2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

이동 컴퓨팅 환경에서의 익명성과 불추적성 지원 기법에 관한 연구

최선영' 엄영익
성균관대학교 전기전자 및 컴퓨터공학부

e-mail:sun391@chollian.net

A study of scheme for Providing Anonymity and Untraceability in Mobile Computing Environment

Sun Young Choi, Young Ik Eom
School of Electrical and Computer Engineering, Sungkyunkwan University

요약

최근 이동 네트워크 상에서의 인터넷 서비스가 활성화되고 있으며, 이에 따른 이동 컴퓨터에 대한 인증 및 비밀성이 요구되고 있다. 따라서, 본 논문에서는 이동 컴퓨터가 도메인간을 이동하면서 노출될 수 있는 이동 컴퓨터의 Identity의 보호를 위해 사용자 Alias를 사용하였으며, 원격 도메인에도 Alias를 사용함으로 익명성 보장 및 불추적성을 지원한 안전한 인증 프로토콜을 제시한다. 또한, 본 논문에서는 안전성을 높이기 위해서 Alias 생성 시 공개키 암호 시스템을 이용하였다.

1. 서론

이동 컴퓨팅 환경이 보편화되고 이동 컴퓨팅 환경에서의 인터넷 서비스가 활성화됨에 따라 이동 호스트 사용자에 대한 인증 및 비밀은 그 중요성이 점차 높아지고 있다.[1]. 특히, 이동 호스트 사용자의 이동에 의해 노출될 수 있는 사용자의 Identity를 보호하기 위한 이동 호스트의 익명성(Anonymity)과 불추적성(Untraceability)은 최근 이동 인터넷 서비스의 보편화로 인한 인증 및 비밀성 분야의 새로운 연구 과제가 되고 있다.

기존 이동 컴퓨팅에서 사용된 GSM 및 CDPD 등의 이동 네트워크 프로토콜들은 인증 및 비밀성 기술은 단순한 인증 과정을 거치며, 약한 비밀성을 제공한다. 즉, 인증 과정에 사용자의 익명성을 일부만 포함함으로서 사용자의 Identity가 노출될 수 있는 한계점을 내포하고 있는 실정이다.

따라서, 본 논문에서는 기존 이동 네트워크 프로토콜들의 인증, 비밀성 및 익명성에 대한 기술을 분석하고 문제점을 진단하며, 이를 개선하여 설계한 익명성 지원을 위한 인증 프로토콜을 제시하고자 한다. 본 논문의 2장에서는 기존의 이동 네트워크 프로토콜들의 기술 현황을 소개하며, 3장에서는 본 인증 프로토콜의 설계를 위한 가정들을 정의하고, 본 인증 프로토콜의 기능 및 동작원리를 소개한다. 4장에서는 본 인증 프로토콜의 평가에 대해 기술하고 요약 및 향후 연구과제를 제시한다[1, 2, 3].

2. 이동 네트워크의 익명성 기술

2.1 기존 이동 네트워크 프로토콜의 익명성 기술

GSM(Global System for Mobile)은 가입자들에게 비밀성을 제공하는 최초의 digital cellular 네트워크로서 TMSI(Temporary Mobile Subscriber Identity)라는 Alias를 사용하여 익명성을 제공한다. TMSI는 사용자 고유의 Identity인 IMSI(International Mobile Subscriber Identity)와의 매핑을 통하여 원격 도메인에서 사용자의 Identity를 보호한다. 그러나, 도청자는 트래픽 분석을 통하여 IMSI와 TMSI간의 관계를 유추할 수 있는 단점을 내포한다.[1, 2, 3].

CDPD(Cellular Digital Packet Data)는 키 교환을 통한 인증으로 GSM에 비해 좀 더 강한 익명성을 제공한다. 즉, 인증 과정 이전에 사용자와 원격 도메인간에 Diffe-Hellman 키 교환 프로토콜을 사용해 비밀 세션 키를 생성한 후, 사용자 Identity를 암호화해서 원격 도메인에게 전달함으로서 도청자가 사용자 Identity를 획득할 수 없다. 그러나 원격 도메인에게 사용자 Identity가 노출될 수 있고, Diffe-Hellman 키 교환 프로토콜의 특성상 도청자가 원격 도메인으로 가장할 수 있는 등의 단점을 갖고 있다[1, 4, 5, 6, 7].

