이다. 4장에서는 제안하는 모델이 유비쿼터스 컴퓨팅 환경에 적용되었을 때의 기대효과를 설명할 것이고, 마지막으로 결론은 5장에서 맺는다.

2. 관련연구

개인 프라이버시는 유비쿼터스 컴퓨팅 환경이 아닌 기존 환경에서도 매우 심각한 문제로 대두되고 있는 상황이다[2]. 사이버 테러 등으로 인한 개인 정보유출이 현재 정보화 사회에 위협을 주는 심각한 요소이다. 이러한 상황이 계속적으로 문제가 되고 있는 현재 법적으로의 대응도 불가피한 상황이다.

이번 장에서는 프라이버시 침해 요소가 어떠한 것이 있으며, 프라이버시 보호를 위한 기술에 대하여 알아본다. 추가적으로 기존 환경의 전자명함 서비스가 어떻게 서비스 되고 있는지를 알아보겠다.

2.1 프라이버시 침해

많은 기술들은 긍정적인 측면이 있는 반면 부정적인 측면도 가지고 있는 경우가 많다. 부정적인 측면으로 프라이버시를 침해하는 기술들도 있다. 예를 들어 교통 지능화 시스템(ITS), GPS, 위치기반시스템(LBS) 등은 사용자로 하여금 편의를 제공하는 기술들이다. 그러나 이러한 기술들을 이용하여 불법적으로 사용자의 위치 정보 추적을 할 수 있다. 또한, 쿠키, 스파이웨어, 웹 로봇, 웹 버그 등 정보수집 기술을 통하여 사용자의 정보를 수집하여 개인 정보를 유출함으로 인해 익명성 위협이라는 개인 프라이버시를 침해당할 수 있다.

2.1.1 익명성 위협

인터넷 관련 기술적 요소 중에 TCP/IP 주소, 이메일, PSN(Processor Serial Number), IPv6[4] 등은 익명성을 위협 할 수 있다[6].

2.1.2 정보 수집, 보호, 분석

정보수집, 정보보호, 정보분석 기술들은 많은 긍정적인 측면이 있는 반면 부정적인 측면도 존재하고 있다.

정보수집 기술은 쿠키, 스파이웨어, 웹 로봇, 웹 버그 등과 같은 기술들이 있다.

정보 분석 기술에서 가장 대표적인 기술로서 데이터 마이닝(Data Mining)이 있다. 이 기술은 대용량의 데이터를 패턴인식, 통계 등의 기법을 이용하여 분석함으로써 의미 있는 새로운 상관관계 및 경향들을 발견하는 프로세스이다. 이는 대체적으로 인터넷 마케팅 전략에 사용되고 있다.

정보보호 기술은 정보를 보호를 위해 접근권한 및 암호화를 함으로써 수많은 정보들을 보호하는 기술들을 말한다. 그러나 정보보호 기술 역시 긍정적인 측면이 있는 반면 부정적인 측면도 존재한다[6].

2.2 프라이버시 보호

프라이버시 보호 기술에서 가장 대표적인 것은 암호화 기술과 익명 기술이다. 암호는 외부의 접근이나 정보의 노출로부터 보호하는데 사용되는 일반적인 기술이고, 익명 기술은 정보의 노출을 보호하는 것이 주목적이 아닌 파일을 송수신 할 때 송신자와 수신자사이의 관계를 비밀로 하여 상호 프라이버시 보호를 위한 기술이라고 볼 수 있다.

프라이버시 보호 기술에는 크게 두 가지의 기술로 나누어 볼 수 있다. 첫 번째는 사용자 선택 기능에 의한 프라이버시 보호기술이며, 두 번째는 보호 메커니즘에 의한 프라이버시 보호기술이다.

2.2.1 사용자 선택에 의한 프라이버시 보호기술

사용자 선택에 의해 프라이버시를 보호하는 대표적인기술로서 P3P(Platform for Privacy Preference) 기술[7,8]이 있다. 이 기술은 익명성과는 관계없이 개인 정보 제공 시 정보 제공에 대한 이용자의 선택과 결정을 가능하게 해주는 기술로서 인터넷상의 개인 프라이버시 보호를 위한 기술적 해결 방안이다.

2.2.2 보호메커니즘에 의한 프라이버시 보호기술

보호 메커니즘에 의한 프라이버시 보호 기술은 침입차단 기술, 암호 기술 등과 같은 정보보호와 관련

된 기술들을 말한다. 앞에서도 언급한 바와 같이 정보 보호와 관련된 기술들은 프라이버시 침해 기술로도 활용되고 프라이버시 보호기술로도 활용되는 기술들이다.

3. 제안하는 개인 프라이버시 보호모델

기존의 전자명함 서비스의 개념은 앞에서 설명한 것과 같이 현재 보편적으로 사용되고 있는 종이 명함과 거의 흡사하다. 유비쿼터스 컴퓨팅은 사용자가 자신이 인지하지 않는 상황에서 자신이 원하는 정보를 남에게 정확하게 전달함으로써 사용자의 편리함을 지향하는 컴퓨팅 환경을 말한다. 따라서 제안하는 개인 프라이버시 보호 모델에서의 전자명함 서비스는 단순히 종이명함을 전자화 시킨 것이 아닌 사용자의 단말기에 저장되어 있는 사용자의 개인 정보를 장소·상황·시간에 고려하여 상대방에게 사용자가 미리 설정해 놓은 범위 내에서 상대방에게 서로의 개인 단말기를 통하여 전달하는 서비스이다.

