유비쿼터스 네트워크에서 안전한 개인정보보호를 위한 프라이버시 보호 방안

김기수°
충북대학교 전자계산학과
caram12th@naver.com

The privacy protect Method for Private information security of Ubiquitous Network

kisoo Kim°
Chungbuk national University
Electronic calculation Department

요 약

유선망, 무선망, 통신 · 방송 융합 등이 이루어진 BcN망은 기존 접속망을 통한 보안성 위협이 나타날 수 있으며, 특히 개방형 망구조로 인해 쉽게 액세스가 용이하므로 공격을 받을 가능성이 높다. 따라서 서비스를 이용하는 사용자들의 개인 프라이버시 유출 위협이 존재하므로, 신뢰성 보장 및 접근 정보의 보호를 지원해주어야 한다. 본 논문에서는 유비쿼터스 네트워크에서 안전한 개인정보보호를 위한 프라이버시 보호방안을 제안하고 있다.

1. 서 론

BcN (Broadband convergence Network)과 NGN (Next Generation Network)은 용어의 명확성과, 방송융합 시점 등에서 다소 차이가 있지만, 통신·방송·인터넷이 융합된 품질 보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊어짐 없이 안전하게 광대역으로 이용할 수 있는 차세대 통합 네트워크라는 공통점을 갖는다. 또한 BcN/NGN에서는 이기종 망간 통합 및 여러 사업자간에 연동이 이루어지는 통합 네트워크이기 때문에 개별 통합망에서의 위협이 전체 통신망으로 확산될 수 있으며, 네트워크 대역폭의 증가로 전송 속도가 빨라져 악성 웜 등의 확산을 가속화 시킬 수 있는 부작용도 공통적으로 갖고 있다. 이에 유비쿼터스 사회를 앞당길 BcN/NGN 망의 발전과 함께 정보보호 문제는 간과할 수 없는 중요한 문제가 되고 있다.

이러한 개방 환경에서 서비스를 제공받는 사용자들은 개인정보 유출 위협에 처하게 된다. 정보의 위·변조 및 거짓 정보를 유포함으로써, QoS를 보장을 저해할 수 있다. BcN에서는 서비스 별로 과금이 이루어질 것으로 보이며 과금의 방식도 사용자가 사용한 시간을 근거로 하는 방식에서 패킷단위의 과금까지 다양한 방식이 도입될 것으로 보인다. 이러한 과금 정보가 별도의 망이 아닌 일반 데이터 망으로 전송될 경우 공격자들은 이러한 정보를 변경하거나 손상시킴으로써 서비스를 공짜로 이용하고자 시도할 것이다. 따라서 전달 계층에서의 데이터 전송에 있어 무결성을 지원해줄 수 있는 기법이 필요하게 된다. 통신하는 양단간의 신뢰성을 보장하는 문제, 이종망간의 상호 연동시 데이터 변조 방지 등이 필요하지만 이는 어디까지나 운영상의 에러에 대한 방안이지 악의적인 공격에 대한 대응 방안이 아니다. 이러한 공격에 대응하기 위해 패스워드의 복잡성이나 인증서 기반의 인증과 같은 강력한 인증 제어 체계, 중요 데이터의 암호화가 갖추어야 할 것이다. 본 논문에서는 안전한 개인정보보호를 위한 익명성 보호방안을 제시하여 보안상의 문제점을 해결하고자 한다.

본 논문의 구성은 다음과 같다.

먼저, 관련 연구로써 유비쿼터스 환경에서의 위협요소와 보안 요구사항을 정의하고, 3장에서 유비쿼터스 환경에서의 프라이버시 보호 기술을 설명하고, 4장에서 보장기술을 평가 후 5장을 통해 결론과 향후 연구 계획에 대해 언급하는 것으로 구성되어진다.