GSM과 CDPD가 익명성 보장을 하지 못하므로 Didier Samfat, Refik Molva 및 N. Asokan은 IBM에서 개발한 인증 및 키 교환 서비스인 KryptoKnight 시스템의 단-방향 인증 프로토콜을 기반으로 하여 익명성을 제공하는 프로토콜을 제안하였다. 이들이 제안한 인증 프로토콜은 사용자 및 원격 도메인 Identity와 랜덤 넘버를 사용하여 사용자 Alias를 생성함으로 익명성을 지원한다. Alias는 사

용자 인증을 위해 사용자와 원격 도메인 및 원격도메인과 홈 도메인간에 교환하며, 세션 키를 생성함으로 비밀 통신을 한다. 이 인증 프로토콜은 제삼자에게 사용자의 익명성 뿐 아니라 원격 도메인의 익명성도 보장하며, 인증 과정에 비밀 키 교환을 포함시킴으로서 인증과 키 교환 과정을 축약시키는 장점을 갖고 있다. 그러나, 각 사이트의 메시지 인증 코드인 $AUTH_{ur}$와 $AUTH_{rh}$내의 Token 생성시 마다 3중의 암호화 과정을 수행해야 하는 오버헤드를 수반한다. 그림 1에서는 인증 프로토콜의 메시지 구조 및 흐름도를 예시한다[1, 2, 3, 4, 7]

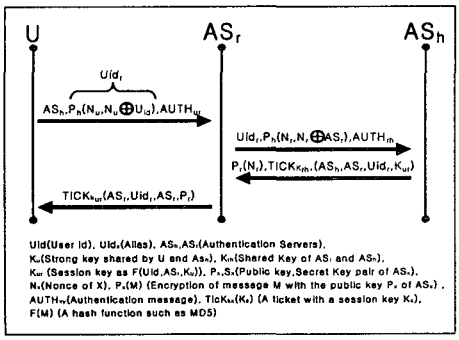

그림 1 Didier Samfat, Refik Molva 및 N. Asokan이 제안한 인증 프로토콜의 흐름도

3. 익명성과 불추적성 지원 프로토콜

3.1 설계를위한 가정

본 논문은 익명성과 불추적성을 위한 인증 프로토콜을 위해 다음과 같은 가정을 정의한다.

사용자는 홈 도메인으로부터 지속적으로 유지될 수 있는 유일한 Identity를 할당받는다. 사용자가 원격 도메인으로 이동하였을 때, 원격 도메인의 인증 서버는 사용자 인증을 위하여 서버 기반의 인증 시스템인 Kerberos 또는 KryptoKnight 등을 사용할 수 있다. 인증 서버들간의 인증을 위해서는 PKI(Public Key Infrastructure) 구조를 이용하는데, 이 때 인증 서버들은 Alias를 통한 상호인증을 전제로 한다. 다음 시나리오는 인증 서버간의 세션수립 과정을 예시한다[1, 7, 8].

(1) 이동 컴퓨팅 환경을 지원하는 인증 서버들은 PKI 구조내의 상위 인증 서버에게 각 인증 서버의 Alias를 등록하고 Alias에 대한 인증서를 획득한다. 획득된 인증서와 Alias는 공개되므로, 인증 서버들은 Alias에 대한 상호 인증을 수립할 수 있다. 따라서 각 인증 서버의 Identity는 도청자들 뿐 아니라 인증 서버들간에도 보호될 수 있다.

(2) 각 인증 서버들은 Alias를 갱신시 마다 상위 인증 서버에게 Alias를 등록하고, 새로운 인증서를 획득하며 이를 재공개한다.

