情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

Gu-Xue의 개선된 Secret Handshake 기법의 안전성 분석*

윤 택 영,[1†] 박 영 호[2‡]
[1]한국전자통신연구원, [2]세종사이버대학교

Security analysis on the Gu-Xue improved secret handshakes scheme*

Taek-Young Youn,[1†] Young-Ho Park[2‡]
[1]Electronics and Telecommunications Research Institutel, [2]Sejong Cyber University

요 약

최근 Gu와 Xue는 Huang와 Cao에 의해 제안되었던 기법을 수정하여 개선된 secret hankshake 기법을 제안하였다. Gu와 Xue의 기법은 Huang와 Cao의 기법이 가지고 있던 취약성을 개선하면서 기존의 기법들에 비해 효율적이라는 장점도 동시에 제공하고 있다. 본 논문에서는 Gu와 Xue에 의해 고려되었던 안전성 요구사항들을 살펴보고 공격자에 대한 정의가 현실적으로 제한되었음을 보인다. 현실성에 맞게 수정된 공격자 모델에서는 Gu와 Xue의 기법이 안전하지 않음을 보인다

ABSTRACT

Recently, Gu and Xue proposed an improved secret handshakes scheme with unlinkability by modifying the Huang-Cao scheme. Their proposal not only solves security weakness in the Huang-Cao scheme but also is more efficient than previously proposed secret handshakes schemes. In this letter, we examine the correctness of Gu and Xue's security requirements and show that the adversary model is not correctly defined. We also show that the Gu-Xue scheme is not secure against the attacks under correctly defined adversary model.

Keywords: Secret Handshake, Security Analysis

I. 서 론

Secret handshake 기법은 두 사용자가 동일한 기관에서 받은 정보를 사용하지 않는 경우에는 소속 정보에 대해서도 알려주지 않고 handshake를 수행하도록 함으로써 각 통신주체의 프라이버시를 보호하는 기법이다. 가장 널리 알려진 응용 환경으로는 CIA와 같이 소속정보가 중요한 기관원들이 자신의 CIA 소속 여부를 밝히지 않고도 서로 같은 기관원임을 확인할 수 있는 handshake를 수행할 수 있다.

[1]에서 Balfanz 등은 페어링 연산을 기반으로 최초의 secret handshake 기법을 제안하였고, 많은 기법들이 효율성을 개선하거나 안전성을 향상하기 위해 제안되었다 [2-7]. [3]에서 Huang와 Cao는 불연결성(unlinkable)을 제공하는 secret handshake 기법을 제안하였다. 그러나, [6]와 [7]에서 해당 기법의 취약성이 밝혀졌다. 최근에 Gu와 Xue는 [3]에서 제안된 기법의 취약성을 개선하여 안전성이

접수일(2012년 3월 7일), 수정일(2012년 4월 30일), 게재확정일(2012년 5월 1일)
* 본 연구는 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업입니다. (No. 2011-0004395).
† 주저자, taekyoung@etri.re.kr
‡ 교신저자, youngho@sjcu.ac.kr

향상된 기법을 제안하였다 [2]. Gu와 Xue의 기법은 Huang와 Cao의 기법이 가지던 취약성을 개선하였을 뿐 아니라 기존의 결과들 중에서 가장 성능이 좋다는 장점도 가진다.

본 논문에서는 [2]에서 고려되었던 secret handshake 기법의 안전성 요구사항들을 살펴보고 위장공격, 공모공격에 대한 안전성 정의가 올바르지 못함을 보인다. 상기 조망을 바탕으로 안전성 정의를 올바르게 수정하고, 개정된 안전성 정의하에서 Gu와 Xue의 기법이 안전하지 않음을 밝힌다.

II. Gu와 Xue의 Secret Handshake 기법

본 장에서는 [2]에서 Gu와 Xue에 의해 제안된 secret handshake 기법을 간략히 살펴보도록 한다. 각 구성요소에 대한 설명은 [2]의 내용을 따른다.

2.1. Setup 단계

본 단계는 총 3개의 알고리즘으로 구성되어있다.

System Parameter - k를 안전성 변수라고 하자. G_1와 G_2는 소수 q를 위수로 갖는 순환군이라고 하자. $e: G_1 \times G_1 \rightarrow G_2$는 페어링 연산으로 정의한다. 따라서 모든 정수 a,b와 포인트 $P,Q \in G_1$에 대해 다음의 관계식이 만족한다: $e(aP,bQ) = e(P,Q)^{ab}$. G_1^*는 G_1의 모든 non-identity 값을 원소로 갖는 집합이다. 본 기법에서는 다음의 두 개의 해쉬함수가 사용된다: $H_0 : \{0,1\}^* \rightarrow G_1^*$, $H_1 : \{0,1\}^* \rightarrow \{0,1\}^k$.

Create Group - 그룹 G를 생성하기 위해 그룹 관리자(GA)는 난수 s를 선택하고 해당 그룹에 할당된 비밀키로 사용한다. 그룹 G는 위 난수 s로 생성된 비밀키를 가진 사용자의 집합으로 정의된다.

Admit Member - 사용자 U_i를 그룹 G의 구성원으로 포함시키려면, 그룹 관리자(GA)는 난수 id_i를 선택하고 $Q_i = H_0(id_i)$와 $S_i = sQ_i$를 계산한다. 그리고 GA는 $cert_i = (id_i, S_i)$를 U_i에서 준다.

2.2. Handshake 단계

두 통신 참여자 U_A와 U_B를 각기 그룹 G_0와 G_1의 구성원이라고 하자. 두 통신주체는 다음과 같은 과정을 수행한다.