제안하는 개인 프라이버시 보호 모델의 목적은 유비쿼터스 컴퓨팅 환경에서 전자명함을 전달하는 과정에서 상대방의 특성에 맞는 정보만을 제공함으로써 과다한 정보유출을 막으면서 개인 프라이버시 보호를 하는 것이다.

3.1 개인 프라이버시 보호모델의 가정

본 논문에서 제안하는 개인 프라이버시 보호 모델을 구성하기 위한 몇 가지 가정들이 있다.

■*전자명함 서비스는 1대1 개인 간에 이루어진다.*

■*모든 사용자는 자기 자신의 정보를 담고 있는 단을 수 있는 단말장치를 가지고 있다고 가정한다.*

■*단말장치를 이용하여 상대방에게 전자명함을 전달한다.*

■*각 사용자는 단말장치에 자신에게 맞는 정책을 설정한다.*

■*상대방 인증을 위해 사용되는 인증서는 단 한번만 사용하는 인증서 이다.*

■*개인 정보 유출의 범위를 제 3자에 의해 유출되는 것을 배제하고, 사용자가 의도하지 않은 상황에서의 유출을 말한다.*

■*각 단말기는 장소·상황·시간을 인지할 수 있다.*

3.2 개인 프라이버시 보호 모델

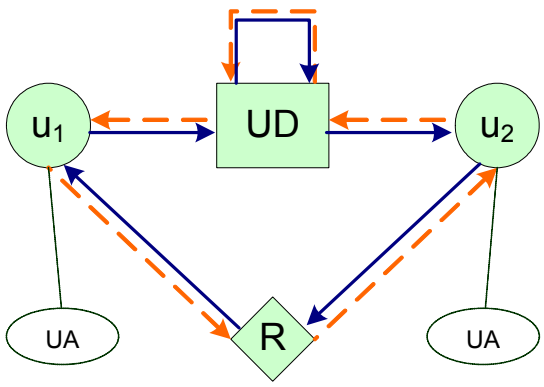
3.2.1 구성요소

개인 프라이버시 보호 모델을 정의하기 위해 몇 가지 구성요소 들이 필요하고 구성요소들 간의 상관관계는 다음과 같다.

- *U (User) = {u1, u2, u3, … , un}* : User는 제안하는 모델을 사용하는 주체를 말하며. 각 사용자를 u로 나타내고 u들의 집합을 U
- *P (Policy) = {p1, p2, p3, … , pn} (p1 ⊂ p2 ⊂ p3 ⊂ … ⊂ pn)* : User가 설정할 수 있는 정책을 p라고 나타내고 p들의 집합을 P
- *C (Certificate) = {c1, c2, c3, … , cn}* : 정책들을 적용하기 위해 상대방에게 배포하는 인증서를 c라고 나타내고 c들의 집합을 C
- *UAL (User's Attribute about Location) = {l1, l2, l3, … , ln}* : 사용자의 특성에 맞게 설정해 놓은 장소를 l이라고 나타내고 l들의 집합을 UAL
- *UAT (User's Attribute about Time) = {t1, t2, t3, … , tn}* : 사용자가 자신의 특성에 맞게 설정해 놓은 시간을 t라고 나타내고 t들의 집합을 UAT
- *UA (User's Attribute) = (UAL, UAT, P)* : 사용자의 속성(정책)을 UA
- *UD (User's Decisions) = (UA, C)* : 사용자의 결정이 해당되는 것으로 UA에 맞는 C를 배포하는 집합을 UD
- *R (Right) = True or False* : 사용자의 정책에 맞는 정보를 상대방에게 전달하기 위해 사전에 배포한 UD에 포함되어 있는 UA와 C가 사용자의 현재 상황과 일치하는지의 여부를 판단하는 것을 R
- *ci = (pi, li, ti)* : C의 속성인 ci 는 설정된 장소와 설정된 시간과 설정된 정책을 포함
- *Allow(c) = {l ∈ UAL, t ∈ UAT, c ∈C | (Now.l = c.l) and (Now.t ⊂ c.t)}* : l이 UAL의 원소이고, t가 UAT의 원소이고, c가 C의 원소일 때, 현재 사용자의 l과 c(상대방이 제시하는 certificate)에 포함되어 있는 장소가 일치하고, 현재 사용자의 시간이 c에 포함되어 있는 시간에 포함되어 있으면 상대방이 요구하는 정보를 제공하는 것을 Allow라고 표현한다.

3.2.2 구조

그림 1은 유비쿼터스 컴퓨팅 환경에서 전자명함 서비스를 제공하기 위한 개인 프라이버시 보호 모델의 구조를 그림으로 나타낸 것이다.



