유비쿼터스 환경에서 TMUCert를 이용한 안전한 지불방식

조영복° 김형도 이상호
충북대학교 네트워크보안 연구실
{bogi0118°, archiroad shlee}@netsec.cbnu.ac.kr

A Secure Payment using TMUCert for Ubiquitous Computing

Youngbok Cho° Hyungdoh Kim Sangho Lee
Dept. of Network Security Laboratory Chungbuk National Univ.

요 약

최근 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경에 대한 연구가 활발히 진행되면서 의료복지, 교통환경, 금융관리 등 다양한 서비스가 제공되고 있다. 유비쿼터스 환경에서 제공되는 다양한 서비스를 위해서는 개인 프라이버시보호를 위한 안전한 지불방식이 요구된다. 기존 지불 프로토콜은 상호 인증을 위해 사용자와 서비스제공자 사이에 개인정보를 전송한다. 이것은 안전성 측면에서 개인 프라이버시 보호의 취약점을 가지고 있다.

따라서 이 논문에서는 지불프로토콜에서 개인프라이버시 보호의 취약점을 보호하기 위해 *TMUCert*라는 임시이동 사용자인증서를 신뢰기관으로부터 발급받아 사용한다. 사용자가 원하는 서비스에서 지불만으로도 사용가능한 컨텐츠 서비스를 이용하기 위해 *TMUCert*을 사용하여 불필요한 개인정보 노출을 방지하여 개인 프라이버시를 보호해 준다. *TMUCert*는 기존 인증서와는 달리 개인정보 노출없이 개인프라이버시를 보호하고 익명성을 제공해 준다. 또한 공개키를 효율적으로 공유할 수 있도록하여 이동성을 동시에 만족시켜 유비쿼터스 환경에서의 안전한 지불 프로토콜을 제공하도록 한다.

1. 서 론

유비쿼터스 환경에 대한 관심이 높아지면서 유비쿼터스의 두 가지 분야인 유비쿼터스 컴퓨팅과 유비쿼터스 네트워크를 기반으로 물리공간을 지능화함과 동시에 물리 공간에 펼쳐진 각종 사물들을 네트워크로 연결시키기 위해 현재 활발히 연구 중에 있다[1]. 유비쿼터스 환경에서는 의료복지, 교통환경, 금융관리 등의 다양한 서비스 사용시 중요한 문제는 프라이버시 보호와 이동성이 제공되어져야 한다[2]. 사용자는 상품구매 뿐만 아니라 모든 서비스 사용에 있어 서비스제공자에게 개인정보를 보낸다. 이것은 유비쿼터스 환경에서 대두되는 문제 중 개인프라이버시 보호에 취약함을 보여준다[3].

이 논문에서는 이런 문제를 해결하기 위해 *TMUCert* (Temporary Mobile User Certificate)라는[4] 임시이동 사용자 인증서를 사용하여 상호 인증을 제공 한다. 제안하는 지불프로토콜은 컨텐츠를 제공받거나 서비스를 제공 받을때 서비스제공자가 사용자의 신원을 알 수 없다. 다만 사용자가 서비스제공자의 신뢰기관으로부터 받은 *TMUCert*을 통해 정당한 사용자임을 확인할 수 있게 된다. 따라서 유비쿼터스 환경에서의 개인프라이버시 보호를 제공하기 위해 *TMUCert*을 사용하여 안전한 지불 프로토콜을 제안한다.

이 논문의 구성은 다음과 같다. 2장에서는 유비쿼터스 환경과 *TMUCert*에 대한 관련연구 3장에서는 유비쿼터스 환경에서 개인프라이버시를 보호하는 안전한 지불프로토콜을 제안한다. 4장에서는 제안한 프로토콜의 안전성을 평가하여 마지막으로 5장에서는 결론 및 향후연구에 대해 기술한다.

2. 관련연구

2.1 유비쿼터스 환경에서의 지불방식

이 논문에서는 아래와 같이 유비쿼터스 환경을[5] 설정한다.

