情報保護學會論文誌
第20卷 第6號, 2010. 12

위임기반 인증 프로토콜의 프라이버시 취약성 분석

윤 택 영,[1†] 김 창 한[2‡]
[1]한국전자통신연구원, [2]세명대학교

Privacy Weakness Analysis of Delegation-Based Authentication Protocol

Taek-Young Youn,[1†] Chang Han Kim[2‡]
[1]ETRI, [2]Semyung University

요 약

최근, Lee 등은 모바일 네트워크에서의 로밍 서비스를 안전하게 제공하면서 모바일 사용자의 프라이버시를 보호하기 위한 기법의 하나로 위임기반 인증 프로토콜을 제안하였다. 본 논문에서는 Lee 등에 의해 제안된 프로토콜이 주장된 바와 같이 사용자의 신원에 대한 직접적인 익명성은 보장하지만 실질적인 프라이버시 보호를 제공하지 못함을 보인다. 이를 보이기 위해 Lee 등의 프로토콜은 연결불능성을 보장하지 못함을 보이고 이로 인해 모바일 사용자의 프라이버시를 보호하지 못함을 보임으로써 안전성에 문제가 있음을 보인다.

ABSTRACT

Recently, Lee et al. proposed a delegation-based authentication protocol for secure and private roaming service in global mobility networks. In this paper, we show that the protocol cannot protect the privacy of an user even though the protocol provides the user anonymity. To prove the weakness, we show that the protocol cannot provide the unlinkability and also examine the weakness of the protocol caused by the lack of the unlinkability.

Keywords: Privacy, Authentication, Security Analysis

I. 서 론

휴대용 통신 시스템(portable communication system)은 모바일 사용자들이 전역의 로밍 서비스를 영유할 수 있게 해주므로 휴대용 통신 시스템은 무선 네트워크에서의 통신을 제공함에 있어 매우 유용한 도구이다 [1,6]. 무선 네트워크에서 모바일 사용자들은 통신 데이터를 무선으로 주고받는다. 따라서 공격자들이 모바일 사용자가 주고받는 통신 내용을 도청하기 쉽다는 안전상의 취약성이 쉽게 드러난다. 결과적으로 휴대용 통신 시스템은 기존의 유선 기반의 시스템에 비하여 많은 취약성을 가진다. 이와 같이 휴대용 통신 시스템에서 발생하는 안전성 문제를 해결하기 위해 다양한 프로토콜들이 제안되어왔다 [1-8].

안전한 로밍 서비스를 위해서는 다양한 특성들이 제공되어야 한다. 이러한 다양한 보안 특성들을 제공하기 위해 DES나 AES와 같은 대칭키 암호 또는 RSA나 ECC와 같은 공개키 암호와 같은 암호화 알고리즘들이 사용된다. 기존에 제안된 기법들 중에서 대부분의 프로토콜은 대칭키를 기반으로 설계되어 있다. 이는 모바일 장비의 연산 및 전력이 유산 장비들에 비하여 매우 제한되어 있기 때문이다. 그러나 개별 암호화 알고리즘의 특성에 의해 대칭키 기반의 기법들은 부인봉쇄라는 특성을 제공할 수 없다. 따라서 부인봉쇄가 반드시 필요한 응용 환경에서 로밍 서비스를 제공하기 위해서는 공개키 기반의 프로토콜이 사용되

접수일(2010년 4월 29일), 수정일(2010년 7월 20일)
게재확정일(2010년 9월 13일)
† 주저자, taekyoung@etri.re.kr
‡ 교신저자, chkim@semyung.ac.kr

어야 한다. 로밍 서비스 이용 내역에 따라 요금이 부과되는 형태의 서비스의 경우에는 서비스 수혜자인 모바일 사용자가 로밍 서비스를 제공받지 않았다는 주장을 하지 못하도록 하기 위해 부인봉쇄 특성이 반드시 필요하다.

공개키 암호를 기반으로 로밍 서비스를 제공하는 경우 암호 알고리즘의 기본이 되는 수학 연산들의 비용이 매우 큰 문제로 작용한다. 실제로 공개키 암호에서 수행하는 기본 수학을 계산하는 것은 대칭키 암호에 비해 수천 배의 비용이 사용된다. 그러나 근래에 이르러 모바일 장비들이 기존에 비해 높은 컴퓨팅 능력을 지니게 되어 모바일 장비에서도 공개키 암호를 사용하는 것이 가능해지고 있으며 향후 더욱 개선될 것이다. 따라서 연산량에 의한 제약은 크지 않은 것으로 판단된다. 오히려 큰 문제로 고려되는 것이 PKI (public key infrastructure)의 필요성이다. PKI를 사용해야 하는 공개키 암호화를 고려하는 경우 인증서의 관리에 관련된 통신 및 연산 비용이 매우 크다. 따라서 PKI와 연관된 비용을 최소화 하는 것이 매우 중요하다. 부인봉쇄 특성을 매우 적은 비용으로 제공하기 위해 Lee와 Yeh는 무선 통신 시스템에 인증서 검증을 간소화하기 위한 일종의 위임이라는 개념을 도입하여 위임기반의 인증 프로토콜을 제안하였다 [7]. 그러나 최근 Lee 등은 Lee와 Yeh에 의해 제안된 프로토콜이 오프라인 인증 과정에서 부인봉쇄 특성을 제공할 수 없음을 보였다 [4]. Lee 등은 자신들이 제안한 공격에 안전한 개선된 프로토콜을 제안하였다 [4].

