이동 컴퓨팅 환경에서의 익명성 보장과 불추적성에 관한 연구

최선영, 박상윤, 한문석, 엄영익
성균관대학교 전기전자 및 컴퓨터공학부
e-mail : sychoi@ece.skku.ac.kr

The Study of Anonymity and Untraceability in Mobile Computing Environments

Sun Young Choi, Sang Yun Park, Mun Suk Han, Young Ik Eom
School of Electrical and Computer Engineering, Sungkyunkwan University

요 약

이동 네트워크 상에서의 인터넷 서비스가 활성화됨에 따라 이동 호스트에 대한 인증 및 비밀성이 요구되었고, 이동 호스트의 이동성에 따른 익명성 및 불추적성이 중요한 고려사항이 되었다. 본 논문에서는 이동 호스트가 도메인간을 이동하면서 노출될 수 있는 이동 호스트의 identity의 보호를 위한 익명성 보장 및 불추적성을 지원하는 안전한 인증 프로토콜을 제시한다.

1. 서 론

이동 컴퓨팅 환경이 보편화되고 인터넷 서비스가 이동 네트워크로 확장됨에 따라 이동 호스트에 대한 인증 및 비밀성이 중요 고려 사항으로 부각되고 있다. 특히 이동 단말기 사용자의 익명성(anonymity) 및 불추적성(untraceability)은 도청자들로부터 사용자의 identity를 숨김으로서 사용자의 위치적 투명성을 제공할 수 있다[1].

그러나 최근의 GSM 및 CDPD 등의 기존 이동 네트워크 프로토콜들은 인증, 비밀성 및 익명성에 대한 고려를 포함하고는 있으나, 단순한 인증 과정과 약한 비밀성 및 유추될 수 있는 익명성의 제공으로 많은 한계점을 내포하고 있는 실정이다.

본 논문에서는 기존 이동 네트워크의 인증, 비밀성 및 익명성에 대한 기술 현황을 분석하고 문제점을 진단하며, 이를 개선하여 설계한 익명성 지원 인증 프로토콜의 기능 및 동작원리를 소개한다. 본 논문의 2장에서는 이동 네트워크의 기존 기술 현황을 소개하고 3장에서는 본 프로토콜 설계에 선행하는 기반 이론을 정의한다. 4장에서는 본 프로토콜의 기능 및 동작원리를 소개하고 5장에서는 요약 및 향후 연구과제를 제시한다[1, 2].

2. 이동 네트워크상의 익명성 기술

2.1 기존 이동 네트워크의 비밀성

GSM(Global System for Mobile)은 가입자들에게 비밀성을 제공하는 최초의 digital cellular 네트워크이다. GSM에서는 TMSI(Temporary Mobile Subscriber Identity)라는 alias에 의해 비밀성이 제공된다. GSM은 IMSI(International Mobile Subscriber Identity)라는 사용자 고유의 불변하는 identity와 TMSI간의 매핑을 통하여 원격 도메인에서 사용자의 identity를 도청자로부터 보호받을 수 있다. 그러나 도청자는 트래픽 분석을 통하여 IMSI와 TMSI간의 관련성을 유추할 수 있다[1, 2, 3].

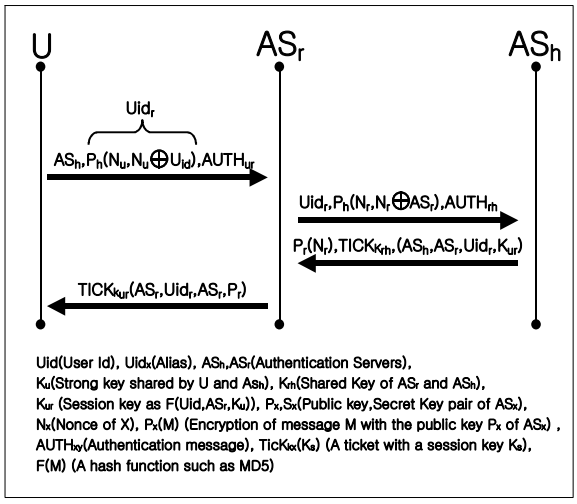
CDPD(Cellular Digital Packet Data)는 GSM에 비해 좀 더 강한 비밀성을 제공하는데, 인증 과정 이전에 사용자와 원격 도메인간에 Diffe-Hellman 키 교환 프로토콜을 사용하여 비밀 세션 키를 생성하고, 사용자 identity를 암호화해서 원격 도메인에게 전달함으로서 도청자가 사용자 identity 획득할 수

韓國領 독도 Dokdo is Korean Territory

없도록 한다. 그러나 원격 도메인에게 사용자 identity가 노출될 수 있고, Diffe-Hellman 키 교환 프로토콜의 특성상 도청자가 원격 도메인으로 가장할 수 있는 등의 단점을 내포하고 있다[1, 6].

