간단하고 효율적인 키 교환 프로토콜

*이성운[O] *김우헌 **김현성 *유기영
*경북대학교 컴퓨터공학과, **경일대학교 컴퓨터공학과
{staroun[O], whkim, hskim, yook}@infosec.knu.ac.kr

Simple and Efficient Authenticated Key Agreement Protocol

*Sungwoon Lee[0] *Woohun Kim **Hyunsung Kim *Keeyoung Yoo
*Dept. of Computer Engineering, Kyungpook Natl. Univ.,
**Dept. of Computer Engineering, Kyungil Univ.,

요 약

본 논문에서는 간단하고 효율적인 상호 인증 가능한 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 두 참여들 사이에 미리 공유된 사람이 기억할 수 있는 패스워드를 이용하여 세션키를 교환하고 서로를 인증한다. 우리는 제안한 프로토콜이 중간 침입자 공격과 패스워드 추측 공격에 안전하고 완전한 전방향 보안성을 제공함을 보여준다. 즉, 제안한 프로토콜은 수동적인 공격자나 적극적인 공격자의 공격들에 안전하다. 제안된 프로토콜의 안정성은 이산대수 문제와 Diffie-Hellman 문제의 어려움에 기반을 두고 있다. 제안된 프로토콜은 구성이 간단하고 효율적이어서 소프트웨어나 하드웨어로 구현하기가 용이할 것으로 기대된다.

1. 서 론

1976년에 제안된 Diffie-Hellman 키 교환 프로토콜은 안전하지 않은 통신상에서 안전하게 세션키를 공유하기 위한 가장 잘 알려진 방법이다[1]. 이 프로토콜은 유한 필드 상에서 이산대수 문제와 Diffie-Hellman문제의 어려움을 이용하여 참여자들간에 세션키를 공유한다. 하지만 참여자들을 인증하는 방법을 제공하지 못하기 때문에 중간 침입자 공격에 대하여 안전하지 못하였다. 이러한 문제를 해결하기 위하여 1992년에 Bellovin과 Merritt는 낮은 엔트로피(entropy)를 가진 패스워드와 대칭키 · 공개키 암호화 알고리즘들을 사용하여 EKE(Encrypted Key Exchange) 프로토콜을 제안하였다[2]. 그 이후로 패스워드를 이용하는 다양한 키 교환 프로토콜들이 제안되어 왔다[3-11].

이러한 패스워드 기반의 기법들은 별도의 장비가 필요 없고 사용자가 알고있는 지식을 이용하므로 큰 비용을 들이지 않고도 쉽게 사용 될 수 있다. 그러나 사용자들은 쉽게 기억할 수 있는 패스워드를 선택하는 경향이 있기 때문에 패스워드 기반의 프로토콜들에게 패스워드 추측 공격은 가장 큰 위협이다. 또한 신뢰할 수 없는 통신망을 사용할 때는 공격자에 의하여 통신이 도청되거나 심지어 변경될 수도 있기 때문에 추가적인 문제들이 발생할 수 있다. 그래서 안전한 프로토콜이 되기 위해서는 패스워드 추측 공격 뿐 아니라 통신 메시지들에 대한 도청(eavesdropping)이나 변경(modification), 반송(reflection), 재전송(replay), 그리고 위장(impersonation) 공격 등을 처리할 수 있어야 한다.

본 논문에서는 이러한 중간 침입자 공격(man-in-the-middle attack)들과 패스워드 추측 공격(password guessing attack)에 안전하고 완전한 전방향 보안성(perfect forward secrecy)을 제공할 수 있는 키 교환 프로토콜을 제안한다.

2. 보안요구사항

패스워드 기반의 키 교환 프로토콜은 사람이 기억 가능한 패스워드를 이용하여 서로를 인증한다. 또한 많은 경우 안전하지 않은 통신망을 사용하여 프로토콜이 진행될 수 있으므로 다음과 같은 보안 요구사항들을 만족해야한다[10].

○ 중간 침입자 공격에 안전해야 한다.