모바일 사용자의 프라이버시를 보호하기 위해 Lee 등이 제안한 프로토콜은 익명성이라는 명칭으로도 알려진 사용자 신원정보 프라이버시를 제공하도록 설계되었다. Lee 등의 프로토콜은 설계된 의도에 맞게 사용자 신원정보 프라이버시는 제공한다 [4]. 그러나 본 논문에서는 Lee 등의 프로토콜이 연결불능성(unlinkability)을 제공할 수 없음을 보이고 이로 인해 모바일 사용자의 프라이버시가 보호받을 수 없음을 보인다.

II. Lee 등의 위임기반 인증 프로토콜

본 장에서는 Lee 등에 의해 제안된 위임기반 인증 프로토콜의 구성에 대해 간략히 살펴본다. p, q는 $q|(p-1)$를 만족하는 두 소수라고 정의하자. g는 Z_p^*의 생성원이다. 프로토콜 초기 설정 단계에서 VLR (visited location register)와 HLR (home location register)는 비밀키 K_{VH}를 공유한다. ID_V와 ID_H는 VLR와 HLR의 신원정보 값으로 정의된다. $[M]_K$는 평문 M을 안전한 대칭키 암호화 기법과 키 K를 사용하여 생성한 암호문으로 정의되고 $h(M)$는 안전한 일방향함수를 사용하여 임의의 길이를 갖는 평문 M에 대해 생성한 k비트 해쉬값으로 정의된다. 또한 해쉬 함수의 연속적인 사용을 정의하기 위해 다음과 같은 표기를 사용한다:

$$h^{(k+1)}(M) = h(h^{(k)}(M)).$$

이때, $h^{(1)}(M) = h(M)$이다. 두 평문 M_1와 M_2의 연접을 다음과 같이 표기한다: $M_1 \| M_2$.

2.1 초기 설정 단계

HLR는 난수인 x와 $v = g^x \bmod(p)$로 계산되는 (x,v)를 개인키/공개키 쌍으로 보관하고 있다. HLR은 MS (mobile station)에게 서비스를 제공하기 위해 난수 k를 생성하고 $\sigma = x + kK \bmod(q)$와 $K = g^k \bmod(p)$를 계산하여 (σ, K)를 안전하게 보관한다. MS는 서비스를 제공받기 위해 인증 정보를 생성하기 위한 데이터로 (σ, K)를 HLR에게 받으며 (σ, K)는 MS의 SIM 카드에 저장된다.

2.2. 온라인 인증 단계

온라인 인증 단계를 수행하기 위하여 MS는 난수 n_1를 생성하고 해쉬 체인을 다음과 같이 생성하고 안전한 데이터 영역에 저장한다:

$$h^{(1)}(n_1), h^{(2)}(n_1), \ldots, h^{(n+1)}(n_1) (= N_1).$$

각 통신 주체들은 온라인 인증을 위하여 다음의 절차를 수행한다:

Step 1. MS는 K를 VLR에게 전송한다.

Step 2. VLR는 난수 n_2를 생성하고 이를 ID_V와 함께 MS에게 전송한다.

Step 3. MS는 난수 t를 선택하고 저장된 N_1를 데이터베이스에서 복원하여 N_1, n_2, 그리고 ID_V에 대한 서명으로 $r = g^t \bmod(p)$와 $s = \sigma \times h(N_1 \| n_2 \| ID_V) + t \times r \bmod(q)$를 계

산한다. 서명이 계산되면 r, s, K, N_1, ID_H, 그리고 ID_V를 VLR에게 전송한다.

Step 4. VLR는 다음의 조건식이 만족하는지 확인함으로써 전송받은 서명 정보를 검증한다: $g^s = (vK^K)^{h(N_1\|n_2\|ID_V)} r^r \bmod(p)$. 해당 조건식이 만족하지 않으면 VLR는 MS의 인증 요청을 거절하고 프로토콜을 종료한다. 위 조건식이 만족하면 암호문 $[N_1\|n_2\|K]_{K_{HV}}$, ID_H, 그리고 ID_V를 HLR에게 전송한다.