(3) 인증 서버들 간에는 정기적으로 또는 필요시에 인증서를 교환하여 Alias에 대한 상호 인증을 수행하고 임시키를 공유하여 이동 호스트의 인증 요구 발생시에 사전에 수립된 임시키를 사용하여 비밀 통신을 하도록 한다.

3.2 익명성과 불추적성을 위한 인증 알고리즘

(1) Alias의 생성

① 사용자 Alias ($U_{alias} = P_h(N_u, N_u \oplus U_{id})$) : 사용자가 생성한 랜덤 넘버와 사용자의 실제 Identity를 배타적 논리합(XOR)한 결과를 홈도메인 인증 서버의 공개키로 암호화하여 Alias를 생성한다. 이 Alias는 홈 도메인 서버의 공개키로 암호화하였으므로 홈 도메인만이 사용자의 Identity를 확인하여 인증할 수 있다.

② 원격 도메인 인증 서버의 Alias ($R_{alias} = P_{as}(N_r, N_r \oplus R_{id})$) : 원격 도메인 인증 서버가 생성한 랜덤 넘버와 원격 도메인 인증 서버의 Identity를 배타적논리합(XOR)한 결과를 상위 인증 서버의 공개키로 암호화하여 원격도메인의 Alias를 생성한다. 따라서, 상위 인증 서버만이 원격 도메인의 실제 Identity를 확인할 수 있다.

(2) 전자 서명의 생성

① 사용자 전자 서명 ($SIG_{ur} = [N_u, T_u, ESk_{ur}(U_{alias}, N_u, T_u)]$) : 사용자의 Alias와 랜덤 넘버 및 타임 스탬프로 구성된 메시지를 메시지 다이제스트하고 사용자와 원격 도메인간의 세션 키로 암호화한다. 이를 다시, 사용자의 랜덤넘버와 타임스탬프를 메시지 다이제스트 코드와 조합하여 전자 서명을 구성한다.

② 원격 도메인 인증 서버의 전자 서명 ($SIG_{rh} = [N_r, T_r, ESk_{rh}(R_{alias}, N_r, T_r)]$) : 원격 도메인 인증 서버의 Alias와 랜덤 넘버 및 타임 스탬프로 구성된 메시지를 메시지 다이제스트하고 원격 도메인과 홈 도메인간의 세션 키로 암호화한다. 이를 원격도메인의 랜덤넘버와 타임스탬프를 메시지 다이제스트 코드와 조합하여 전자 서명을 구성한다.

③ 홈 도메인 인증 서버의 전자 서명 ($ASIG_{rh} = [N_r, N_h, T_h, Ek_{rh}(K_{ur}, N_r, N_h, T_h)]$) : 홈 도메인 인증 서버는 사용자와 원격 도메인 인증 서버의 세션 키와 원격 도메인과 홈 도메인의 랜덤 넘버 및 홈 도메인 인증 서버의 타임 스탬프를 원격 도메인과 홈 도메인간의 세션 키로 암호화한다. 원격 도메인과 홈 도메인의 랜덤 넘버, 홈 도메인의 타임 스탬프 및 암호화된 코드를 조합하여 전자 서명을 구성한다.

④ 원격 도메인 인증 서버의 전자 서명 ($ASIG_{ur} = [N_u, N_r, T_r, Ek_{ur}(AS_h, N_u, N_r, T_r)]$) : 원격 도메인 인증 서버가 이전 단계에서 수신하여 적재한 홈 도메인 인증 서버의 Identity와 사용자, 원격 도메인의 랜덤 넘버 및 타임 스탬프를 사용자와 원격 도메인의 세션키 K_{ur}로 암호화한다. 사용자와 원격 도메인의 랜덤 넘버와 타임 스탬프 및 암호화 코드를 조합하여 전자 서명을 구성한다.

(3) 세션 키의 생성

① 원격 도메인과 홈 도메인간의 세션 키 (K_{rh}) : 원격 도메인과 홈 도메인은 3.1절의 가정에서 언급한 바와 같이 Alias를 수반하는 PKI 구조를 통하여 인증 서버들간에 인증을 수립하고 인증된 서버들간에 정기적인 세션 키를 관리함으로서 사용자의 이동에 따른 인증 서버간의 안전한 동적 통신을 지원하도록 한다.