키 교환 프로토콜은 안전하지 않은 통신상에서 메시지 교환을 통해 세션키를 공유하고 세션키의 정확성을 검증한다. 그래서 공격자는 통신 선로 중간에서 세션키 교환에 사용되는 전송 메시지들을 도청(eavesdropping)하여 세션키의 정보를 알아내려고 할 수 있다. 그리고 전송 메시지들을 변경(modification), 반송(reflection), 또는 이전 세션의 메시지들을 저장해 두었다가 다음 세션들에서 재전송(replay)하는 방법 등으로 참여자들이 알지 못한 상태에서 잘못된 세션키를 공유하도록 유도할 수도 있다. 또한 공격자는 정당한 참여자로 위장(impersonation)하여 다른 정당한 참여자와 정상적인 방법으로 세션키를 공유하려고 할 수 있다. 키 교환 프로토콜은 이러한 공격들에도 세션키와 패스워드에 관한 정보를 노출시켜서는 안되며 잘못된 세션키의 공유를 탐지할 수 있어야 한다.

○ 패스워드 추측 공격에 안전해야 한다.

패스워드 추측 공격은 온라인 패스워드 추측 공격과 오프라인 패스워드 추측 공격으로 나뉠 수 있다. 온라인 패스워드 추측 공격은 패스워드 인증 실패 횟수를 셈으로써 쉽게 탐지되고 시도 횟수를 제한함으로서 쉽게 조치될 수 있다. 그러나 공격자는 안전하지 않은 통신상의 메시지를 도청하거나 정당한 사용자로 가장하여 다른 사용자와 세션키 교환 시에 발생하는 정보들을 모아 오프라인으로 패스워드에 관한 정보를 알아내려고 할 수 있다. 이러한 공격을 오프라인 패스워드 추측 공격이라 한다. 오프라인 패스워드 추측 공격은 사용자가 쉽게 기억할 수 있도록 낮은 엔트로피를 가진 패스워드를 사용해야 하는 패스워드 기반의 키 교환 프로토콜들에는 가장 큰 위협이다. 그러므로 패스워드 기반 키 교환 프로토콜은 패스워드 추측 공격에 안전해야 한다.

○ 완전한 전방향 보안성을 제공해야 한다.

공격자가 참여자의 패스워드를 알아내었다 할지라도 이전에 사용된 세션키에 관한 정보는 알 수 없어야 한다. 이러한 성질을 완전한 전방향 보안성이라 한다. 패스워드 기반의 키 교환 프로토콜은 이러한 성질을 만족해야 한다.

3. SEKA 프로토콜

본 장에서는 Diffie-Hellman 키 교환 프로토콜을 기반으로 사람이 기억할 수 있는 패스워드를 이용하여 참여자들 사이에 서로를 인증하고 세션키를 교환할 수 있는 간단하고 효율적인 키 교환 프로토콜(SEKA)을 제안한다.

프로토콜의 참여자인 A와 B는 합법적인 사용자들이라 가정한다. 또한 A와 B는 안전하게 Z_n^*상의 생성자인 g, 큰 소수인 n, 그리고 패스워드 π를 미리 공유하고 있다고 가정한다. A와 B는 프로토콜이 시작하기 전에 그들 사이에 미리 결정된 방법으로 패스워드 π로부터 정수 Q를 계산하고, Z_n^*상의 Q의 역수인 Q^{-1}를 구한다. 예를 들어 간단하게 Q를 구하는 방법은 π를 취하거나 $h(\pi)$를 취하는 것이다. $h()$는 일방향(one-way) 해쉬 함수이다. 간편함을 위해 'mod n' 연산 표기를 생략한다. 제안된 프로토콜은 다음과 같이 수행된다.

