로밍 서비스를 위한 개인키 로밍 프로토콜

문성원°, 김영갑, 박대하, 문창주, 백두권
고려대학교 컴퓨터학과
{kdunkman°, ygkim}@software.korea.ac.kr, dhpark@stitec.com, {mcj, baik}@software.korea.ac.kr

A Private Key Roaming Protocol for Roaming Services

SungWon Moon°, YoungGab Kim, DeaHa Park, ChangJoo Moon, Dookwon Baik
Korea University

요 약

'키로밍(Key Roaming)' 서비스는 임의의 단말기에서 인증서, 전자서명 등의 사용자의 비밀정보를 네트워크를 통해서 접근할 수 있는 기능을 지원한다. 현재 은행의 뱅킹 시스템이나 그 밖의 인터넷 서비스에서는 비밀정보를 사용자의 컴퓨터에 저장해서 사용한다. 그러나 사용자가 그 비밀정보를 다른 컴퓨터에서 사용하고자 할 때에는 디스크나 스마트카드와 같은 보조기억장치에 저장해야 하는 불편함이 존재한다. 종래의 이러한 방식은 사용이 불편할 뿐만 아니라 공간과 비용의 부담이 크므로 키로밍 프로토콜에 대한 요구가 더욱 증대하였다.

키로밍 프로토콜은 공간과 비용의 절감이라는 효과가 있지만 해결해야 할 보안상의 문제가 존재하며 이 문제점들을 해결하기 위한 많은 방법들이 제시되어 왔다. 본 논문에서는 베리사인의 프로토콜과 한국정보보호센타에서 제시한 다중서버를 이용하는 프로토콜에 대해서 살펴본 후 그 문제점을 지적하고 이를 해결할 수 있는 새로운 프로토콜을 제안한다.

1. 서 론

키로밍 프로토콜은 사용자에게 공간적, 시간적 제약 없이 비밀키(private key)와 전자서명(digital signature) 그리고 인증서(certificate)와 같은 비밀정보를 안전하게 제공하는 것을 목적으로 한다. 관련연구로는 사용자의 패스워드(password)만을 기반으로 하는 방법과 패스워드를 기반으로 함과 동시에 다중서버를 이용하는 방법이 있다. 전자의 방법으로는 EKE(Encrypted Key Exchange) 프로토콜[1]과 SPEKE(simple password exponential key exchange) 프로토콜[2]이 해당된다. 후자는 비밀키를 획득할 때 패스워드 기반의 방법과 분산된 서버를 동시에 사용하여 이전의 프로토콜이 공격자의 중앙서버에 대한 사전공격에 대한 방어의 취약성을 보완한다. 대표적인 프로토콜로는 Ford와 Kaliski가 제안한 베리사인(verisign)의 키로밍 프로토콜[3]과 한국정보보호센터에서 제안한 프로토콜[4]이 존재한다.

베리사인의 프로토콜은 SSL(Socket Secure Layer)이나 TLS(Transport Layer Security)와 같은 별도의 보안 프로토콜이 필요하며 이를 해결하기 위해서 한국정보보호센타에서는 별도의 보안 프로토콜을 사용하지 않고도 로밍 서비스를 제공할 수 있는 프로토콜을 제안하였다. 그러나 이 프로토콜 역시 키서버의 개인키가 공개될 수 있는 위험이 있어 보안상 취약점이 존재한다. 본 논문에서는 이러한 문제점을 지적하고 이를 증명하며 그에 대한 해결책을 제시하고자 한다.

2. 베리사인의 키로밍 프로토콜

각 프로토콜에 관한 과정은 표1, 표2와 같으며 프로토콜 과정을 번호 순서대로 나열하였다.

1) 프로토콜 인자

- $p = 2q + 1$: p와 q는 각각 소수
- $1 \le a \le q-1$: 사용자가 선택하는 난수 숨은 요소(blinding factor)
- $W = f(PWD)$: f는 패스워드를 Zp상의 곱 연산에 대한 위수가 q인 원소로 대응시키는 함수
- $1 < b_i < q-1$: 각 i번째 로밍서버의 비밀정보
- $KDF(K_1, \ldots, K_2)$: 키 파생 함수
- $OWF(K, j)$: 일방향 함수