2. 관련 연구

2.1 유비쿼터스 환경에서의 위협 요소

유비쿼터스 컴퓨팅 환경은 기존의 유선망과 무선 인터넷, 무선랜, 블루투스, 홈네트워킹 등의 분야를 통합하는 통신 환경이라 할 수 있다. 유비쿼터스 환경에서 발생할 수 있는 위협으로는 장치의 절도 및 분실, Rogue AP, IP 스푸핑(Spoofing), DoS(Denial of Service)공격, 트로이목마, 웜, 바이러스, 신호방해 공격, 배터리 소진 공격 등이 있다.

표 2-1 유비쿼터스 네트워크 환경의 보안 위협

보안위협	침해유형	원인 및 문제점	대응방법
장치 분실 및 도난	기밀성, 인증	장치 소유자가 인증 정보 소유	사용자 인증, 암호화
Rouge 억세스	인증	불법접근	양방향인증
IP Spoofing	기밀성	무선신호 도청	암호화
DoS	가용성	가용성 침해	접근 제어
악성코드	가용성, 기밀성, 무결성	가용성, 비밀성, 무결성 침해	백신 프로그램
신호 방해 공작	가용성	통신채널 혼선	확산대역 주파수 호핑
배터리 소진 공격	가용성	빠른 배터리 소진	가용성
신원, 위치 노출	기밀성	프라이버시 침해	익명성

3. 유비쿼터스 환경에서의 프라이버시 보호 기술

이 장에서는 유비쿼터스 환경에서의 프라이버시 보장을 위한 익명성 보장 기술에 관하여 분석한다. 분석을 통하여 기존 프라이버시 보장기술이 네트워크 환경에서 유비쿼터스 환경으로 진화에 감에 따라 발생할 수 있는 새로운 문제점 도출과 그에 대한 해결 방안을 제시한다.

3.1 프라이버시 익명성 보장기술

개인정보보호 관련 산업에 대한 분석과 전망은 정보보호산업의 한 측면으로서 우선 개인정보보호 기술 현황에 대한 분석이 선행되어야 할 것이다. 개인정보보호기술은 일반적으로 기술적인 개인신원확인자(personal identifier)에 대항하여 인터넷상에서 이용자의 익명성을 보호하는 데에 초점이 맞춰지고 있다. 현재 주로 사용되고 있는 개인정보보호기술은 다음과 같다.

① SSL(Secure Socket Layer), WTLS 등 암호화 기술(Encryption Tools)

② 프라이버시정책생성기(Privacy Policy Statements Generator : P3P) 등 정책협상기술(Policy Association)

③ 스팸 필터링(Spam Filtering) 쿠키 컷터(Cookie Cutters), 스파이웨어 킬러(Spyware Killers)등 필터링 기술(Filtering Tools)

④ Anonymizer 등 익명성 기술(Anonymizers Tools)이 있다.

익명성 기술은 프라이버시 보호가 전 세계적인 이슈로 등장하면서 이론적 연구가 크게 부각되고 있으며, 익명성 기술은 전자서명 기반, Mix-Network 기반 그리고 기타 기술들이 있다.

가. 서명 기반 익명성 기술

1) 그룹 서명

그룹 서명은 1991년 D.chaum과 Van Heyst에 의해 처음으로 제안되었다. 그룹 서명은 그룹의 구성원이 그룹을 대표하여 서명하며, 서명자가 누구인지 알려져서는 안되고, 분쟁 시 그룹 관리자에 의해 서명자의 신원이 밝혀져야 한다. 그룹 서명은 효율성 제고와 부가기능 향상이라는 두 가지 측면에서 발전하여 왔다.

2) Ring 서명

Ring서명은 2001년 Rivest, Shamir와 Tauman에 의해 제안되었다. Ring서명은 그룹서명과 거의 유사하면, 그룹 관리자가 없다는 점이 다르다. 따라서 서명자가 누구인지 추적할 수가 없다. Ring 서명의 응용으로는 내부 고발을 생각할 수 있다. Ring 서명을 하면 고발자에 대한 무조건적인 익명성이 지켜진다.

