유비쿼터스 컴퓨팅 환경에서 보안 시스템 설계

박용[O] 백청호* 전기환** 김영규** 김효남*** 김진봉****
강원대학교 컴퓨터과학과[O], 강원대학교 컴퓨터과학과*, 한림성심대학 IT계열**,
청강문화산업대학 컴퓨터소프트웨어과***, 안산공과대학 컴퓨터정보과****
ypark[O] @daum.net

Design of Security System in Ubiquitous Computing Environment

Yong Park[O]
Kang Won University, Computer Science[O]

요 약

유비쿼터스 네트워크는 기존의 네트워크와 같이 네트워크 인프라가 구축된 상태에서 통신을 수행하는 것이 아닌 인프라가 존재하지 않은 상태에서 각 단말들 상호간의 라우팅으로 데이터 송·수신 등의 통신 기능을 수행할 수 있는 형태의 네트워크 구조를 가지므로 유비쿼터스 컴퓨팅 환경에서 보안성을 제공한다는 것은 많은 어려움이 따른다. 본 논문에서는 프로토콜에서 기본적으로 보안성을 제공하기 위한 2가지 형태의 패킷 형태를 제시하였고, 이러한 구조를 통한 데이터 전송은 보다 빠른 데이터 처리를 수행할 수 있다.

1. 서 론

유비쿼터스 컴퓨팅(Ubiquitous Computing)은 라틴어에서 유래한 것으로 '언제 어디서나', '동시에 존재한다'는 뜻으로 그림 1과 같이 도로, 터널, 빌딩, 건물, 벽 등 모든 물리공간에 보이지 않는 컴퓨터를 집어넣어 모든 사물과 대상이 지능화되고 전자공간에 연결돼 서로 정보를 주고받는 공간을 만드는 개념으로 기존 홈 네트워킹·모바일 컴퓨팅보다 한 단계 발전된 컴퓨팅 환경이다.

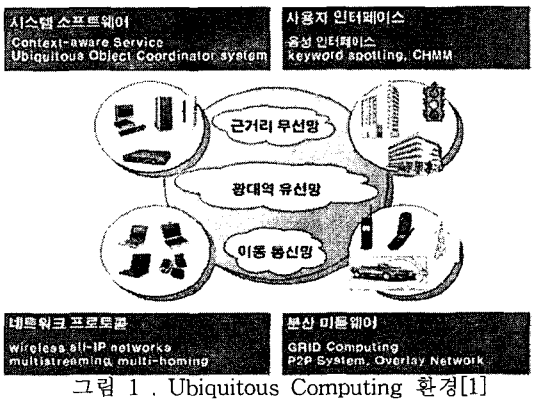

그림 1 . Ubiquitous Computing 환경[1]

이러한 유비쿼터스 컴퓨팅 환경을 위한 구성 요소는 산재한 자원들을 긴밀하게 묶어줄 수 있는 기반 네트워크 시스템, 자원을 효율적으로 관리하고 사용의 용이성을 제공하는 미들웨어 시스템, 미들웨어 서비스를 이용하여 각 자원의 Context를 지능적으로 파악하고 유연한 컴퓨팅 환경을 지속적으로 제공하는 시스템 소프트웨어, 사용자가 자연스럽게 컴퓨팅 자원에 접근할 수 있도록 하는 사용자 인터페이스 시스템 마지막으로 네트워크를 통한 안전한(Secure) 데이터의 전송을 위한 유비쿼터스 보안이 필요하다. 본 논문에서는 유비쿼터스 컴퓨팅 환경에서 보안성을 제공하는 보안 시스템을 설계하고자 한다.

2. 관련 연구

2.1 P3P를 활용한 보호 방법

P3P는 각 웹 사이트의 개인정보를 자동으로 검색 파악한 후 사용자의 공개 수준과 비교 판단할 수 있도록 하는 표준이다. 이 기술은 쿠키 제어를 통해 사용자가 직접 통제가능한 개인정보 보호 기술로 평가된다. 동작원리는 각 개인의 클라이언트 PC에 설정된 개인정보 공개수준을 설정하고 웹 사이트 방문시 해당 사이트의 개인정보보호정책 수준을 취득하여 이를 비교한 후 수준이 일치하는 경우는 자동 접속하지만 일치하지 않으면 경고 메시지를 출력하며 접속하지 않는다[2].