2) 키등록 과정

표 1 베리사인 프로토콜의 키등록 과정

사용자	메시지	키서버
⑤K 생성 ⑥V_i생성	① $M=W^a \bmod p$ (로밍요청) ④$C_i=(M)^{b_i} \bmod p$ (로밍응답) ⑦ V_i 전송	②난수b_i생성 ③ID, b_i저장 ⑧V_i 저장

$K = KDF(K_1, \ldots, K_2)$ (단, $K_i = C_i^{1/a} \bmod p$)……(1)
$V_i = OWF(K, j)$ (j : 로밍서버 아이디)……(2)

3) 키로밍 과정

표 2 베리사인 프로토콜의 키로밍 과정

사용자	메시지	키서버
④K 생성 ⑤V_i생성	① $M=W^a \bmod p$ (로밍요청) ③$C_i=(M)^{b_i} \bmod p$ (로밍응답) ⑥ V_i 전송	② b_i 검색 ⑦저장된 V_i와 비교를 통한 사용자 인증

4) 특징 및 문제점

베리사인의 프로토콜은 사용자 측에서 임의로 선택한 숨은 요소 a를 이용함으로서 사용자의 패스워드와 관련한 정보나 실행 도중 생성되는 키의 조각 값에 대한 정보를 서버에게 공개하지 않는다. 그리고 (1)식에서처럼 분산된 서버로부터 전송된 키 조각으로부터 전체키 K를 얻기 때문에 하나의 서버를 공격해서 얻은 정보만으로는 전체 비밀키를 얻을 수 없다는 특징이 있다. 그러나 키 로밍 동안에 프로토콜 메시지에 대한 무결성을 보장하지 않으므로 SSL이나 TLS와 같은 별도의 보안 프로토콜을 사용하지 않는다면 사용자의 패스워드에 대한 사전공격을 허용할 수 있는 위험을 내포한다.

3. 한국정보보호센터의 키로밍 프로토콜

베리사인의 프로토콜의 과정을 기본 모델로 하지만 서버에 대한 인증과정을 포함시켜 별도의 보안 프로토콜 없이 키를 로밍할 수 있는 프로토콜을 제안한다.

1) 프로토콜 인자

n개의 로밍서버가 존재하며 각 서버에 대한 개인키(X_i)가 존재하고 서버 측을 대표하는 그룹 공개키를 갖는 것을 특징으로 한다. 베리사인의 프로토콜 인자에 다음을 추가한다.

- g : $g^q = 1 \bmod p$
- X_i : i 번째 키 서버의 비밀키
- ch_j : 서버 측의 챌린지 값
- $y = \prod_{i=1}^{n} g^{X_i} \bmod p$: 키서버의 그룹 공개키

2) 키등록 과정

표 3 한국정보보호센터의 키등록 과정

사용자	메시지	키 및 응용 서버
④K,K_j 생성	① $M = g^a W \bmod p$(로밍요청) →	② ID 저장
	← ③ $C_i=(M)^{X_i} \bmod p$(로밍응답)	⑥ K_j 저장
	⑤ K_j,ID 전송 →	

$K = KDF((\prod_{i=1}^{n} C_i)/y^2 \bmod p)$ ……(3)

$K_j = OWF(K,j)$ (이때, j(인증서버) = 1, …, m)…(4)

3) 키로밍 과정

표 4 한국정보보호센터의 키로밍 과정

사용자	메시지	키 및 응용 서버
④K,K_j 생성 ⑥$OWF(K_j,Ch_j)$계산	① $M = g^a W \bmod p$(로밍요청) →	② ID 검색
	← ③ $C_i=(M)^{X_i} \bmod p$(로밍응답)	⑧저장된 K_j, Ch_j의 OWF값과 전송된 값 비교
	← ⑤ 응용서버에서 Ch_j값 전송	
	⑦ $OWF(K_j,Ch_j)$ 전송 →	

4) 문제점

한국정보보호센터에서 제안한 키로밍 프로토콜은 베리사인에서 사용했던 별도의 보안 프로토콜의 사용하지 않도록 하기 위해서 키서버에 대한 개인키와 그룹 공개키를 제안하였다. 이를 통해 사용자가 서버에 대해서 인증할 수 있는 방법을 제공한다. 하지만 서버에 대한 인증만으로는 이 프로토콜이 안전하다고 할 수는 없다.