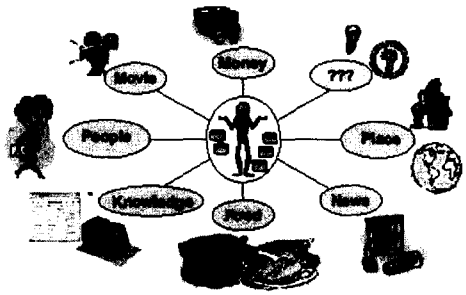

그림2-1 유비쿼터스 환경

유비쿼터스 환경에서 제공되는 다양한 서비스 중 지불 프로토콜은 크게 사용자(지불자), 서비스제공자(상인), 지불게이트웨이(은행)로 나누어 설계할 수 있다[3]. 지불 시스템의 요건은 사용자가 지불에 참여하기 위하여 가지고 있어야 할 정보는 최소로 되어야 한다. 지불 과정이 일어날 때 사용자, 서비스제공자 간에 전송되는 메시지의 크기가 최소로 가지고 있다.[6]

이 논문에서 유비쿼터스 환경에서의 *TMUCert*를 사용한 안전한 지불방식을 설명하기 위해 다음 두 가지 가정을 한다.

[가정1] : 사용자는 유비쿼터스 환경에서 주어지는 다양한 서비스를 사용하기 위해 이미 안전하게 사용자 인증이 이루어진 상태이다.

[가정2] : 사용자 인증은 ID-basde 기반의 인증방식을 사용한다.

2.2 임시 이동사용자 인증서(TMUCert)

[4]에서 제안한 임시 이동 사용자 인증서는 ASPeCT의 AIP(Authentication and Initialization of Payment)프로토콜[7]에서 이동 사용자가 서로 다른 도메인의 서비스 제공자에게 인증서를 검증할 수 있는 공개키를 보다 효율적으로 공유할 수 있도록 한 것이다. [그림2-2]에서 임시 이동 사용자 인증서 발급 프로토콜 모델을 설명한다.

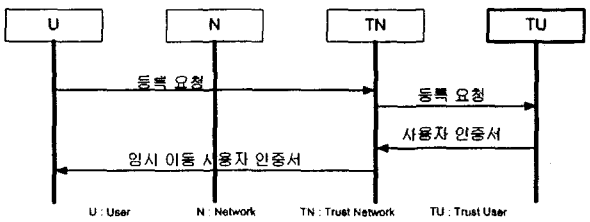

그림2-2 TMUCert 발급 프로토콜

U는 TN에서 발급한 임시 이동 사용자 인증서를 사용하여 N의 도메인에서 서비스를 받을 수 있다. 사용자는 다른 서비스를 사용하기 이전에 TN에서 발급하는 $TMUCert$를 발급받는 전처리 과정을 거쳐야 한다. 이 논문에서 사용자와 디바이스에 대한 인증은 향후연구로 남겨두고 유비쿼터스 환경에서는 $TMUCert$ 발급과정에서 디바이스 사용에 대한 사용자 인증이 이루어졌다고 가정한다.

3. 제안 프로토콜

이 논문에서 제안하는 방식은 유비쿼터스 환경에서 단순한 컨텐츠 이용과 같은 서비스 이용시 사용자 프라이버시보호 및 이동성을 제공하는 안전한 지불방식이다 . 제안 프로토콜의 안전성은 유한군G와 생성원 g에서 이산대수문제가 어렵다는 가정을 근거로 한다. [그림3-1] 제안 프로토콜은 각 참여자와의 세션키 설정은 Diffie-Hellman 키 설정 방식을 사용 한다

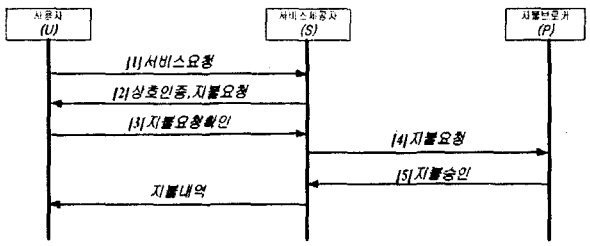

그림3-1 제안프로토콜

제안하는 프로토콜은 사용자가 서비스제공자에 서버에 접속을 하여 서비스를 요청하면서 단계1이 시작된다. [표 3-1]은 제안 프로토콜에서 사용되는 계수의 설명이다.