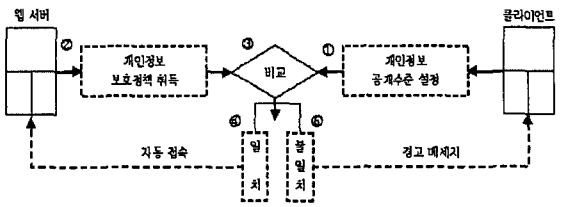

그림 2. 일반 환경에서 P3P 동작원리

유비쿼터스 환경에서도 이를 활용 할 수 있다. 개인이

소지한 Post PC나 스마트 핸드폰, RFID가 첨부된 개인 ID에서 자신의 개인정보를 공개할 수준을 미리 설정해 놓는다. 주변의 유비쿼터스 컴퓨팅 환경에서도 개인정보를 취득할 수준을 설정해 놓고 이를 비교해서 일치하면 개인정보를 취득하고 개인이 이를 낮게 설정하여 취득할 수 없는 경우는 취득하지 않는다. 궁극적으로 개인정보 노출 정도를 각 개인이 설정할 수 있는 것이다.

2.2 홈 게이트웨이를 활용한 보호 방법

홈 게이트웨이(Home Gateway)는 홈 네트워킹 시스템에서 가정과 외부 네트워크를 연결하는 부분이다. 또한 가정 내 여러 가지 기기들을 제어하는 주요 구심점이 될 것이다. 또한 가정 내의 유비쿼터스 컴퓨팅 환경에서 발생하는 정보들을 외부로 전달하게 되는 관문이 된다. 가정 내에서 발생하는 모든 개인정보는 홈 게이트웨이에서 제어하는 것이 타당하다.

홈 네트워킹은 유·무선을 통합하는 네트워킹 기술을 기반으로 가정의 기기들을 제어하고 관리하는 하드웨어나 기반 소프트웨어 그리고 정보가전기기들을 통합하여 외부의 인터넷 망에 연결하는 것을 총칭한다.

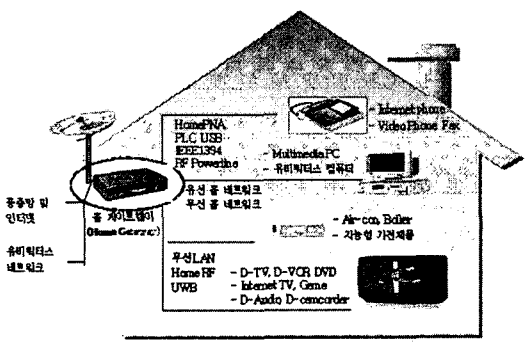

그림 3. 홈 네트워킹에서 홈 게이트웨이의 역할

홈 네트워킹에서는 유선 홈 네트워크와 무선 홈 네트워크 기술이 사용된다. 유선 홈 네트워크 기술에는 Home PNA(Home Phoneline Networking Alliance, 전화선), PLC(Power Line Communication, 전력선), 이더넷(Ethernet), USB(Universal Serial Bus), IEEE1394 등이 있고, 무선 홈 네트워킹 기술에는 무선 LAN(IEEE 802.11 등), Home RF(Radio Frequency), Bluetooth, IrDA(Infrared Data Association), UWB 등이 있다. 이때 홈 네트워킹에서 사용되는 네트워크를 가정의 맨 앞에서 제어할 수 있는 것이 홈 게이트웨이이다[3].

가정 내에서 사용되는 지능형 가전기기나 유비쿼터스 컴퓨팅에서 자동으로 개인정보를 취득하여 개인에게 편리한 서비스를 제공할 수 있다. 개인의 취향 및 개인이 주로 사용하는 기기 등의 정보가 개인정보로 분류될 수 있다. 하지만 외부에서 이것을 알게 되면 개인 사생활 침해가 될 것이다. 그렇기 때문에 이러한 정보를 외부로 전달되지 않도록 홈 게이트웨이에서 통제하며, 외부의 불법 접근도 차단할 수 있도록 기능을 부여한다.

