다중 도메인 환경에서 디바이스를 위한 효율적인 등록 기법

이병래, 장경아
소프트웨어센터, CTO, 삼성전자
{byungrae.lee, kachang}@samsung.com

Efficient Authentication Scheme for Mobile Devices in Multiple Domains

Byung-Rae Lee, Kyung-Ah Chang
Software Center, CTO, Samsung Electronics

요 약

본 논문에서는 다중 도메인 환경에서 사용자의 이동 디바이스가 효율적으로 등록 할 수 있는 프로토콜을 제안한다. 제안한 등록 프로토콜은 공개키 암호 시스템에 기반하여 다중 도메인에 접근 시 인증 기관을 통하여 도메인들 안에서 인증을 포함하는 등록 과정을 효율적으로 수행할 수 있게 하는 티켓을 받게 된다. 사용자의 다바이스는 획득된 티켓을 이용하여 다중 도메인 환경에서 여러 도메인을 관리하는 프락시와 효율적인 등록 수행을 할 수 있게 된다. 제안한 기법은 여러 도메인 환경이 되는 여러 홈 네트워크 및 회사 네트워크의 환경을 지원한다.

1. 서론

여러 개의 홈 네트워크 또는 회사 네트워크와 같은 다중 도메인 환경에서 디바이스는 도메인에 진입하기 위해서는 등록 과정을 거쳐야 한다. 등록 과정은 디바이스에 대한 인증과 키 교환 과정을 포함하고 있다.

홈 네트워크와 같은 환경에서 인증과 등록 문제를 다루고 있는 Universal Plug and Play (UPnP)[1]에서는 디바이스간의 인증 및 키 교환에 대한 내용을 다루고 있으나 다중 도메인간 환경에서의 인증에 대한 문제를 해결하고 있지는 않다.

본 논문에서는 홈 네트워크 또는 회사 네트워크와 같은 다중 도메인 환경에서 디바이스를 위한 등록 프로토콜을 제시하고 그에 따른 효율적인 인증과 키 교환 기법을 제안한다. 제안한 프로토콜은 공개키 암호 시스템에 기반하여 디바이스가 도메인에 접근 시 인증 기관을 통하여 다중 도메인들 안에서 등록을 하는데 사용할 수 있는 티켓를 받게 된다. 사용자의 다바이스가 이 티켓을 이용하여 다른 다바이스들이 제공하는 서비스를 이용할 때 서로간의 인증 및 키 교환을 할 수 있도록 확장도 가능하다.

제안된 등록 프로토콜을 통하여 발급된 티켓을 이용하여 검증 시 필요한 공개키 분배 문제를 해결할 수 있으며 결과적으로 등록 프로토콜 수행 시에 개선된 효율성을 제공할 수 있다.

제안한 등록 프로토콜을 기존 도메인간의 인증 프로토콜 Siemens, C 프로토콜[2,3,4]에 적용하여 그 효율성을 검증하고 성능 비교를 하였다.

우선 사용자의 디바이스는 자신의 인증 기관이 발행한 인증서를 소유하고 있다는 가정에서 다중 도메인에 진입시 등록 과정을 통해 도메인에서 사용이 가능한 티켓의 발급 과정이 들어가는 등록 프로토콜을 제안하였다. 티켓을 기반으로 한 효율적인 등록 프로토콜을 제안하였으며 기존의 도메인간의 등록 프로토콜과 성능을 비교하였다.

본 논문의 구성은 다음과 같다. 2 장에서는 이동 디바이스를 위한 기존의 등록 프로토콜을 고찰한다. .3 장에서는 제안하는 모델에 대해서 설명하고 4 장에서는 새로운 등록 프로토콜을 제안한다. 5 장에서는 4 장에서 제안한 등록 프로토콜의 수행으로 획득된 티켓을 이용한 효율적인 등록 프로토콜을 제시한다. 6 장에서는 성능 평가를 하고 7 장에서는 결론을 제시한다.

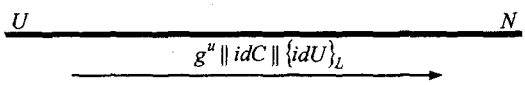
2. 기존 등록 프로토콜

사용자의 홈 도메인이 아닌 다른 도메인에서 등록 과정의 수행을 위해 Siemens 의 프로토콜 C[2]가 제안되었다. 본 장에서는 Siemens, 프로토콜 C 를 간략히 살펴본다.

프로토콜의 표기 형식은 다른 암호 시스템으로의 응용을 위하여 일반적인 방식을 이용하였다. 프로토콜의 참여자는 사용자 U, 네트워크 운영자 N, 인증 기관 C 이다. idX 는 X 의 신원을 의미하며, $CertX$ 는 X 의 인증서를 뜻한다. U, T 의 메시지 M 에 대한 전자서명 알고리즘은 각각 $Sig_U(M)$, $Sig_T(M)$ 로 표기된다. 세션키 K 로 암호화된 메시지 M 은 $\{M\}_K$ 로 나타내어진다. h 는 해쉬 함수이다.