1단계. A는 임의의 정수 a를 선택하고 다음과 같이 X_A를 계산하여 B에게 전송한다.

$$X_A = g^a \oplus Q$$

2단계. B는 임의의 정수 b를 선택하고 다음과 같이 X_B를 계산하여 A에게 전송한다.

$$X_B = g^b \oplus Q^{-1}$$

그리고 B는 다음과 같이 Y_B와 K_B, 그리고 V_B를 계산한다.

$$Y_B = X_A \oplus Q = g^a$$

$$K_B = (Y_B)^b = g^{ab}$$

$$V_B = h(B, X_A, K_B)$$

3단계. A는 B로부터 메시지 X_B를 받은 후에 다음과 같이 Y_A, K_A, 그리고 V_A를 계산한다.

$$Y_A = X_B \oplus Q^{-1} = g^b$$

$$K_A = (Y_A)^a = g^{ab}$$

$$V_A = h(A, X_B, K_A)$$

그리고 A는 V_A를 B에게 전송한다.

4단계. B는 A로부터 받은 V_A가 $h(A, X_B, K_B)$와 같은지를 검사한다. 만약 그들의 값이 같다면 B는 K_A가 정확하다고 확신한다. 그리고 V_B를 A에게 전송한다.

5단계. A는 B로부터 받은 V_B가 $h(B, X_A, K_A)$와 같은지를 검사한다. 만약 그들의 값이 같다면 A는 K_B가 정확하다고 확신한다.

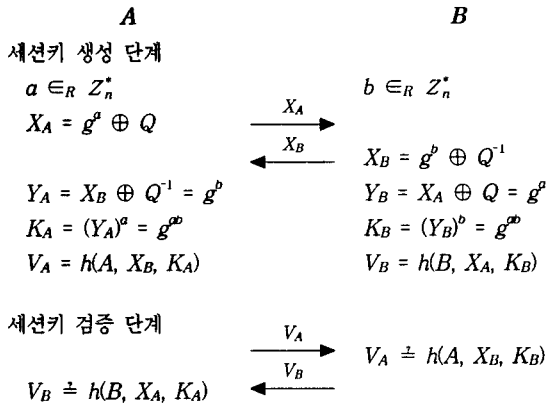

그림 1. 제안된 프로토콜

4. 안전성 분석

본 장에서는 본 논문에서 제안한 프로토콜인 SEKA가 2장에 제시된 네 가지 보안 요구사항을 만족하는지를 분석한다. Bellare와 Rogaway는 두 참여자들 사이의 인증된 키 교환 프로토콜의 안전성을 검증하기 위해 랜덤 오라클 모델(random oracle model)이라 불리는 첫 검증 모델을 제안하였다[12]. 우리는 랜덤 오라클 모델에서 제안한 프로토콜의 안전성을 검증한다.

정리1. 제안된 프로토콜은 중간 침입자 공격에 안전하다.

(증명) 공격자가 세션키를 계산할 수 있거나 참여자들로 하여금 알지 못하게 잘못된 세션키를 계산하도록 유도할 수 있다면 그 공격자는 성공한다고 가정하자. 우리는 랜덤 오라클 모델에서 공격이 성공할 수 없음을 보여줄 것이다.

첫째로, 수동적인 공격자가 공격하는 경우를 고려하자. 즉 공격자는 전송 메시지들을 도청을 하여 X_A, X_B, V_A, V_B를 얻을 수 있다. 그러나 공격자가 이 값들을 획득한다 하더라도 Q, Q^{-1}, K_A, K_B 값을 계산할 확률은 이산대수 문제와 Diffie-Hellman 문제의 어려움에 근거하여 무시할만하다. 둘째로, 적극적인 공격자의 수정 공격을 고려하자. 공격자가 X_A와 X_B를 중간에서 변경하여 상대에게 전송한다면, 이 위조된 값들은 A와 B에 의해 K_A와 K_B를 생성하는데 각각 사용되게 된다. 그러나 A는 임의의 정수 a를 사용하여 K_A를 계산하고 B는 임의의 정수 b를 사용하여 K_B를 계산하기 때문에 K_A와 K_B의 값이 같게 될 확률은 무시할만하다. 결국, 이 공격은 검증단계에서 검증 값이 다르게 되므로 탐지되게 된다. 셋째로, 적극적인 공격자의 재전송 공격을 고려하자. 전송 공격은 이전 세션의 전송 메시지들을 저장해 두었다가 이후 세션들에 이용하는 공격이다. 그러나 매 세션마다 각 참여자들은 새로운 임의의 난수들을 선택하여 사용한다. 공격자가 이 난수들을 알 수 있는 확률은 이산대수문제와 Diffie-Hellman 문제의 어려움에 근거하여 무시할만하다. 결국 재전송 공격은 수정 공격과 같이 검증 단계에서 검증 값이 다르게 되므로 탐지되게 된다. 넷째로, 적극적인 공격자의 반송 공격을 고려한다. 즉 공격자는 통신선로 중간에서 A가 B에게 보낸 X_A를 A에게 되돌려보내고, B가 A에게 보낸 X_B를 B에게 되돌려 보낼 수 있다. 제안된 프로토콜에서는 이러한 반송 공격을 막기 위하여 각 참여