2.3 법·제도를 통한 보호 방법

법과 제도를 제정하여 유비쿼터스 컴퓨팅 환경에서의 개인정보 취득과 이용을 제한해야 개인정보가 보호된다. 개인정보를 보호하기 위한 많은 기술과 시스템이 있다고 하여도 법과 제도가 이를 보호하도록 하지 않으면 개인정보보호 시스템은 시간이 지나면 또 다른 시스템에 의해 해킹되거나 취득될 것이다.

하지만 단순하게 개인정보 취득을 못 하도록 하는 것은 유비쿼터스 컴퓨팅 환경에 맞지 않는다. 개인에게 다양한 서비스를 제공하기 위해서는 개인정보 취득이 필수이기 때문이다. 결국 개인의 의사에 반하여 개인정보 취득을 못하도록 해야 하는데 이을 위하여 옵트 인(Opt-in)과 옵트 아웃(Opt-out)을 활용한다.

Opt-in과 Opt-out은 스팸 메일 차단을 위한 법과 제도에 속한다. Opt-in제도는 각 개인의 허락을 먼저 선행하여야 광고 메일 등을 발송할 수 있게 하는 제도이다. Opt-out은 개인의 허락을 받지 않아도 1회는 그냥 보낼 수 있다. 일단 보내진 메일을 수신한 개인이 수신거부를 하게 되면 더 이상 메일을 보내면 안 된다.

유비쿼터스 컴퓨팅 환경에서도 이를 활용하여 개인정보를 활용하는 시스템마다 Opt-in과 Opt-out을 선택적으로 적용할 수 있다. 개인에게 민감한 정보를 취득하는 시스템은 Opt-in 방식으로만 개인정보를 취득하도록 한다면, 개인정보는 유비쿼터스 서비스를 우선으로 하는 개인에게는 제공될 것이고, 이를 거부하는 개인은 개인정보 노출을 피할 수 있다.

2.4 보안 기술을 이용한 보호 방법

유비쿼터스 컴퓨팅 환경에서는 개인을 식별하는 기술이 RFID 칩이 내장된 신분증이 활용되는 것이 가장 일반적인 방법이 될 것이다. 신분증만으로 개인의 정당 여부를 판별하여 개인 서비스를 제공하게 될 때 신분증의 오용과 남용 및 불법 취득에 의한 사용시 큰 혼란에 빠지게 된다. 개인의 인식이 잘못되면 잘못된 유비쿼터스 서비스나 원하지 않은 유비쿼터스 서비스를 제공 받을 수 있기 때문이다. 결국 개인 식별 기술이 생체인식으로 보안적 식별이 되어야 하고 이를 활용한 데이터 송수신에도 암호화된 통신 네트워크를 이용하여 중간에 불법적인 접근을 막아야 한다.

생체인식(Biometrics)은 계측 가능한 신체, 습관성 행위 특성을 추출하여 기존에 등록한 내용과 동일 여부를 확인하는 기술 및 과정을 말한다. 생체인식 기술이 갖추어야 할 특징에는 보편성, 유일성, 영구성, 획득성 등이 있으며, 이용 가능한 생체인식 방법에는 지문, 홍체, 얼굴, 손모양, 정맥, 음성, DNA 등이 있다. 이러한 기술을 이용하여 정당한 개인을 확인한 이후에 개인정보의 송·수신이 이루어져야 한다.

이 때 전송되는 통신 데이터는 유선 상의 통신 암호화 기술인 SSL(Secure Socket Layer), PKI(Public Key Infrastructure) 등을 이용하고, 무선 통신은 w-PKI(wireless PKI), m-VPN (mobile VPN) 등의 보안 기술을 이용하여 중간의 불법적인 접근으로부터 보호할 수 있다[4].