3) Blind 서명

Blind 서명은 프라이버시 보호를 위한 기본 프리미티브로서 전자화폐를 위한 프로토콜이며, 1981년에 chaum이 RSA에 기반을 둔 프로토콜을 제안하였다. Blind 서명이란 사용자가 메시지에 대한 서명을 받는 경우, 서명자는 서명한 메시지에 대한 정보를 전혀 알 수 없도록 하며, 사용자는 메시지 하나에 오직 한번만 유효한 서명을 받아야 한다. 사용자에게 완벽한 익명성을 주기 때문에 전자 투표에 이용되기도 한다.

나. Mix-Network 기반 익명성 기술

Mix network는 암호화된 메시지를 입력받아 재암호화한 후 랜덤한 순서로 출력하는 방식으로 입력 메시지와 출력 메시지간의 대응관계를 알 수 없게 한다. 이것은 anonymous 전자우편, 웹 브라우징, 익명화 자블 시스템 등에 응용된다.

1) Anonymizer: 웹 사용자의 인터넷 이용에 관련된 정

보를 숨기는 기술임. Anonymizer Inc.의 웹 사이트를 통해 제공된 IP주소와 같은 사용자의 인터넷 이용 정보를 숨기는 툴로써 유료 서비스와 무료 서비스가 있음

2) Onion Routing: Mix-network를 통하여 데이터 트래픽의 내용을 숨기는 기술임. 네트워크상에서 패킷(packet)의 익명성을 유지하는 것을 목표로 개발한 안전한 통신 제공 시스템 구조로서, 자동적으로 사용자의 통신 내용에 대한 익명성 보장

3) Crowds: 라우팅되는 HTTP 트래픽의 내용을 숨기는 기술임. 인터넷(특히, 웹을 사용한 네트워크)에서 사용자의 익명성을 보호하기 위해 AT&T Labs에서 개발한 시스템으로, 암호화를 사용하여 통신하는 데이터 트래픽이 어떤 전달 과정을 거쳐 서버까지 오게 되었는지에 대한 라우팅 경로 정보를 알수 없게 함으로써, 송신자의 익명성 제공

4) Janus: URL을 암호화하여, 클라이언트와 서버의 익명성을 동시에 제공하는 Proxy서버 기술임. 2001년에 개발된 Janus는 최초로 서버의 익명성을 제공하는 기술로, 전자메일을 추적할 수 없는 방법에 기반하여, 사용자가 공개키 암호 알고리즘을 이용하여 웹을 익명으로 사용할 수 있으면서, 서버의 IP주소와 호스트 이름을 숨겨 서버의 익명성도 제공하는 시스템임.

5) TAZ(Rewebber network): URL을 암호화하는 것뿐만 아니라, 브라우저와 원래의 서버 사이에서 전송되는 데이터 스트림까지 암호화 함으로써 데이터에 대한 무결성 및 보안을 제공하는 기술임. 이 기술은 Janus와 같은 방법으로 암호화를 하여 사용자가 요청한 페이지들을 전송함으로써, 공격자가 사용자의 어떠한 웹 페이지의 링크를 선택하더라도, 사용자가 누구인지 알 수 없게 되며, Janus의 문제점으로 지적되었던 데이터 트래픽의 암호화를 제공한다.

다. 기타

1) Anonymous Credential

Anonymous Credential 시스템은 pseudonym시스템이라고도 불리며, 1985년 Chaum에 의해 제안되었다. 이 시스템은 기관과 사용자로 구성되며 기관은 사용자의 가명(pseudonym)만을 알고 그에 대한 Credential을 발급할 뿐 사용자의 신원에 대해선 알 수 없다. 한 사용자가 여러 개의 가명을 사용할 수 있고, 반대로 한 기관이 사용자의 가명에 대해 발급한 Credential을 다른 기관에 사용할 수 있다. 기관은 Credential을 받은 사용자의 가명 이외에는 어떠한 정보도 알 수 없으므로 사용자의 프라이버시를 보호한다.