표3-1시스템 계수

ID_i	i의 식별자
g^a	A의 공개키
K_{AB}	A와 B의 세션키
T_a	A에 의해 생성된 타임 스탬프
PM_{info}	지불정보(서비스종류 or 상품정보)
$info$	서비스 요청정보
$Cert_a$	a의 인증서
$TMUCert$	사용자의 임시인증서

지불프로토콜의 동작과정은 아래와 같다.

단계1. 서비스 요청

$g^u, ID_S, info$

U는 S에게 사용하고자 하는 서비스를 요청

단계2. 상호인증, 지불요청

$r, h(K_{US}, r, ID_S), PM_{info}, T_S, Cert_S$

S는 U에게 상호 인증시 사용될 자신의 인증서와 지불요청

단계3. 지불요청확인

$\{Sig_U(h(g^u, g^s, r, ID_s, T_s, PM_{info})), TMUCert\}K_{US}$

$\{Sig_U(h(ID_U, ID_S, T_U, PM_{info})), TMUCert, T_U, PM_{info}\}K_{UF}$

U는 S와 상호인증을 위해 U의 $TMUCert$과 S의 $Cert_s$을 이용하고 지불정보를 전송

단계4. 지불요청

$\{TMUCert, ID_S, PM_{info}\}K_{SP},$

$\{Sig_U(h(ID_U, ID_S, T_U, PM_{info})), TMUCert, T_U, PM_{info}\}K_{UP}$

S는 U가 보낸 지불정보를 P에게 전송하여 지불을 요청

단계5. 지불승인

$\{Sig_P(h(TMUCert, ID_s, T_p, PM_{info}))\}K_{SP},$

$\{Sig_P(h(TMUCert, ID_s, T_P, PM_{info}\}K_{up}$

P는 S가 보낸 U의 지불정보를 확인하여 지불을 승인

단계6. 지불내역

$\{Sig_P(h(TMUCert, ID_s, T_P, PM_{info}\}K_{up}$

S에게 지불한 지불내역을 U에게 전송

제안하는 프로토콜은 단계2,3에서 상호인증이 이루어진다. 사용자가 선택적으로 $TMUCert$을 사용함으로써 개인프라이버시보호 및 이동성을 제공해준다. 기존 지불프로토콜에서는 상호인증을 위해 사용자와 서비스제공자 사이에 개인정보를 전달하였다. 그러나 제안하는 이 논문에서는 컨텐츠를 제공받거나 서비스를 제공 받을 때 서비스제공자가 사용자의 신원을 알 수 없고 다면 사용

자가 서비스제공자의 신뢰기관으로부터 받은 *TMUCert*을 통해 정당한 사용자임을 확인할 수 있게 된다. 따라서 *TMUCert*을 사용할 수 있도록 하여 개인 프라이버시를 제공한다. *TMUCert*은 공개키를 효율적으로 공유할 수 있도록 함으로 이동성을 동시에 만족시킨다. 또한 *TMUCert*에는 개인정보가 들어있지 않기 때문에 사용자의 익명성을 제공해 준다.

4. 안전성 평가

이 장에서는 제안한 유비쿼터스 환경에서 사용자 프라이버시 보호 및 이동성을 제공하는 안전한 지불 프로토콜의 안전성 성능을 평가 한다.

표4-1 성능 평가

항목	평가
메시지 교환횟수	6회
상호인증	○
기밀성/무결성	○
종단간 보안	○
개인프라이버시	△(선택적지원)
로밍지원	○
임시이동사용자인증서	○
익명성	△(선택적지원)

서비스제공자에 대한 키 확인과 인증을 단계2에서 해쉬를 통해서 제공된다. 사용자에 대한 인증은 단계3에서 전송되는 *TMUCert*을 가지고 제공된다. 3단계의 인증은 상호인증을 제공한다. 서비스제공자로부터 생성된 난수r을 통해 재전송 방지가 제공되며 전자서명을 통해 데이터의 부인방지를 제공해 준다. 암호화와 난수를 사용하여 기밀성과 무결성을 제공해주고 MG(Mobile Gateway)를 통해 종단간 보안을 제공해준다.