② 사용자와 원격 도메인간의 세션 키 ($K_{ur} = H(U_{id} \oplus R_{alias})$) : 사용자의 Identy와 원격 도메인의 Alias를 H 해쉬 함수의 입력으로 하여 생성된 고정 길이 해쉬 코드를 세션 키로 한다.

3.3 익명성과 불추적성을 위한 인증 시나리오

(1) 1단계 (사용자 ⇒ 원격 도메인 인증 서버)

사용자가 홈 도메인을 벗어나 외부 영역에 진입한 경우 먼저 원격 도메인 인증 서버와의 통신을 위해 사용자 인증이 필요하게 된다. 이때, 사용자는 자신의 실제 Identity의 노출을 막기 위해 Alias를 사용하게 되고, Alias등록과 사용자 인증을 위해 홈 도메인 인증 서버에 메시지를 보내게 된다. Alias의 사용으로 제 삼자와 원격

Samfat, Refik Molva 및 N. Asokan가 제시한 프로토콜	본 논문에서 제시한 프로토콜
U-->AS_r : AS_h, Uid_r, $AUTH_{ur}$ 암호화 회수 $Uid_r = P_h(N_u, N_u \oplus U_{id})$, -->공개키로 한번 암호화 $AUTH_{ur} = [N_u, T_u, TokenK_{ur}(U_{id}, T_u, N_u)]$ $TokenK_{ur}(U_{id}, T_u, N_u) = E(U_{id} \oplus E(T_u \oplus E(N_u)))$ -->삼중 암호화 P_h: 홈 도메인 인증 서버의 공개키로 암호화 E: 암호화 키 K_{ur}로 DES와 같은 암호화 함수로 암호화한 것	U-->AS_r : AS_h, U_{alias}, $SIG_{ur}(U_{alias}, N_u, T_u)$ 암호화 회수 $U_{alias} = P_h(N_u, N_u \oplus U_{id})$ -->공개키로 한번 암호화 $SIG_{ur} = [N_u, T_u, ESK_{ur}(U_{alias}, N_u, T_u)]$ -->단일 암호화 P_h: 홈 도메인 인증 서버의 공개키로 암호화 ESK_{ur} : K_{ur}로 암호화
AS_r-->AS_h : Uid_r, $P_h(N_r, N_r \oplus AS_r)$, $AUTH_{rh}$ 암호화 회수 $P_h(N_r, N_r \oplus AS_r)$ -->홈 도메인의 공개키로 한번 암호화 $AUTH_{rh} = [N_r, T_r, TokenK_{rh}(R_{id}, T_r, N_r)]$ $TokenK_{rh}(R_{id}, T_r, N_r)] = E(R_{id} \oplus E(T_r \oplus E(N_r)))$ -->삼중 암호화	AS_r-->AS_h : U_{alias}, R_{alias}, $SIG_{rh}(R_{alias}, N_r, T_r)$ 암호화 회수 $R_{alias} = P_{as}(Nr, Nr \oplus ASr)$ -->상위 인증 서버의 공개키로 한번 암호화 $SIG_{rh} = [N_r, T_r, ESK_{rh}(R_{alias}, N_r, T_r)]$ -->단일 암호화

도메인 인증 서버에게 사용자의 실제 Identity는 숨길 수 있다. 메시지 인증을 위해서 사용자와 원격 도메인 인증 서버간의 세션 키로 암호화한 SIG_{ur}을 원격 도메인 인증 서버에게 보낸다.

(2) 2단계 (원격 도메인 인증 서버 ⇒ 홈 도메인 인증 서버)

메시지를 받은 원격 도메인 인증 서버는 사용자의 Alias(U_{alias}), 원격 도메인의 Alias(R_{alias}) 및 SIG_{rh}를 조합한 메시지를 홈 도메인 인증 서버에게 보낸 후에 향 후 사용자 인증과 메시지 인증을 위해 SIG_{ur}를 저장한다. 이때, 원격 도메인의 Alias를 사용함으로 도청자와 홈 도메인으로부터 원격 도메인의 실제 Identity를 숨길 수 있다.