2) Threshold Cryptography

유비쿼터스 환경에서는 수많은 컴퓨팅 디바이스들이 잠시 동안 그룹을 이루었다가 흩어지는 일이 반복될 것이므로 전통적인 암호학으로는 접근할 수 없다. 이런 상황에 대한 해결책으로 Threshold Cryptography가 유력하다. Threshold Cryptography는 분산 암호라고도 한다. 1979년 Shamir가 최초로 마스터 비밀키에 대한 비밀 공유 문제를 다루었다. 마스터 키를 한 사람에게 맡겨 놓는 것은 정보보호 차원에서 매우 위험하다. 그러므로 키에 대한 정보를 모두에게 나누어서 위험을 줄이려는 것이다.

3) 익명성이 보장되는 인터넷 검색 AN.ON 프로그램

이 프로그램을 컴퓨터에 설치하면 웹브라우저가 설치되기 전에 먼저 프록시가 설치되어 서버에 대한 문의사항 모두를 암호화한다. 이렇게 암호화된 메시지는 첫 번째 다단계 혼합기를 거쳐 뒤섞인 형태로 전달된다. 따라서 해당 프로그램의 제공자로차도 발신자 메시지의 최종 목적지를 알 수 없게 된다.

4. 프라이버시 보장기술 평가

이 절에서는 프라이버시 보장기술을 평가하기 위해 익명성 보장 기술 프라이버시 보장 기술을 비교평가한다.

1. 익명성 보장 기술 평가

정보의 노출 자체와는 무관하게 정보와 소유자간의 관계나 송주신 자간의 관계를 비밀로 하여 사용자의 개인정보보호를 제공하는 기술로 사용자들간의 비연결성을 통하여 익명성을 제공하는 기술들이 필요하다. [표 4-1]에서는 익명성 보장 기술들을 Mix Network 기반, 서명기반, 기타로 구분하여 익명성 보장 기술을 비교한다.

표 4-1 익명성 보장 기술 비교

기법		활용분야	익명 강도	효율성
Mix Network 기반	Anonymizer	Web	중	상
	Onion routing	Web	상	상
	Crowds	Web	상	하
	Janus	Web	중	중
	TAZ	Web	중	하
서명 기반	그룹서명	멤버관리	하	중
	Ring서명	다이바스 관리	중	중
	Blind서명	전자화폐	상	하
기타	Anonymous Credential	인증서	중	중
	Threshold Cryptography	키관리	중	상

[표4-1]처럼 프라이버시는 익명성과 밀접한 관계가 있다. 프라이버시는 대중속에 섞여 구분되지 않는 한 보장되지

만, 반대로 익명성을 악용한 불법적인 행위를 막아야 한다. 따라서 익명성 보호를 위한 암호 프로토콜은 법적인 분쟁이 있을 때를 대비한 추적 기능도 포함하는 경우가 많다.

5. 결론 및 향후 연구과제

본 논문에서는 차세대 네트워크 환경인 유비쿼터스에서 개인정보보호를 위한 기술적 정보보호 방안을 제시하였다.

- 유비쿼터스 관련 보안기술을 기반으로 유비쿼터스 환경 특성 및 위협요소를 분석하고 이를 통하여 유비쿼터스 환경에서의 개인정보보호를 위한 보안 요구사항을 도축하였다.
- 유비쿼터스 환경에서 익명성을 기반으로 프라이버시 보장기술에 대하여 분석하고 기존 문제들의 문제점과 개선사항을 제시하였다.

향후의 과제로는 홈네트워크, 텔레메틱스 및 휴대인터넷 등에서의 프라이버시 보호 방안에 대한 연구를 진행할 계획이다.

참고문헌

남택용, 장종수, 손승원 "유비쿼터스 환경에서의 개인정보보호 기술", 전자통신동향분석, 통권 91호, 제20권 제1호, pp.54~62. 2005.2

서동일, "IT839전략 추진을 위한 정보보호 기술", ITA 주간 기술동향, 1179호, pp.24~35, 2005.1.19

서동일, 김광식, 장종수, 손승원, "IT839전략 추진을 위한 정보보호 기술 개발 방향", 전자통신동향분석, 통권 91호, 제 20권 제1호, pp1~8, 2005.2