3. 유비쿼터스 컴퓨팅 환경의 보안 시스템 구조

유비쿼터스 네트워크는 기존의 네트워크와 같이 네트워크 인프라가 구축된 상태에서 통신을 수행하는 것이 아니라 인프라가 존재하지 않은 상태에서 각 단말들 상호간의 라우팅으로 데이터 송·수신 등의 통신 기능을 수행할 수 있는 형태의 네트워크를 말한다. 따라서 네트워크에 참여하는 각 단말들은 기지국이나 AP의 도움 없이 자신들이 라우터, 서버의 역할 등을 모두 수행할 수 있어야 한다. 이러한 유비쿼터스 컴퓨팅 환경에서 여러 기기(Device)들 간의 통신을 수행하다보면 보안과 효율성 면에서 취약한 문제점을 가지게 된다. 그 이유는 유비쿼터스 컴퓨팅 환경에서는 신호를 받아서 상황 인식(Context aware) 처리기에 의해서 적절한 서비스를 제공한다. 만일 사용자가 많다면 기존의 방법으로 수행하면 권한이 없거나 수행할 필요가 없는 신호에 대해서도 유비쿼터스 컴퓨팅 시스템은 많은 오버헤드로 시스템이 바쁜(Busy) 상태에 있게 된다. 그래서 본 논문에서는 보안성을 제공하면서도 효율적인 처리를 위한 유비쿼터스 컴퓨팅 환경을 구축하고자 한다.

일반적인 유비쿼터스 컴퓨팅 환경의 네트워크 구조는 다음 그림 4와 같다.

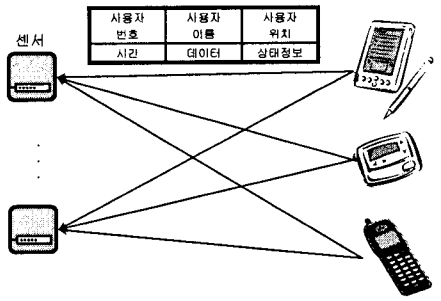

그림 4 기존 네트워크 구조

네트워크 구조는 기기간의 통신을 위해 여러 센서를 통해 사용자 번호, 사용자 이름, 사용자 위치, 시간, 데이터, 상태정보 등의 데이터를 전송한 후 전송이 이루어지는 구조를 가지고 있다. 이러한 구조의 단점은 여러 센서 통해 인증된 사용자는 통신하고자하는 데이터 전체를 한 번에 보내거나 아니면 다시 인증을 통해서만 전송해야 하는 문제점을 가지고 있다. 본 논문에서는 효율적인 전송을 위해 사용자 인증과 데이터 전송을 위한 시간을 나누어 처리함으로써 처음 한번만 인증처리하고 그 이후부터는 패킷의 처음에 사용자의 ID를 검색하는 것으로써 처리의 성능을 높이고자 한다.

사용자 ID	사용자 password	상태정보

그림 5. 사용자 인증을 위한 패킷 구조

사용자 인증번호	사용자 위치	시간	데이터	상태정보

그림 6. 데이터 전송을 위한 패킷 구조

패킷 구조에서 상태정보 필드는 사용자 인증을 위한 패킷인지 데이터 전송을 위한 패킷인지 구별할 수 있게 정보를 저장한다. 사용자 인증을 위한 패킷의 사용자 ID, 사용자 password, 상태정보 필드는 센서를 통해 얻은 후 상황 인식 처리기에서 인증 후 사용자 인증 번호를 다시 사용자에게 전송한 후 통신이 이루어지는 구조이다. 처음에는 인증 과정을 수반하지만 그 이후에는 할당된 사용자 인증 번호를 통해 통신을 수행함으로써 보다 빠르면서 보안성동 한 층 높일 수 있다.

4. 결론

유비쿼터스 네트워크는 기존의 네트워크와 같이 네트워크 인프라가 구축된 상태에서 통신을 수행하는 것이 아닌 인프라가 존재하지 않은 상태에서 각 단말들 상호간의 라우팅으로 데이터 송·수신 등의 통신 기능을 수행할 수 있는 형태의 네트워크 구조를 가지므로 유비쿼터스 컴퓨팅 환경에서 보안성을 제공한다는 것은 많은 어려움이 따른다. 본 논문에서는 프로토콜에서 기본적으로 보안성을 제공하기 위한 2가지 형태의 패킷 형태를 제시하였고, 이러한 구조를 통한 데이터 전송은 보다 빠른 데이터 처리를 수행할 수 있다.

참고문헌

[1] http://hpcs.sogang.ac.kr/research/bk2_01.php

[2] Cranor, L., "The Platform for Privacy Preferences 1.0. W3C Working Draft," www.w3.org/TR/P3P, May, 2000.

[3] ISO/IEC 8802-11, "Information Technology Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)," Specifications, 1999.

[4] F. Stajano, "Security for Ubiquitous Computing," First Security & Privacy Supplement to IEEE Computer, Apri. 2002.