자의 식별자 값인 A와 B를 검증 단계에서 사용한다. 공격자의 반송 공격은 세션키 정보 검증 단계에서 검증 값을 다르게 만듦으로 A와 B에 의해서 탐지될 수밖에 없다. 다섯째로, 공격자는 참여자로 위장하여 정상적인 방법으로 합법적인 참여자와 세션키를 공유하려고 할 수 있다. 그러나 이러한 위장 공격은 공격자가 패스워드를 알지 못하기 때문에 위의 경우들처럼 검증 단계에서 모두 탐지될 것이다.

결국 제안한 프로토콜은 이와 같은 중간 침입자 공격들에 안전하다.

정리2. 제안한 프로토콜은 패스워드 추측 공격에 안전하다.

(증명) 먼저, 도청한 메시지들을 이용한 패스워드 추측 공격을 고려한다. 공격자는 메시지 X_A, X_B, V_A, V_B를 가로채 저장하고, 패스워드로 사용될 수 있는 π'를 선택하여 Q'와 Q'^{-1}를 계산한다. 그리고 Q'나 Q'^{-1}들이 정확한지 미리 저장해 둔 값들을 이용하여 검증한다. 이를 패스워드 범위에 있는 모든 π'에 대해서 반복 수행함으로써 선택된 π'가 참여자들이 사용하고 있는 π인지를 확인할 수 있다. 그러나 제안된 프로토콜에서는 전송 메시지인 X_A, X_B, V_A, V_B에 Q'나 Q'^{-1}를 적용하여도 Q'나 Q'^{-1}가 정확한지를 검증할 방법이 없다.

또한 공격자가 정당한 참여자로 위장한 경우를 두 가지로 나누어 고려해 보자. 첫 번째로 공격자 A로 위장했다면 공격자가 얻을 수 있는 값들은 자신에 의해 만들어진 a, g^a, $g^a \oplus Q'$와 B에 의해 보내진 $g^b \oplus Q^{-1}$ 값이다. 그러나 이들에는 검증 가능한 자료가 없기 때문에 패스워드 추측 공격이 불가능하다. 그리고 공격자는 V_A로 응답을 해야하지만 정확한 응답을 할 수 있는 확률은 무시할만하다. 두 번째로 공격자 B로 위장했다면 공격자가 얻을 수 있는 값들은 자신에 의해 만들어진 b, g^b, $g^b \oplus Q'^{-1}$와 A에 의해 보내진 $g^a \oplus Q$와 $h(A, g^b \oplus Q'^{-1}, (g^b \oplus Q'^{-1} \oplus Q^{-1})^a)$이다. 그러나 또한 이들에도 검증 가능한 자료가 없기 때문에 패스워드 추측 공격이 불가능하다. 그리고 공격자는 V_B로 응답을 해야하지만 정확한 응답을 할 수 있는 확률은 무시할만하다. 즉 프로토콜은 공격자에게 패스워드를 추측하는데 필요한 충분한 정보를 제공하지 않는다. 그러므로 제안된 프로토콜은 패스워드 추측 공격에 안전하다.

정리 4. 제안한 프로토콜은 완전한 전방향 보안성을 제공한다.