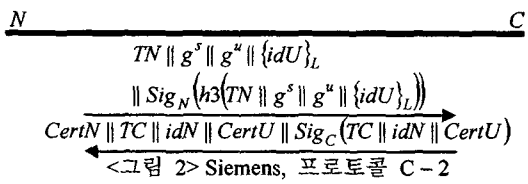
U 는 C 와 같이 ElGamal 키 설정 방식[3]으로 세션키를 성립하고, N 와는 Diffie-Hellman 방식[4]에 의하여 세

션키를 설정한다.



<그림 1> Siemens, 프로토콜 C - 1

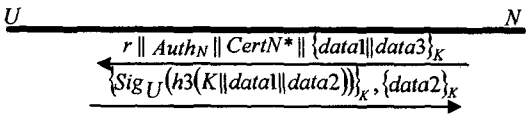
프로토콜(<그림 1>)이 시작되면 U 는 난수 u 를 생성하여 키 설정용 공개키 g^u 를 생성하고 C 의 공개키 g^w 와 같이 세션키 $L = g^{wu}$ 을 계산한다. 이와 같이 자신의 C 의 신원 idC, 그리고 자신의 신원 idU 를 세션키 L 을 이용해서 암호화해서 N 에게 보낸다.



<그림 2> Siemens, 프로토콜 C - 2

<그림 2>에서 N 은 U 로 부터 전송 받은 g^u, $\{idU\}_L$ 를 타임스탬프 TN 와 같이 C 에게로 보낸다.

C 는 U 의 공개키 g^u 와 같이 세션키 $L = g^{uw}$ 을 계산한다. C 는 N 로부터 전송 받은 메시지를 통하여 인증서 $CertU$ 와 $CertN$ 을 찾는다. C 는 타임스탬프 TC 를 생성하고 $CertU$, $CertN$ 에 전자서명을 수행하여 N 에게 전송한다.



<그림 3> Siemens, 프로토콜 C - 3

<그림 3>을 보면 N 은 U 의 공개키 g^u 를 이용하여 세션키 $K = h(g^{us} \| r)$ 를 계산해 낸다.

U 는 g^s 를 이용하여 세션키 $K = h(g^{su} \| r)$ 를 계산해내고 자신의 전자 서명을 암호화 하여 N 에게 전송한다.

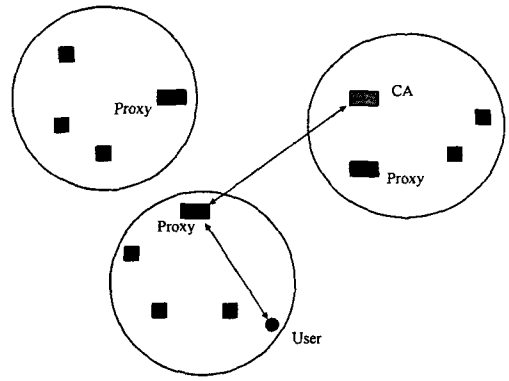
3. 제안한 등록 및 인증 모델

사용자의 디바이스는 다중의 홈 네트워크 또는 여러 도메인의 회사 네트워크에서 사용할 수 있는 디바이스를 최초로 인증 받는 등록 과정을 통과하게 된다.

최초의 등록 과정에서 인증에 성공한 사용자의 디바이스는 다중 도메인을 관리하는 인증 기관(CA)로부터 해당되는 여러 도메인의 자원을 활용할 수 있는 티켓을 부여 받게 된다.

처음의 등록 과정에서 제공 받은 티켓을 이용하여 다른 도메인에서의 프락시들과 효율적인 등록이 가능하다.

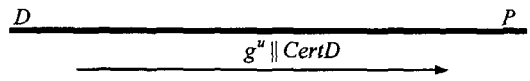
<그림 4>는 여러 도메인에서 프락시(Proxy), 인증 기관(CA) 그리고 사용자(User)의 관계를 보여준다.



<그림 4> 제안한 인증 및 등록 모델

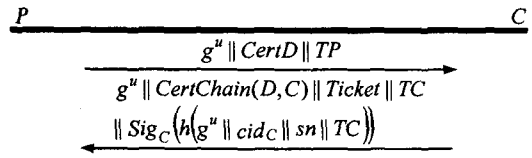
4. 제안한 등록 프로토콜 I

아래의 프로토콜 기술에서 사용자의 디바이스 D, 각 도메인을 관리하는 프락시 P, 그리고 다중 도메인에 대한 인증 기관 C 가 참여한다.