2.2 익명성 및 인증 지원을 위한 프로토콜

Didier Samfat, Refik Molva 및 N. Asokan은 IBM에서 개발한 인증 및 키 교환 서비스인 KryptoKnight 시스템의 단-방향 인증 프로토콜을 기반으로 하여 익명성을 제공하고, 세션키를 통한 비밀 통신을 할 수 있는 인증 프로토콜을 제안하였다. 인증 프로토콜은 사용자 및 원격 identity와 랜덤 넘버를 사용하여 사용자 alias를 생성하고, alias를 사용자, 원격 도메인 및 홈 도메인간에 교환하여 사용자를 인증하며 세션 키를 생성하여 비밀 통신을 한다. 인증 프로토콜은 사용자의 익명성 뿐 아니라 원격 도메인의 익명성도 보장될 수 있고, 인증 과정에 비밀 키 교환이 포함됨으로서 인증과 키 교환 과정을 축약하는 장점을 갖고 있다. 반면, 각 사이트의 alias의 생성시 마다 공개 키 암호화 기법을 사용하고, 메시지 인증 코드인 AUTHab 내의 Token 생성시 마다 3중의 암호화 과정을 포함하는 많은 시간적 오버헤드 유발하는 단점을 갖는다. 그림 1에서는 인증 프로토콜의 메시지 구조 및 흐름도를 예시한다[1, 2, 3, 4].



(그림 1) 인증 프로토콜의 흐름도

2.3 이동 네트워크를 위한 비밀성의 분류

이동 네트워크 상에서의 인증 및 비밀성은 사용자, 홈 도메인, 원격 도메인 및 도청자 등에 대한 identity 노출 여부에 따라 다단계 등급으로 분류된다. 표 1에서 예시하는 바와 같이 Didier Samfat, Refik Molva 및 N. Asokan은 인증 및 비밀성의 강도를 5단계로 분류하고 있다[1, 5].

<표 1> 이동 네트워크상에서의 비밀성의 강도

단계	설 명
C1	Hiding User Identity from Eavesdropper
C2	Hiding User Identity from Foreign Authorities
C3	Hiding Home Domain Identity from Third Parties
C4	Hiding Home Domain Identity from Foreign Authorities
C5	Hiding User Behavior from Home Authorities

대부분의 현존하는 이동 네트워크의 비밀성의 강도는 C1 단계에 속하는데, 사용자의 identity 정보가 직접 노출되지는 않지만 alias와 홈 도메인간의 트래픽 분석에 의해 유추될 수 있다. C2 단계는 C1 단계에 부가적으로 원격 도메인에 사용자의 identity 정보가 숨겨질 수 있고, C3 단계는 C2에 부가적으로 제 3의 기관에게 홈 도메인의 identity를 숨길 수 있으므로 홈 도메인과 사용자의 identity간의 유추가 불가능하다. C4는 C3에서 추가적으로 홈 도메인의 identity를 원격 도메인에게 숨길 수 있는데, 원격 도메인이 홈 도메인의 identity를 인지하는 것을 방지함으로서 강한 불추적성을 보장할 수 있다. C5 단계는 C4에 추가적으로 사용자의 이동을 홈 도메인에 숨김으로서 완벽한 불추적성을 보장할 수 있다.

3. 익명성 보장 지원 기술

3.1 설계의 기본원칙

본 논문에서는 이동형 컴퓨터 사용자의 익명성과 위치 불추적성을 지원하기 위하여 비밀성 강도를 C5로 한다. 프로토콜 설계에 앞서 다음과 같은 가정을 갖는다.

사용자는 홈 도메인 안에서 지속적으로 사용할 수 있는 유일한 identity를 하나 할당받게 되며, 새로운 도메인으로 이동하였을 때, 이동 컴퓨터 사용자의 인증을 위해서 server-based 인증 메카니즘인 Kerberos 또는 KryptoKnight을 이용한다. 인증 서버들간의 인증을 위해서는 PKI(Public Key Infrastructure)구조를 이용한다.

인증 서버간의 세션수립을 위한 시나리오는 다음과 같다.[5, 6, 7].

(1) 각각의 이동 컴퓨팅 환경을 지원하는 인증 서버들은 사전에 인증 서버를 통해 alias를 등록하고, alias에 대한 인증서를 받는다. 이때, 인증서와 alias

韓國領 독도 Dokdo is Korean Territory

를 공개한다. 따라서, 도청자들이나 홈 도메인으로부터 원격 도메인 인증 서버의 실제 아이디는 숨기게 되며, 실제 아이디는 인증 서버만이 알고, 관리하게 된다.

(2) 각각의 인증 서버들은 alias를 갱신할 때마다 상위 인증 서버에 등록하고, 인증서를 받는다.