(증명) 완전한 전방향 보안성을 제공하기 위해서는 패스워드가 공격자에게 노출되었다 할지라도 이전에 사용된 세션키들은 안전해야 한다. 제안된 프로토콜에서 패스워드를 취득한 공격자가 이전 세션키를 얻기 위하여 취할 수 있는 방법은 다음과 같다. 공격자가 패스워드 π를 알아내었다면 π로부터 Q와 Q^{-1}를 구한다. 공격자가 Q와 Q^{-1}을 안다면 X_A와 X_B를 가로채 각각 Q와 Q^{-1}를 이용하여 g^a와 g^b도 구할 수 있을 것이다. 그렇지만 g^a와 g^b이 드러난다 할지라도 이 값들과 V_A, V_B를 이용하여 세션키인 g^{ab}를 구할 수 있는 확률은 이산대수 문제와 Diffie-Hellman 문제의 어려움 때문에 무시할만하다. 결국, 오랫동안 사용되는 사용자의 패스워드가 공격자에게 노출되어도 공격자는 과거에 사용되었던 세션키들을 알아낼 수 없다.

5. 결론

본 논문에서는 참여자들 사이에 미리 공유된 패스워드를 기반으로 상호 인증을 제공하는 키 교환 프로토콜을 제안하였다. 제안된 프로토콜의 안전성은 이산대수 문제와 Diffie-Hellman 문제의 어려움에 기반하고 있다. 우리는 랜덤 오라클 모델에서 제안된 프로토콜이 안전함을 증명하였다. 그러므로 제안된 프로토콜은 중간 침입자 공격과 패스워드 추측 공격에 안전하고 완전한 전방향 보안성을 제공한다. 또한 제안된 프로토콜은 이산대수 문제와 Diffie-Hellman 문제의 어려움을 갖는 다른 그룹들에도 쉽게 적용될 수 있다. 마지막으로 우리의 프로토콜은 구성이 간단하기 때문에 이해하기 쉽고 하드웨어나 소프트웨어로 구현하기에 무척 용이할 것으로 기대된다.

참 고 문 헌

[1] Diffie W., and Hellman M.E., "New directions in cryptography," *IEEE Trans., IT-22*, 1976, (6), pp. 644-654.

[2] S. M. Bellovin, and M. Merrit, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," *IEEE Symposium on Research in Security and Privacy*, pp. 72-84, 1992.

[3] D. Jablon, "Strong Password-Only Authentication Key Excahnge," *ACM Computer Communication Review*, vol. 26. 5, 5-26, October 1996.

[4] T. Kwon, and J. Song, "Authenticated key exchange protocols resistant to pasword guessing attacks," *IEE Proceedings-Communications*, 145(5), pp. 304-308, October 1998.

[5] B. W. Simon, and M. Alfred, "Authenticated Diffie-Hellman Key Agreement Protocols," *Proceedings of SAC 98*, LNCS, 1998.

[6] Seo D. H., and Sweeney P., "Simple authenticated key agreement algorithm," *IEE Electronics Letter*, 1999, 35, (13), pp. 1073-1074.

[7] V. Boyko, P. MacKenzie, and S. Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," *Advances in Cryptology-EUROCRYPT' 2000*, pp, 156-171, 2000.

[8] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks," *Advances in Cryptology-EUROCRYPT'2000*, pp, 139-155, 2000.

[9] T. Kwon, and J. Song, "A Study on the Generalized Key Agreement and Password Authentication Protocol," *IEICE TRANS. COMMUN.*, vol.E83-B, no.9, pp.2044-2050, SEP 2000.

[10] Simon B.W. and Alfred M., "Authenticated Diffie-Hellman Key Agreement Protocols," *Proceedings of SAC 98*, LNCS, 1998.

[11] P. MacKenzie, and R. Swaminathan, "Secure Network Authentication with Password Identification," *Submission to IEEE P1363a*, July, 1999.

[12] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," *Advances in Cryptology-CRYPTO'93*, Vol. 773, pp. 232-249, 1994.