모바일 디바이스를 위한 경량화된 인증·인가·과금에 관한 연구1)

강수영*, 여상수**, 박종혁***
*한국인터넷진흥원 보안성평가팀
**목원대학교 컴퓨터공학부
***서울산업대학교 컴퓨터공학과
e-mail: bbang814@paran.com

A Study on Lightweight Authentication· Authorization·Accounting for Mobile Device

Soo-Young Kang*, Sang-Soo Yeo**, Jong Hyuk Park***
*IT Security Evaluation Lab, Korea Internet and Security Agency
*Divison of Computer Engineering, Mokwon University
**Department of Computer Science and Engineering, Seoul National University of Technology

요 약

IT 기술은 인터넷 및 휴대 디바이스의 발전으로 인해 유비쿼터스 환경으로 발전해 나가고 있다. 이와 같은 변화는 사용자들에게 다양한 서비스를 제공될 것이며, 사용자들은 모바일 디바이스를 이용하여 이동하면서도 서비스를 받고자 하는 요구가 증대되고 있다. 그러나 현재의 발전 예상과 다양한 서비스와는 반대로 무선 환경이라는 특성으로 인해 기존의 유선망보다 다양한 위협사항 및 취약점을 가지고 있다. 즉 무선 환경에서 모바일 디바이스에 대한 스니핑, 도청, 서비스거부 공격, 중간자 공격, 비인가 장비 공격, 악성소프트웨어 감염 등의 보안 취약성을 내포하고 있으며, 또한 기존의 무선 환경이 가지는 위협사항을 그대로 가지고 있어 모바일 디바이스 보안에 대한 연구는 매우 중요한 실정이다. 이러한 문제점을 해결하는 방안으로 기존의 유선망뿐만 아니라 비약적으로 발전하고 있는 무선망의 WiBro, Mobile IP 등과 같은 다양한 서비스 및 프로토콜 상에서 안전하고 신뢰성 있는 인증・인가・과금을 체계적으로 제공하도록 경량화된 디바이스 보안 기술에 대한 연구를 수행하고자 한다.

1. 서론

현대사회는 IT 기술의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 u-지식사회라는 새로운 문화적 변환기를 맞이하고 있다. 이와 같은 변화는 현대 사회에서 디지털화의 가속 및 통신 인프라의 확충 등으로 인해 IP 네트워크로 연결되어 영상 및 음성 정보를 서로 공유할 수 있는 환경이 제공 되고 통합 서비스에 대한 수요가 증가하고 있다. IP 네트워크를 통해 IPTV를 제공받는데 있어 IPTV는 불법제어, 콘텐츠 불법 유통, 서비스 도용, 비인가자 접근 등의 문제점과 더불어 스니핑, 도청, 서비스거부 공격, War Dialing 공격, 중간자 공격, 비인가 장비 공격, 악성소프트웨어 감염 등의 보안 취약성을 내포하고 있다. 이러한 여러 취약점이 존재함에 따라 본 연구에서는 모바일 IPTV 서비스 제공을 위한 AAA 메커니즘에서의 가입자 인증 기술에 관한 연구와 병합하여 진행함으로써 차세대 모바일 IPTV에서의 가입자 측면의 안전성과 효율성을 제공할 수 있도록 하였다.

1) 이 논문은 2OO8년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (KRF-2008-331-D00580).

2. 기존 문제점

국내・외에서는 디바이스에 대한 인증・인가・과금에 관한 연구가 활발히 진행되고 있다. AAA 인증 서버를 통해 인증을 수행하고 있으나 핵심 요소들에 대한 연구는 모바일 환경의 다양한 요구사항을 만족할 수 없으며, 모바일 환경에 적용하기에는 부적합하여 경량화된 핵심 보안 기술이 필요한 실정이다. 이러한 경량화된 핵심 보안 기술에 대한 연구가 선행되지 않는다면, 개인의 프라이버시 침해뿐만 아니라 모바일 환경을 위한 다양한 서비스 적용에 많은 어려움이 발생하게 된다. 이로 인해 모바일 환경으로의 발전에 있어 경량화된 핵심 보안 기술에 대한 연구는 반드시 선행되어야 하며, 다양한 문제점과 해결방안에 대한 연구를 진행하여 한다. 본 연구는 차세대 모바일 환경에서 보안 기술 개발뿐만 아니라 서비스 발전의 밑거름으로 시장경제 발전과 국가 경쟁력 확보를 위한 선도적 연구가 될 것으로 사료된다.

3. 제안 연구

본 과제에서는 모바일 환경에서 안전하고 효율적인 경량화된 디바이스 인증・인가・과금 기술을 연구하여 차세대 유비쿼터스 환경을 선도할 수 있는 연구를 수행하고자 한다. 이를 위해 연구의 기술을 3가지 분야로 구성하여 추진하고자 한다.

첫째, 모바일 디바이스를 위한 경량화된 인증 기술 연구를 수행함에 있어서 연구 동향 및 인증 기술을 분석하고 모바일 디바이스를 위한 보안 요구 사항을 도출해야 한다.