<그림 5> 제안한 등록 프로토콜 I - 1

프로토콜(<그림 5>)이 시작되면 D 는 난수 u 를 생성하여 공개키 g^u 를 생성하여 자신의 인증서 $CertD$ 와 같이 P 에게 보낸다



<그림 6> 제안한 등록 프로토콜 I - 2

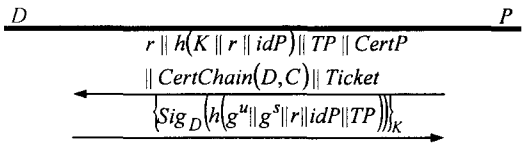
<그림 6>에서 P 은 D 로 부터 전송 받은 g^u, $CertD$ 타임스탬프 TP 를 C 에게로 보낸다.

C 는 $CertD$ 를 검증하고 D 가 도메인에서 사용할 수 있는 $Ticket$ 을 생성한다. $Ticket$ 은 다음과 같은 구조를 가진다.

$$Ticket = sn \| TS \| PK \| Sig_C(sn \| TS \| PK)$$

C 는 생성한 $Ticket$ 을, 타임스탬프 TC, D 가 C 의 공개키를 얻을 수 있는 $CertChain(D,C)$ 에 전자 서명을 하여 P 에게 전송한다.

<그림 7>을 보면 P 는 *Ticket* 를 이용하여 D 의 공개키를 검증할 수 있다. P 은 자신이 받은 메시지와 난수 r 을 생성하여 D 에게 전송하고 g^u 를 이용하여 세션키 $K_s=\left(g^{us}\|r\right)$를 계산해 낸다.

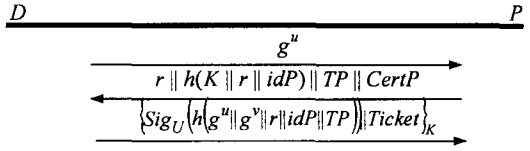


<그림 7> 제안한 등록 프로토콜 I - 3

D 는 P 로부터 받은 $CertChain(D,C)$를 이용하여 C 의 전자서명을 검증할 수 있도록 공개키를 얻고 P 의 공개키 g^s 를 이용하여 P 와의 세션키 $K_s=\left(g^{su}\|r\right)$를 계산해낸다.

5. 제안한 등록 프로토콜 II

D 는 사용자, P 는 한 도메인을 관리하는 프락시를 나타낸다. U 는 등록 프로토콜의 수행 결과로 *Ticket* 과 *CertP* 를 검증할 수 있는 공개키를 가지고 있다.



<그림 8> 제안한 등록 프로토콜 II

프로토콜(<그림 8>)이 시작되면 D 는 세션키 설정을 위한 공개키 g^u 를 P 에게 보낸다.

P 는 난수 r 을 생성하고 g^u 와 자신의 공개키 g^v 를 이용하여 세션키 $K=h\left(g^{uv}\|r\right)$ 를 계산해 낸다. P 는 K, r, idP 를 해쉬화 하고 타임스탬프 TP, 인증서 *CertP* 를 D 에게 전송한다.

D 는 세션키 $K=h\left(g^{vu}\|r\right)$를 생성하고 g^u, g^v, r 과 P 의 신원 idP 와 타임스탬프 TP 를 해쉬 함수 h 로 처리하고 서명을 구한 후 자신의 인증서 *Ticket* 과 같이 P 에게 전송한다.

6. 성능 평가 및 분석

도메인에 접근했을 때 수행되는 등록 프로토콜을 통하여 디바이스는 *Ticket* 을 획득하게 되고 이를 통하여 효율적인 등록 프로토콜의 수행이 가능하다.

기존의 등록 프로토콜과 제안한 프로토콜과의 성능 평가는 [표 1]에 나와 있다. 비교는 초기에 요구되는 등록 프로토콜 I 이후에 계속적으로 사용될 수 있는 등록 프로토콜 II 와 기존의 Siemens, 프로토콜 C 를 비교 하였다.

제안된 프로토콜은 메시지의 교환 횟수를 감소하였다. 암호화 등에서 개선된 효율성을 보여준다.

[표 1] 제안한 등록 프로토콜 II 와의 성능 평가

	Siemens, Protocol C	제안한 등록 프로토콜 II
키 설정 알고리즘	ElGamal, Diffie-Hellman	Diffie-Hellman
참여자의 수	3	2
메시지의 수	5	3
세션키의 수	2	1
사용자의 서명 생성	1	1
사용자의 암호화	3	1
사용자의 복호화	1	0

7. 결론 및 향후 연구 과제

본 논문에서는 다중 도메인에서 사용자가 디바이스를 효율적으로 등록하는 기법을 제안하였다. 제안한 방법은 처음 도메인에 등록 하는 과정에서 인증 기관을 통하여 티켓을 부여 받게 된다. 사용자는 티켓을 이용하여 다중 도메인에서 효율적으로 등록할 수 있게 되는 장점이 된다.

참고문헌

[1] Universal Plug and Play (UPnP) Forum, http://www.upnp.org.

[2] ACTS AC095, ASPeCT Deliverable D02, Initial report on security requirements, Feb. 1996.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, No.4, pp.469-472, 1985.

[4] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 1976.