Step 5. HLR는 전송받은 암호문 $[N_1\|n_2\|K]_{K_{HV}}$를 복호화하고 K를 복원한다. HLR는 자신이 서비스를 제공하는 모바일 사용자들의 정보를 저장한 데이터베이스에서 K에 대응되는 σ를 검색한다. 해당하는 값이 존재하면 난수 n_3를 선택하고 $C_1 = h(N_1\|n_2\|n_3\|\sigma)$와 $l = N_1$를 계산한다. 마지막으로 HLR은 $[[N_1\|n_3\|ID_V]_\sigma\|n_2\|l\|C_1]_{K_{HV}}$, ID_H, 그리고 ID_V를 VLR에게 전송한다.

Step 6. VLR는 전송받은 암호문 $[[N_1\|n_3\|ID_V]_\sigma\|n_2\|l\|C_1]_{K_{HV}}$를 복호화하여 $[N_1\|n_3\|ID_V]_\sigma$, n_2, l, C_1를 복원하고 n_2와 l를 확인한다. $SK = C_1$를 VLR와 MS 사이의 세션키로 설정하고 $[N_1\|n_3\|ID_V]_\sigma$와 ID_V를 MS에게 전송한다.

Step 7. MS는 $[N_1\|n_3\|ID_V]_\sigma$를 복호화하여 N_1를 복원하고 $SK = C_1$를 세션키로 계산한다.

2.3. 오프라인 인증 단계

프로토콜 구성의 설명에서 l의 초기 값은 N_1으로 설정되어있다. MS는 자신의 데이터베이스에서 $h^{(n-i+1)}(n_1)$를 찾아 $[h^{(n-i+1)}(n_1)]_{C_i}$를 계산하여 VLR에게 전송한다. 여기서 상수 n은 오프라인 인증의 회수 제한을 의미한다. VLS는 MS에게 받은 값을 복호화하여 복원된 $h(h^{(n-i+1)}(n_1))$이 l과 동일한지 확인한다. 두 값이 동일하면 l을 $h^{(n-i+1)}(n_1)$로 갱신하고 새로운 세션키를 $C_{i+1} = h(l, C_i)$로 계산한다. VLS는 현재까지 수행한 오프라인 인증 회수에 대한 카운터 i를 $i = i+1$로 업데이트하고 $i \le n$를 검사하여 오프라인 인증의 수행이 허용된 회수를 넘지 않았는지 검사한다.

III. Lee 등의 위임기반 인증 프로토콜의 취약성

연결불능성 (unlinkability)는 공격자가 주어진 서로 다른 통신 데이터가 동일한 주체에 의해 생성되었는지 알 수 없음을 의미하는 특성이다. 일반적인 인증서 기반의 인증시스템의 경우, 인증서에 통신 주체의 아이디 등이 기입되어 있기 때문에 공격자가 다른 통신 데이터라고 하더라도 데이터 생성자의 동일성 여부를 쉽게 판단할 수 있으므로 연결불능성을 만족하지 못한다. 본 장에서는 위임기반 인증 프로토콜이 모바일 사용자들의 프라이버시를 보호하기 위해서는 연결불능성을 만족해야 함을 보일 것이다. 위임기반 인증 프로토콜에 대한 기존의 연구에서는 연결불능성의 필요성이 인지되지 않았다. 그러나 다음과 같은 시나리오를 고려하면 연결불능성이 필요함을 알 수 있다. 동일한 K를 사용하여 다수의 영역을 방문하는 경우에 발생할 수 있는 문제점을 예를 들어 살펴보자. 참고로, K는 동일한 사용자에게 할당된 난수로 처음 키 생성시에는 난수가 선택되어 계산되는 값이지만 MS에게 할당된 이후에는 동일한 값으로 사용되는 것이다. 핸드폰과 같은 모바일 디바이스를 고려하는 경우 공격자는 N개의 영역에서 K라는 동일한 값이 사용된다는 것을 인지하면 해당 영역에서 공통적으로 존재하던 사용자를 추려낼 수 있으므로 K를 사용하는 사용자에 대한 신원정보를 알게 되는 것과 마찬가지의 정보유출을 예상할 수 있다. 또한 어떠한 영역에 존재하는 모바일 디바이스가 매우 적은 경우(극단적으로는 1개) 해당 영역에 있던 모바일 디바이스 중에서 K를 사용하는 것을 찾는 것은 어렵지 않다. 이와 같은 프라이버시 침해의 우려가 가능하기 때문에 위임기반 인증 프로토콜은 모바일 사용자들의 프라이버시를 보호하기 위해 연결불능성을 만족해야한다.