(3) 각각의 인증 서버들은 사전에 혹은 필요시에 서로의 인증서와 세션키를 교환함으로써 서버들 간에 상호 신뢰함을 전제로 한다.

3.2 프로토콜에 사용되는 기본 알고리즘과 용어

본 논문의 프로토콜에서 이동 컴퓨터 사용자의 익명성을 위해 alias를 사용하며, 인증 프로토콜에 사용되는 용어와 알고리즘은 다음과 같다.

S_{ku} : one-way hash function F(U, R_{alias}, Ku)로 이동 컴퓨터 사용자와 원격 도메인의 인증 서버가 사용
ES_{kur} : 이동 컴퓨터 사용자(u)와 원격 도메인에 있는 인증 서버(r)와의 공유키로 암호화
E_{SKrh} : 원격 도메인 인증 서버와 홈 도메인 인증 서버간의 세션키
K_u : 사용자와 홈 도메인 인증 서버간의 공유키
U_{id} : 사용자의 실제 identity
R_{id} : 원격 도메인 인증 서버의 실제 identity
$P_h()$: 홈 도메인에 있는 인증 서버의 공개키로 암호화
$P_s()$: 원격 인증 서버의 상위 인증기관의 공개키로 암호화
M_u : 사용자(u)가 생성한 메시지
N_u : 사용자가 생성한 random number
T_u : 사용자가 생성한 timestamp
Sig_{ur} = [N_u, Tu, ESkur(Mu, Nu, Tu)]
SIG_{rh} = [Nr, Tr, ESKrh(Ralias, Nr, Tr)]
$ASIG_{rh}$ = [Nr, Nh, Th, ESKrh(Kur, Nr, Nh, T_h)]
$ASig_{ur}$ = [Nu, Nr, Tr, ESkur(ASh, Nu, Nr, Tr)]
U_{alias} = Ph(Nu, Nu ⊕ Uid) 사용자의 alias
R_{alias} = Ps(Nr, Nr ⊕ Rid) 원격 도메인 인증 서버의 alias
AS_r : 원격 도메인의 인증 서버
AS_h : 홈 도메인의 인증 서버
U : 이동 컴퓨터

4. 익명성보장과 위치 불추적성을 위한 인증 프로토콜

이 장에서는 시나리오를 통한 인증 프로토콜의 설계와 본 논문에서 제시한 프로토콜의 장점을 설명하고자 한다.

4.1 이동 컴퓨터 사용자들의 익명성과 위치 불추적성을 위한 인증 시나리오

(1) 1단계

사용자가 홈 도메인을 벗어나 외부 영역에 진입한 경우 먼저 원격 도메인의 인증 서버와의 통신을 위해 사용자 인증이 필요하게 된다. 사용자는 먼저 alias등록과 사용자 인증을 위해 홈 도메인 인증 서버에 메시지를 보내게 된다.

이때, alias를 이용하여 메시지를 보냄으로써, 제 삼자와 원격 도메인 인증 서버에게 사용자의 실제 identity는 숨기게 된다.

메시지 인증을 위해서는 사용자와 원격 인증 서버의 공유키로 암호화한 Sig_{ur}를 원격 인증 서버에게 보낸다.

(2) 2단계

메시지를 받은 원격 인증 서버는 U_{alias}에 자신의 alias(R_{alias})와 SIG_{rh}를 첨부하여 홈 도메인 인증 서버에게 보낸 후에 사용자 인증과 메시지 인증을 위해 SIG_{ur}과 U_{alias}를 저장한다.

(3) 3단계

① 메시지를 받은 홈 인증 서버는 SIG_{rh}를 세션키(SK_{rh})로 복호화하여 메시지 인증을 하게 된다. 또한, 사용자의 alias(U_{alias})를 자신의 비밀키로 복호화하여 이동 컴퓨터의 사용자 인증을 하게 된다.

② 사용자의 실제 identity와 원격 도메인 인증 서버의 alias(R_{alias})를 이용해 K_{ur}를 생성한다. 이 단계에서 홈 도메인 인증 서버는 원격 도메인의 실제 identity를 모르기 때문에 현재 이동 컴퓨터 사용자가 어디에 있는지 알 수 없으므로 사용자의 이동을 숨길 수 있다. 또한, 제삼자에게 완전한 익명성을 보장하게 된다.

③ 홈 도메인 인증 서버는 $ASIG_{Krh}$(K_{ur}, N_h, T_h)를 원격 도메인 인증 서버에게 보낸다.