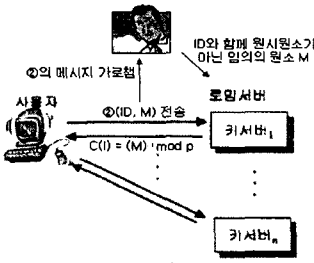

그림 1 한국정보보호센터의 프로토콜에 대한 공격

그림 1에서처럼 사용자가 서버로 로밍 요청정보(ID,M)를 전송할 때 공격자가 중간에서 ②의 메시지를 가로챈 후 M값 대신에 임의의 값으로 대체하여 전송한 경우 서버에서 이 사실을 모르고 응답정보를 전송하게 되고, 공격자가 임의의 M값과 이 정보로부터 서버의 개인키를 좀 더 쉽게 획득할 수 있게 된다.

응답정보 $C_i=(M)^{X_i} \bmod p$는 Diffie-Hellman의 식을 이용하여 암호화함으로서 패스워드에 대한 정보를 공격할 수 없도록 한다. DH(Diffie-Hellman) 문제 역시 다른 공개키 알고리즘과 마찬가지로 이산 로그 문제(discrete logarithm problem)를 기반한다. 이때, M, C_i, p는 모두 공개된 정보이며, M은 p의 원시근(primitive root)이어야 한다. M의 값이 원시근인 경우, 전체 순열의 차수는 $\varnothing$[1](p)이다. 따라서 p가 충분히 크면 무차별 공격(brute force attack)을 이용해서 X_i를 찾는 것은 불가능하다. 하지만 원시근이 아닌 다른 적절한 M을 선택한다면 같은 순열의 반복적인 출현을 이용하여 X_i를 좀 더 쉽게 획득할 수 있다.

- **M이 원시근인 경우 비용**
  1) 최소 비교 횟수 : 1번
  2) 최대 비교 횟수 : $\varnothing(p)$번
  => **평균비교횟수 : $\varnothing(p) / 2$** ……(5)

- **공격자가 적절한 M을 대입할 경우**
  m : $ord_p(M)$[2]
  1) 최소 비교 횟수 : 1번
  2) 최대 비교 횟수 : $\frac{m}{2} * \frac{\varnothing(p)}{m}$
  => **평균비교횟수 : $[\frac{m}{2} * \frac{\varnothing(p)}{m}] / 2$**……(6)

- **(5) - (6) = $\varnothing(p) / 2$** ……(7)

(7)의 결과 M이 원시근이 아닌 경우, 서버의 개인키가 노출될 확률이 더 높다는 것을 예상할 수 있다. Xi의 노출은 베리사인 프로토콜에서의 문제와 마찬가지로 사용자의 패스워드를 사전탐색 공격을 가능하게 한다.

---

1) $\varnothing(p)$: Euler's Totient 함수(function). p가 소수인 경우 이 값은 p-1

2) $ord_p(M)$: modulo p인 경우에 메시지 M의 차수

4. 해결방안

한국정보보호센터의 프로토콜이 별도의 보안 프로토콜을 사용하지 않고 키를 로밍할 수 있도록 하기 위해서는 서버에 대한 인증을 제공해야한다. 그리고 사용자로부터 전송받은 로밍요청정보가 아이디에 해당되는 사용자로부터 받은 정보인지 제3자(공격자)가 서버의 공격을 위해서 전송한 정보인지를 서버 측이 확인할 수 있는 수단이나 절차가 필요하다. 현재의 프로토콜은 이러한 절차 없이 바로 응답 정보를 전송하기 때문에 서버의 개인키가 공개될 수 있는 취약성이 존재한다. 이를 해결하기 위해서는 공격자가 임의로 M의 값을 바꿀 수 없는 방법을 제시해야 할 것이다.

대칭키 알고리즘은 같은 키를 공유하고 있는 사용자간에 비밀성과 무결성을 동시에 제공할 수 있는 알고리즘이다. 따라서 로밍요청정보가 전달되는 순간에만 사용할 공유키를 사용자와 각 키 서버가 공유할 수 있다면 문제가 해결될 수 있다. 그림 2의 새로운 프로토콜은 대칭키의 이런 성질을 이용하여 메시지의 무결성을 제공할 수 있도록 하였으며, 세션키 교환을 Diffie-hellman의 키 교환 방법을 사용한다.