(3) 3단계 (홈 도메인 인증 서버 ⇒ 원격 도메인 인증 서버)

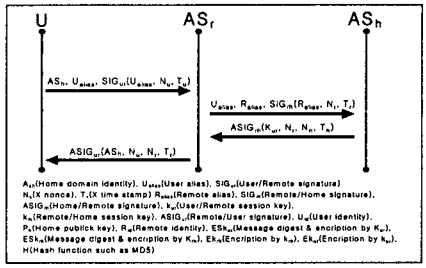

그림 2 익명성과 불추적성을 지원하는 인증 프로토콜의 동작 시나리오

① 메시지를 받은 홈 도메인 인증 서버는 SIG_{rh}를 세션 키(K_{rh})로 복호화하여 메시지 인증을 하고 사용자의 Alias(U_{alias})를 홈 도메인의 비밀키로 복호화하여 사용자의 Identity를 획득한다.

② 홈 도메인 인증 서버는 사용자의 Identity와 원격 도메인 인증 서버의 Alias(R_{alias})를 이용해 K_{ur}를 생성한다. 이 단계에서 홈 도메인 인증 서버는 원격 도메인의 실제 Identity를 알 수 없기 때문에 현재 사용자의 위치를 유추할 수 없게 되고, 제 삼자에게도 완전한 익명성을 보장하게 된다.

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

④ 원격 도메인 인증 서버는 $ASIG_{rh}$를 세션키(K_{rh})로 복호화하여 K_{ur}를 얻는다. K_{ur}로 저장해 두었던 SIG_{ur}를 복호화하여 사용자 인증과 사용자가 보낸 메시지 인증을 하게 된다.

(4) 4단계 (원격 도메인 인증 서버 ⇒ 사용자)

① 원격 도메인 인증 서버는 사용자에게 $ASIG_{ur}$를 생성하여 보낸다.

② 사용자는 $ASIG_{ur}$를 K_{ur}로 복호화하여, 원격 도메인 인증 서버의 인증과 메시지 인증을 하게된다. 따라서, 이 단계에서 최종적으로 상호 인증이 수립된다. 그림 2는 본 프로토콜의 인증 시나리오를 예시한다.

4. 프로토콜 평가 및 결론

4.1 프로토콜 평가

(1)프로토콜 간소화

Didier Samfat, Refik Molva 및 N. Asokan이 제안한 익명성 및 불추적성을 지원하는 인증 프로토콜에서 사용한 메시지 인증 코드를 비교해보면 다음과 같다. 첫째, $AUTH_{ur}$, $AUTH_{rh}$ 생성 시 각각 삼중 암호화 과정을 거치게 되며, 본 논문에서 제시한 메시지 인증 코드인 SIG_{ur}과 SIG_{rh}는 다중 암호화 과정의 오버헤드를 줄이기 위해 단일 암호화 과정으로 간소화하였다. 따라서 Didier Samfat, Refik Molva 및 N. Asokan가 제안한 프로토콜에서는 사용자의 Alias 생성 시 한번의 공개키 암호화, $AUTH_{ur}$ 생성 시 삼중 암호화, 원격 도메인의 Alias 생성 시 한 번의 공캐키 암호화, $AUTH_{rh}$ 생성 시 삼중 암호화 과정을 거쳐, 사용자로부터 홈 도메인까지 메시지를 보내는데 8번의 암호화 과정을 거치게 된다. 반면, 본 논문에

서 제시한 프로토콜은 사용자의 Alias 생성 시 한번의 공개키 암호화, SIGur 생성 시 한번의 암호화, 원격도메인의 Alias 생성 시 한번의 공개키 암호화, SIG_{rh} 생성 시 한번의 암호화 과정을 거치므로 사용자로부터 홈 도메인까지 메시지를 보내는데, 4번의 암호화 과정을 거치게 된다. 따라서, 사용자로부터 홈 도메인까지 메시지를 보낼 때 총 암호화 회수가 반으로 감소하는 것을 볼 수 있으며, 비교표는 다음과 같다.