이 논문에서는 *TMUCert*을 사용함으로 제공되는 몇가지 안전성을 살펴보면 아래와 같다.

- 개인 프라이버시 보장 : 신뢰기관으로부터 전 처리로 발급받은 *TMUCert*을 사용하여 서비스제공자로부터 사용자는 개인 프라이버시를 제공받을 수 있다. *TMUCert*은 컨텐츠를 제공받거나 서비스를 제공받을때 서비스제공자가 사용자의 신원을 알수 없다. 다만 사용자가 서비스제공자의 신뢰기관으로부터 받은 *TMUCert*을 통해 정당한 사용자임을 확인할수 있게 된다.
- 이동성 : *TMUCert*은 공개키를 효율적으로 공유할 수 있도록 함으로 안전하면서도 자유로운 사용자의 이동성을 보장해준다
- 익명성보장 : *TMUCert*은 사용자에 대한 어떤 정보도 들어있지 않기 때문에 사용자에 대한 익명성을 보장해 준다.

5. 결론 및 향후 연구방안

유비쿼터스 환경에 대한 연구는 차세대 IT 기술로써 많은 각광을 받고 있다. 유비쿼터스 환경은 사용자들에게 아주 많은 편리함을 제공해 줄 수 있는 신기술임에도 불구하고 개인 프라이버시 침해와 같은 취약점을 가지고 있었다[3]. 또한 유비쿼터스 환경에서는 사용자 이동성을 완벽히 보장해야 한다.

이 논문에서는 이런 취약점을 해결해보기 위해 서비스에 따라 사용자가 선택적으로 인증서를 사용함으로 개인정보가 필요하지 않은 서비스인 경우 *TMUCert*을 사용하여 개인 프라이버시 보호 및 이동성과 익명성을 제공하는 유비쿼터스 환경에서의 안전한 지불방식을 제안하였다. 향후과제로는 지불프로토콜을 설계하기 위해 가정으로 설정한 사용자의 안전한 인증방식을 구현하고자 한다.

참고문헌

[1] SeungJong Lee, Keecheon Kim, *"The Wireless Technology Applied to the Ubiquitous Network Environment"*, Proceedings of the20th KISS Fall conference Vol.30,N03,2003

[2] 권수갑, "Ubiquitous Compution 개념과 동향" 전자부품연구원 전자정보센터정보통신기술사

[3] Boddupalli, P.; Al-Bin-Ali, F.; Davies, N.; Friday, A.; Storz, O.; Wu, M.; *"Payment support in ubiquitous computing environments"* , Mobile Computing Systems and Applications, 2003. Proceedings. Fifth IEEE Workshop on , 9-10 Oct. 2003, Pages:110 - 120

[4] Byung-Rae Lee, Kyung-Ah Chang, Tai-Yun Kim, *"Temporary Mobile User Certificate for Mobile Information Services in UMTS"*, IEICE TRANS. COMMUN. Vol.E83-B, No.8, 2000

[5] Stephan Steglich, Raju N.Vaidya, Olga Gimpeliovskaja, Stefan Arbanowski, R.Popescu-Zeletion *"I-Centric Services Based on Super Distributed Objects"* proceedings of the Sixth international Symposium on Autonomous Decentralized Systems (ISADS'03), IEEE 2003

[6] 임수철,김정범,이윤정,김태윤, *"무선인터넷에서의 안전한 신용카드 지불 프로토콜 설계"*, 한국정보과학회춘계학술발표논문집 Vol.29, No.1 ,2002.

[7] SunHyoung Kim, TaiYun Kim, *"End-to-End Authentication and Payment Protocol in Mobile Telecommunication System"* ,Proceedings of the20th KISS Fall conference Vol.29,N01,2002