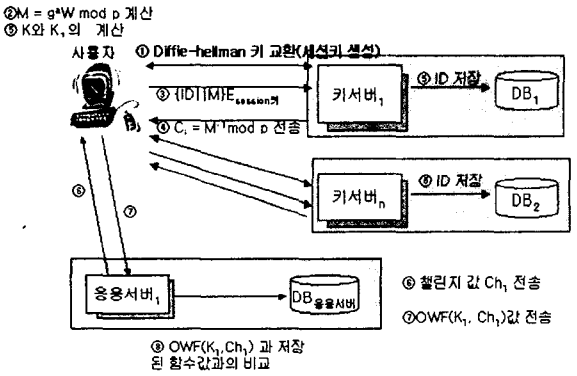

그림 2 제안한 프로토콜

그림 2에서는 ID ||[3] M의 메시지를 바로 각 키 서버로 전송하였다. 하지만 새로운 프로토콜은 키서버의 개인키를 보호하기 위해 다음의 과정을 추가한다.

① 키서버와 사용자는 Diffie-Hellman의 키 교환 방법을 이용하여 로밍요청정보 전송을 위한 세션키를 생성한다.

② 로밍요청정보 M = g^aW mod p 생성

③ (ID || M)을 ①에서 교환한 세션키를 이용해서 암호화하여 전송한다.

이 후의 과정은 한국정보보호센터의 프로토콜 과정과 동일한 과정을 거친다.

5. 비교 및 평가

분산서버를 사용하는 키로밍 프로토콜에 대해서 표 5와 같이 비교 평가하였다. Ford와 Kaliski에 의해서 제안된 프로토콜은 분산 서버의 사용을 제안한 최초의 프로토콜이었으며 키로밍 서비스를 제공하는 안전한 방법을 제공한다. 하지만 이 프로토콜은 별도로 SSL이나 TLS와 같은 보안 프로토콜이 필요하다는 단점을 가지고 있다. 한국정보보호센터에서 제안한 방법은 서버에 대한 인증을 제공함으로서 따로 보안 프로토콜이 필요하지 않으며 좀 더 쉽고 빠른 연산 방법을 제공한다. 하지만 서버의 개인키의 노출 위험이 존재하므로 완벽한 안정성을 제공하지 못한다고 볼 수 있다. 4장에서 제시한 새로운 방법은 표 1에서처럼 별도의 보안 프로토콜을 사용하지 않을 뿐만 아니라 서버의 개인키 노출 역시 막을 수 있는 프로토콜이라고 할 수 있다.

표 5 키로밍 알고리즘 비교 평가

	Verisign Key Roming	KISA Key Roaming	Proposed Protocol
키로밍권한분산	○	○	○
안정성	○	△	○
보안프로토콜 사용여부	○	×	×

6. 결론 및 향후 연구과제

키로밍 서비스는 보안에 대한 지식을 갖지 않은 사용자에게도 서비스를 사용하는데 있어서 매우 쉽고 안전한 보안 서비스를 제공할 수 있는 특성을 가져야 한다. 이를 제공하기 위한 시도로써 한국정보보호센터의 프로토콜은 서버에 대한 인증을 제공하지만 서버의 개인키가 노출될 수 있는 문제점이 존재한다. 이를 해결하기 위한 방안으로서 Diffie-hellman의 알고리즘을 이용한 세션키의 생성을 제시하였다.

향후 연구로써 본 논문에서 제시한 해결책에 대한 보완과 그에 대한 검증이 필요하다. 특히 이 프로토콜은 분산 시스템을 이용하기 때문에 이로 인한 많은 문제점이 존재하며, 이에 대한 발견과 해결책을 제시하는 것 또한 하나의 앞으로의 과제가 될 수 있을 것이다.

참고문헌

[1] S. Bellovin and M. Merritt, "Encryped Key Exchange: Password-based Protocols Secure against Dictionary Attacks", Proc. IEEE Symposium on Research in Security and Privacy, May 1992.

[2] D. Jablon, "Strong password-only authenticated key exchange", ACM Computer Communications Review, October 1996.

[3] W.Ford and B. Kaliski, Server-Assisted Generation of a Strong Secret from a Password, Proc. 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE, June 14-16, 2000.

[4] 김지연, 서버의 사전 탐색 공격을 고려한 패스워드 기반의 사용자인증 프로토콜, 대한민국특허, 2002년04월10일

[5] R. Perlman and C. Kaufman, "Secure Password-Based Protocol for Downloading a Private Key", Proc. 01999 Network and Distributed System Security Symposium, Internet Society, January 1999.

3) || : 연결연산자