(2) 강화된 익명성과 불추적성

기존 이동 컴퓨팅을 위한 인증 프로토콜들은 사용자 Identity를 도청자로부터 보호하거나 원격 도메인에게 숨기는 정도에 그치고, Didier Samfat, Refik Molva 및 N. Asokan에 의해 제안된 인증 프로토콜도 홈 도메인에게 사용자의 위치 정보를 완전히 숨기지는 못하게 된다. Didier Samfat, Refik Molva 및 N. Asokan가 제시한 프로토콜에서 사용한 Ralias는 원격 도메인의 실제 Identity와 랜덤 넘버를 배타적논리합(XOR)한 값을 홈 도메인 인증 서버의 공개키로 암호화하여, 랜덤 넘버와 함께 보내기 때문에 이 메시지를 받은 홈 도메인 인증 서버는 자신의 비밀키로 메시지를 복호화하여 나온 값을 랜덤 넘버로 배타적논리합(XOR)하여 원격도메인의 실제 Identity를 얻어 낼 수 있다.

이에 반해 본 논문에서 제시한 Ralias는 상위 인증 서버의 공개키로 원격 도메인의 실제 Identity와 랜덤 넘버를 배타적논리합(XOR)한 값을 암호화하였기 때문에, 메시지를 받은 홈 도메인은 원격 도메인의 실제 Identity를 유추해 낼 수 없다. 따라서, 도청자들 뿐 아니라, 사용자의 홈 도메인에게도 사용자의 위치 정보를 숨길 수 있게 된다.

Didier Samfat, Refik Molva 및 N. Asokan에서 사용한 R_{alias}

$$R_{alias} = P_h(Nr,\ Nr \oplus ASr)$$

본 논문에서 제시한 R_{alias}

$$R_{alias} = P_{as}(N_r,\ N_r \oplus R_{id})$$

4.2 결론

이동 컴퓨팅 환경에서의 인터넷 서비스가 활성화되고, 인증 및 비밀성이 요구되는 이동 인터넷 응용의 개발이 급속히 확산되고 있다. 특히, 이동 인터넷 서비스의 인증 및 비밀성 분야 중에서 이동 호스트 사용자의 이동에 의해 야기되는 사용자 Identity의 노출을 보호하기 위한 연구가 진행 중에 있다.

본 논문에서 제시한 프로토콜은 프로토콜의 간소화와 이동 컴퓨팅 환경에서 사용자의 이동에 따라 노출될 수 있는 사용자의 Identity와 원격 도메인의 Identity를 숨겨 사용자의 익명성 및 불추적성을 보장한다는 장점을 갖는다. 또한, 익명성과 불추적성 보장을 위해서 사용자의 실제 Identity 대신 사용자의 Alias를 사용하였으며, 원격 도메인 인증 서버도 Alias를 사용함으로서 도청자 뿐 아니라 홈 도메인에게도 사용자의 익명성과 불추적성을 보장할 수 있도록 하였다. 따라서, 이동 호스트의 사용자가 증가되고 사용자의 프라이버시 보호의 요구가 증가됨에 따라 사용자 익명성과 불추적성을 지원하는 본 인증 프로토콜은 제삼자로부터 사용자의 Identity와 이동성 보호를 위해 유용하게 사용될 수 있을 것으로 생각된다.

[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] Jungjoon Kim, Mina Oh, and Taegun Kim, "Security Requirements of Next Generation Wireless Communications", Communication Technology Proceedings, 1998

[4] 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, Aug. 1995

[5] 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

[6] Min-Shiang H., Yuan-Liang Tang and Heng-Chi Lee, "An efficient authentication protocol for GSM networks" UROCOMM 2000. Inforamation Systems for Inhanced Public Safety and Securi IEEE/AFCEA, 2000

[7] 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

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

[9] Michael Burrows et al., "A Logic of Authentication", Digital System Research Center, Tchinical Report 39, February 1990, May 1994