(4) 4단계

① 원격 도메인 인증 서버는 $ASIG_{Krh}$를 세션키(SK_{rh})로 복호화하여 K_{ur}를 얻는다. K_{ur}로 저장해 두었던 Sigur를 복호화하여 사용자 인증과 사용자가

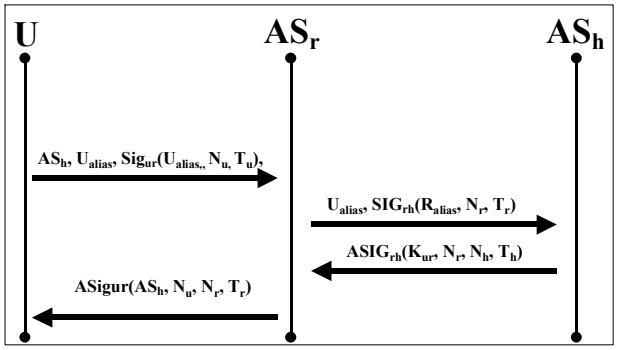
韓國領
독도
Dokdo is Korean Territory

보낸 메시지 인증을 하게 된다.

② 원격 도메인 인증 서버는 사용자에게 $ASig_{ur}$를 생성하여 보낸다.

③ 사용자는 $ASig_{ur}$를 K_{ur}로 복호화하여, 원격 도메인 인증 서버의 인증과 메시지 인증을 하게된다. 따라서, 이 단계에서 최종적으로 상호 인증이 수립된다.

이상과 같은 시나리오의 인증 프로토콜 흐름도는 다음과 같다.



(그림 2) 사용자의 익명성과 불추적성을 고려한 인증 프로토콜의 흐름도

4.2 사용자의 익명성 보장과 불추적성을 위한 인증 프로토콜의 장점

본 논문에서 제시한 인증 프로토콜의 장점을 크게 두 가지로 요약하면 다음과 같다.

본 논문에서 제시한 프로토콜은 양방향 인증을 지원하고, 기존의 인증 프로토콜에서 사용한 메시지 인증 코드인 $AUTH_{ab}$ 내의 Token 생성시 수반되는 오버헤드를 줄이기 위해, SIG_{rh}를 사용함으로 암호화 과정을 간소화하였다.

이동 컴퓨터 사용자와 원격 도메인 인증 서버의 identity로 alias를 사용함으로서 도청자 뿐 아니라 홈 도메인 인증 서버에게도 사용자의 익명성을 보장할 수 있도록 하였다.

5. 결론

이동 전화와 같은 이동 컴퓨팅 환경에 있는 사용자들은 개인의 위치정보가 기지국과 같은 홈 도메인의 서버에 노출되어 있다. 따라서, 개인의 위치정보를 숨기고, 여러 서비스를 받기 위한 사용자 인증은 이동 컴퓨팅 환경에서는 중요한 이슈라 할 수 있다. 본 논문에서는 이런 이슈를 만족하기 위해서 alias를 이용한 인증 프로토콜을 설계하였다.

본 논문에서 제시한 프로토콜은 이동 컴퓨팅 환경에서 사용자의 익명성을 보장하고, 사용자의 위치 불추적성을 지원함으로 사용자의 프라이버시를 최대한 보장할 수 있도록 하였다.

이동 컴퓨터의 사용자가 늘어감에 따라 본 논문에서 제시한 익명성 보장과 불추적성 인증 프로토콜은 제삼자로부터 개인의 프라이버시를 지키기 위해서 유용하게 응용되어질 것으로 기대된다.

따라서, 향후에 본 논문에서 제시한 프로토콜을 이용한 시뮬레이션과 인증 절차의 수학적 증명에 따른 검증이 요구된다.

참고문헌

[1] D. Samfat, R. Molva and N. Asokan, "Untracealibity in Mobile Networks", MobiCom '95, November, 1995

[2] Willian Stallings, CRYPTOGRAPYH AND NETWORK SECURITY: Principles and Practice, 2nd ed. Prentice-Hall, 1999

[3] Y. Frankel, A. Herzberg, P. A. Karger, H. Krawczyk, C. A. Kunzinger, M. Yung, "Security Issues in a CDPD Wireless Network," IEEE Personal Communications, Vol. 2, No. 4

[4] G. Pierce and C. Paar, "Recent Developments in Digital Wireless Network Security" Technical conference on Telecommunications Research and Development in Massachusetts, Lowell, March 12, 1996

[5] Refik Molva Didier Smafat, Gene Tsudik, "Authentication of Mobile Users" IEEE Network, Social Issue on Mobile Communication Technologies, Vol. 8, No. w, March/April 1994

[6] M. Rahnema, "Overview of he GSM and Protocol System and Protocol Architecture", IEEE Communication magazine, April 1993

[7] R. Molva, G. Tsudik, E. Van Herreweghen, S. Zatti, "KryptoKnight Authentication and Key Distribution System", Proceedings of ESORICS'92, November 1992

韓國領
독도
Dokdo is Korean Territory