둘째, 익명성을 지원하는 ID 기반 티켓을 이용한 인가 기술을 연구하는 것은 티켓 기반, 익명화 기술, ID 기반 기술을 분석하고 익명성을 위한 보안 기술의 필요성 및 중요성을 도출하여 ID 기반 티켓을 이용한 인가 기술을 연구해야 한다.

셋째 로밍환경에서 계층적 방식을 이용한 과금 기술 연구 및 통합 AAA 기술을 연구하는데 있어서 로밍환경에서 디바이스 취약성 및 과금 서비스 필요성을 분석하고 계층적 방식을 이용한 과금 요구 사항 및 기술을 분석해야 한다.

제안 연구는 다음과 같은 중요성을 내포하고 있다.

◈ 모바일 환경 구축에 필요한 핵심 보안 기술 : 차세대 모바일 환경 구축을 위해서는 다양한 서비스 분야에서 다양한 요구사항을 만족할 수 있는 보안 기술에 대한 연구가 수행되어야 한다. 특히 모바일 디바이스를 위한 경량화된 인증 기술 및 익명성을 지원하는 ID 기반 티켓을 이용한 인가 기술과 로밍 환경에서 안전한 과금 기술의 연구는 모바일 환경의 보안을 위해 필수 요소기술 이다. 또한 인증・인가・과금 기술을 통합한 AAA 기술은 향후 차세대 모바일 환경의 다양한 서비스에 활용할 수 있다. 따라서 안전한 모바일 환경을 위한 통합 AAA 기술은 다양한 서비스 창출뿐만 아니라 차세대 모바일 시장을 장악할 수 있는 핵심 보안 기술이다.

◈ 국가 최고 핵심 산업 및 국가경제 성장동력기술과 직접 관련된 연구 주제 : 정보통신산업협회에서 발표한 통계에 따르면 정보통신서비스산업 매출액이 증가세를 보이고 있으며, 무선통신서비스의 매출액도 지속적인 증가세를 나타내고 있다. 따라서 차세대 모바일 환경이 도래하면 디바이스를 이용한 다양한 서비스 이용이 증가할 것이며, 이에 따른 보안 기술에 대한 연구는 모바일 서비스 보안 기술의 우위를 선점할 수 있는 매우 중요한 연구 과제이다.

또한 제안 연구는 디바이스를 위한 경량화된 인증 기술을 연구함으로써 모바일 환경에 적용할 수 있으며 사용자 측면과 서비스 제공자 측면의 보안을 모두 만족할 수 있다. ID 기반 티켓을 이용해서는 인가 기술에 대하여 연구함으로써 오버헤드 및 빠른 로밍을 제공할 수 있으며, 익명성을 지원하는 기술을 연구함으로써 사용자 프라이버시를 보호할 수 있다. 계층적 방식의 과금 방식을 이용하는 것은 로밍 환경에서 서버의 오버헤드를 줄일 수 있으며, 안전한 과금 서비스를 제공할 수 있다는 장점이 있다.

4. 결론

동일한 서비스를 지속적으로 제공받을 수 있는 차세대 모바일 환경이 도래되고 있다. 이러한 상황에서 모바일 환경에 적합한 보안 기술의 개발은 아무리 강조해도 지나치지 않을 것이다. 본 연구에서는 도래하는 차세대 모바일 환경에서 디바이스를 위한 인증・인가・과금 기술을 개발하여 다양한 응용 서비스 및 기술 선점을 위한 Killer-Application으로 활용하는 것을 목표로 한다. 따라서 본 연구의 최종 목표는 모바일 디바이스를 위한 경량화된 인증 기술 연구와 익명성을 지원하는 ID 기반 티켓을 이용한 인가 기술 연구 및 로밍 환경에서 계층적 방식을 이용한 과금 기술을 연구하여 최종적으로 차세대 모바일 환경에서 안전하고 효율적인 경량화된 디바이스 통합 AAA(Authentication : 인증, Authorization : 인가, Accounting : 과금) 보안 기술 연구를 목표로 해야 할 것이다.

참고문헌

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," CRYPTO'84, pp.47-53, 1984.

[2] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service," RFC 4120, 2005.

[3] D. Harkins, D. Carrel, "The Internet Key Exchange(IKE)," RFC 2409, 1998.

[4] Gwanyeon Kim, Chinu Lee, Sehyun Park, Ohyoung Song, and Byungho Jung, "A Study on Mobile Commerce AAA Mechanism for Wireless LAN," HSI 2003, pp.719-724, 2002.

[5] H. S. Kim, S. W. Lee and K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating Systems Review, Vol. 37, No. 4, pp.32-41, 2003.

[6] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electronics Letters, Volume 38, Issue 12, pp.554-555, 2002.

[7] Joaquín Torres, Antonio Izquierdo, Arturo Ribagorda, Almudena Alcaide, "Secure Electronic Payments in Heterogeneous Networking: New Authentication Protocols Approach," ICCSA, pp.729-738, 2005.

[8] Jong Sik Moon, Im Yeong Lee, "A Study on Ticket-based AAA Mechanism Including Time Synchronization OTP in Ubiquitious Environment" , ICCSA 2007, pp.666-677, 2007.08