(그림 1) 개인 프라이버시 보호 모델의 구조

위 구조는 u1이 u2에게 c를 발급할 때 UA를 참조하여 UD에 의해 c가 발급이 되고, 발급된 c를 이용하여 u2는 u1에게 u1의 명함(개인 정보)을 요구할 수 있다. u2가 u1에게 명함을 요구하게 되면 R을 통하여 c가 이전에 사용하였던 것인가 아닌가를 판단하고, Allow(c)를 판단하여 True가 되었을 때 u1은 u2에게 자신의 명함을 제공하게 된다.

3.2.3 알고리즘

제안한 개인 프라이버시 보호 모델을 구현하기 위한 알고리즘은 상황에 맞는 인증서를 발급하는 과정과 인증서를 상대방으로부터 받아서 그 인증서가 유효한 것인지 아닌지를 판단하고 명함을 전달하는 과정으로 표현할 수 있다.

3.2.3.1 인증서 발급

인증서 발급은 사용자가 상대방으로부터 인증서 요청을 받았을 때 실행되는 현상으로 인증서 발급 과정은 표 1과 같은 알고리즘으로 표현할 수 있다.

<표 1> 인증서 발급을 위한 알고리즘

```
If (Receivedrequest Certification from ui){
    Wait User Decisions (UD)
    If (Receive UD){
        ci. pi = UD.UA.pi
        ci. li = UD.UA.li
        ci. ti = UD.UA.ti
        Send ci  to ui
    }
}
```

3.2.3.2 명함전달

명함전달은 사용자가 사전에 배포한 자신의 인증서를 받았을 때 실행되는 현상으로 명함 전달과정은 표 2와 같은 알고리즘으로 표현할 수 있다.

<표 2> 인증서 발급을 위한 알고리즘

```
If (Received published Certification by me from ui){
    Check R(){
        Check Used or not
        If (Used)
            Return false
        else{
            If (ci. li = Now.li && ci. ti = Now.ti)
                Return true
            Else
                Return false
        }
    }
    If(Check R())
        Send My information by ci. pi to ui
}
```

4. 기대효과

제안한 전자명함 서비스를 유비쿼터스 컴퓨팅 환경에서 적용을 한다면 사용자가 원하는 정보만을 상대방에게 제공함으로써 개인 정보유출이 최소화 될 것이며, 유비쿼터스 컴퓨팅 환경에 맞게 사용자가 인지하지 않는 상황에서 편리하게 자신의 제공하고 싶은 정보만을 제공함으로써 미래지향적인 모델이 될 수 있을 것이다. 더 나아가 전자명함 서비스뿐만 아니라 현재 연구 중에 있는 수많은 익명성 관련 연구에 이 모델을 추가하여 사용하게 되면 익명성과 개인 정보유출의 문제도 해결될 것으로 보인다.

5. 결론

전 세계적으로 유비쿼터스 컴퓨팅 환경을 실현하기 위해 수많은 연구들이 진행 중에 있다. 우리나라 역시 유비쿼터스 컴퓨팅 환경을 실현하기 위해 많은 연구들이 진행 중에 있으며, 그 중 유비쿼터스 컴퓨팅 보안에 대한 문제들도 수많은 연구가 진행 중이다. 보안 관련 문제 중 프라이버시 문제가 매우 심각한 문제가 될 것이다. 이 논문에서는 유비쿼터스 컴퓨팅 환경이 실현되었을 때 실현가능성이 있고, 현실성이 있는 전자명함 서비스 기반의 개인 프라이버시 보호 모델을 제안하였다. 이 모델을 유비쿼터스 컴퓨팅 환경에 적용 시켰을 때 사용자가 인지하지 않는 상황에서 자신이 원하는 정보만을 상대방에게 전달함으로써 사용자 개인의 프라이버시를 보호할 수 있게 하였다. 제안한 모델을 향후 익명성을 보장하기 위한 프라이버시 관련 연구에 활용되어 사용된다면 개인 프라이버시 보호 측면에서 많은 성과가 기대 된다.

참고문헌

1. http://www.epic.org/privacy/tools.html
2. 조동기, 김성우, "인터넷의 일상화와 개인정보보호", KISDI 이슈리포트, 정보통신정책연구원, 2003
3. Takagi Hiromitsu, "Open화와 프라이버시 확보(Japanese)", 유비쿼터스 정보사회에서의 안심·안전한 휴먼인터페이스에 관한 워크샵, 2003.03
4. 이인호, "정보통신기술의 발전과 프라이버시", 정보사회의 인권, 국가인권위원회 발간 자료집, http://www.humanrights.go.kr
5. 최경진, "쿠키의 활용과 프라이버시 보호", 한국정보보호진흥원, http://www.1336.or.kr/pds/p_11.hwp
6. 박춘식, "e-privacy와 정보보호기술", 정보보호학회지, 정보보호학회, 2004. 02
7. http://www.w3.org/P3P/brochure.html
8. 윤재석, "P3P 논의 현황과 문제점 및 국내 정책방향", 2001. 06, http://www.kisa.or.kr/Information_Security_Policy/Information_Security_Policy_m_02.html