[4]에서 분석되었듯이 Lee 등의 프로토콜은 사용자 신원에 대한 프라이버시는 제공되지만 모바일 사용자에 대한 프라이버시가 완전히 보호받지 못하고 있다. 이는 Lee 등의 프로토콜이 연결불능성을 만족하지 못함에서 기인한다. 연결불능성을 만족하지 못하는 이유는 다음과 같다. MS는 모든 온라인 인증 단계에서 동일한 상수 K를 사용한다. 다음과 같은 경우를 고려해보자. $Area_i$를 VLR_i에 의해 관리되는 영역이라고 정의하고, C_j^i를 $Area_i$에서 생성된 j번째 세션키라고 정의하자. 그리고 MS가 N개의 지역을 다음과 같은 순서로 이동한다고 가정하자: $Area_1 \rightarrow Area_2 \rightarrow \cdots \rightarrow Area_N$. MS는 $Area_{i-1}$에서 $Area_i$로 이동하면서

VLR_i와 온라인 인증을 수행하여 새로운 세션키 C_1'를 생성한다. 온라인 인증을 수행하기 위해서 MS는 K를 모든 VLR_i에게 전송해야한다. 즉, MS는 새로운 영역에 방문하면 해당 영역을 관리하는 VLR와 키를 교환하기 위해 공개된 채널을 통해 K를 전송한다. 따라서 공격자는 이와 같은 정보를 사용하여 MS가 N개의 영역을 $Area_1$에서 $Area_N$순으로 방문한다는 정보를 획득할 수 있다. 결과적으로 공격자는 모바일 사용자의 동선을 추적함으로써 프라이버시를 훼손할 수 있다.

MS가 다수의 지역으로 이동하지 않으면 연결불능성의 중요성은 크지 않다. 그러나 가동성이 모바일 사용자의 중요한 특성이므로 연결불능성은 위임기반 인증 프로토콜의 안전성을 위해 매우 중요한 특성이다.

IV. 결 론

본 논문에서는 Lee 등의 위임기반 인증 프로토콜이 연결불능성을 제공하지 못함으로 보였다. 또한 이로 인해 Lee 등의 프로토콜은 주장한 바와 같이 사용자의 신원 정보에 대한 직접적인 익명성은 제공하였지만 사용자의 프라이버시를 보호할 수 없고 이로 인하여 안전한 로밍 서비스를 제공할 수 없음을 보였다. 이는 서로 다른 두 통신 메시지를 생성한 주체가 동일함을 통신의 수행에서 사용되는 정보 K가 동일한지를 검사함으로써 확인할 수 있기 때문에 연결불능성이 제공되지 못하여 발생한 취약성이었다. 따라서, 안전한 위임기반 인증 프로토콜을 설계하기 위해서는 연결불능성이 반드시 고려되어야 한다.

참고문헌

[1] M.J. Beller, L.F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," IEEE J. Sel. Areas Commun., vol. 11, pp. 821-829, Aug. 1993.

[2] C.C. Lo and Y.J. Chen, "Secure communication mechanisms for GSM networks," IEEE Trans. Consum. Electron., vol. 45, pp. 1074-1080, Nov. 1999.

[3] T.-F. Lee, C.-C. Chang, and T. Hwang, "Private authentication techniques for the global mobility network," Wireless Personal Commun., vol. 35, no. 4, pp. 329-336, Dec. 2005.

[4] T.-F. Lee, S.-H. Chang, T. Hwang, and S.-K. Chong, "Enhanced Delegation-Based Authentication Protocol for PCSs," IEEE Transactions on Wireless Communications, vol. 8, no. 5, pp. 2166-2171, May 2009.

[5] H.-Y. Lin and L. Harn, "Authentication protocols with non-repudiation services in personnel communication systems," IEEE Commun. Lett., vol. 3, no. 8, pp. 236-238, Aug 1999.

[6] H.-Y. Lin, "Security and authentication in PCS," Comput. Elect. Eng., vol. 25, no. 4, pp. 225-248, Jul. 1999.

[7] W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," IEEE Trans. Wireless Commun, vol. 4, no. 1, pp. 57-64, Jan. 2005.

[8] M. Rahnema, "Overview of the GSM system and protocol architecture," IEEE Commun. Mag., pp. 92-100, Apr. 1993.

[9] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Trans. Wireless Commun., vol. 4, pp. 734-742, Mar. 2005.

〈著者紹介〉

윤 택 영 (Taek-Young Youn) 일반회원
2003년 2월: 고려대학교 수학과 졸업
2005년 2월: 고려대학교 정보보호대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
2010년 7월~현재: 한국전자통신연구원 연구원
〈관심분야〉 정보보호 프로토콜, 공개키 암호

김 창 한 (Chang Han Kim) 정회원
1985년 2월: 고려대학교 수학과 학사
1987년 2월: 고려대학교 수학과 석사
1992년 2월: 고려대학교 수학과 박사
1992년 3월~현재: 세명대학교 정보통신학부 교수
〈관심분야〉 정보보호, 공개키 암호, 연산기