Step 1. U_A는 난수 x를 선택하고 $Q_A = H_0(id_A)$에 대해 $E_A = xQ_A$를 계산하고 U_B에게 전송한다.

Step 2. U_B는 E_A를 받으면 난수 y를 선택하고 $Q_B = H_0(id_B)$에 대해 $E_B = yQ_B$, $K_B = e(E_A, yS_B)$, $V_B = H_1(K_B, E_B, resp)$를 계산한다. U_B는 E_B와 V_B를 U_A에게 전송한다.

Step 3. U_A는 전송받은 E_B와 V_B를 사용하여 $K_A = e(xS_A, E_B)$를 계산하고 $V_B = H_1(K_A, E_B, resp)$가 만족하는지 검증한다. 만약 위 조건식이 거짓이면, U_A는 프로토콜 수행을 종료한다. 그렇지 않으면 $V_A = H_1(K_A, E_A, init)$를 계산하고 이를 U_B에게 전송한다. U_A는 $sk_A = H_1(K_A, E_A, E_B, agree-on)$를 계산하고 세션키로 사용한다.

Step 4. U_B는 $V_A = H_1(K_B, E_A, init)$를 검사하고 거짓이면 프로토콜을 중단한다. 만약 해당 조건이 참이면, $sk_B = H_1(K_B, E_A, E_B, agree-on)$를 계산하고 세션키로 사용한다.

프로토콜 구성의 설명에서 $cert$, $init$, $resp$, $agree-on$은 [2]에서 정의된 문자열로 자세한 내용은 해당 논문을 참조하기 바란다.

III. Gu-Xue 기법의 취약성

본 장에서는 Gu-Xue 기법의 분석에 사용된 안전성 요구사항들을 살펴보고 위장공격(Masguerade Attack), 공모공격(Collusion attack), 구성원 검색공격(Member Detection Attack)에 대한 안전성 정의가 제한적임을 보인다. 따라서 현실적인 공격환경을 고려한 수정된 안전성 공격자 모델을 제안하고 이 안전성 공격자 모델 기준에서는 Gu와 Xue의 기법이 안전하지 않음을 보인다.

3.1. 안전성 요구사항의 재검토

다양한 안전성 요건들이 [2]에서 secret hand-

shake 기법의 분석을 위해 사용되었고 Gu-Xue 기법은 해당 기준들을 모두 만족하였다. 그러나 Gu-Xue 기법은 위장공격, 공모공격, 구성원 검색공격에 안전하지 않다. 가장 큰 문제점은 [2]에서 고려된 공격자 모델의 한계이다. 상기 기술된 공격들에서 공격자는 다양한 방법으로 올바른 사용자의 비밀키를 획득할 수 있는 것으로 가정되어야 한다. 물론 [2]에서도 올바른 사용자의 비밀키 노출은 가정이 되어있지만 공격 대상 그룹의 구성원은 아니라는 비현실적인 가정을 두었다. 결론적으로 공격 대상이 되는 그룹의 모든 구성원이 비밀 정보를 노출하지 않을 것이라는 과도한 사실을 가정한 것이다. 그러나 현실적으로 공격 대상이 되는 그룹의 구성원도 비밀키를 노출할 수 있다는 가정이 타당하다.

3.2. 개선된 공격자 모델에서의 Gu-Xue 기법의 안전성

Gu-Xue 기법의 취약점을 설명하기 위해 공격 대상 그룹에 비밀키를 노출한 사용자가 존재하는 것으로 가정하고 이를 U_A라고 하자. A는 U_A의 비밀키를 사용해서 공격을 수행하는 공격자로 가정한다. U_A와 같은 그룹원인 공격대상을 U_B라고 하자. U_A의 비밀키는 $S_A = sQ_A$와 $Q_A = H_0(id_A)$에 대해 (id_A, S_A)이다. 공격자는 U_A의 비밀키를 사용하여 새로운 의미 있는 비밀키 $S_{A'} = rS_A$를 만들 수 있다. 여기서 $Q_{A'} = rQ_A$이고 r은 임의로 선택된 난수이다. 공격자는 S_A대신 $S_{A'}$를 사용하여 올바른 사용자 U_B와 동일한 세션키를 생성할 수 있다.

Step 1. A는 난수 x를 선택하고 $E_{A'} = xQ_{A'}$를 계산하여 U_B에게 전송한다.

Step 2. U_B는 $E_B = yQ_B$, $K_B = e(E_{A'}, yS_B)$, $V_B = H_1(K_B, E_B, resp)$를 임의로 선택된 y로 계산하고 E_B와 V_B를 A에게 전송한다.

Step 3. 공격자는 E_B를 받아 $K_{A'} = e(xS_{A'}, E_B)$, $V_{A'} = H_1(K_{A'}, E_{A'}, init)$, $sk_{A'} = H_1(K_{A'}, E_{A'}, E_B, agree-on)$를 계산하고 $V_{A'}$를 U_B에게 전송한다.

Step 4. U_B는 $V_{A'} = H_1(K_B, E_{A'}, init)$를 검사하고 만족하지 않으면 프로토콜을 종료한다. 그렇지 않으면 세션키 $sk_B = H_1(K_B, E_{A'}, E_B, agree-on)$를 계산한다.

공격자는 $K_{A'} = K_B$이 만족하는 경우에만 상기 절차를 통하여 올바른 사용자 U_B와 동일한 세션키를 교환할 수 있다. 공격자와 U_B가 공유한 키는 다음의 식을 통해 같음을 확인할 수 있다:

$$K_{A'} = e(xS_{A'}, E_B) = e(Q_A, Q_B)^{xyrs} = e(E_{A'}, yS_B) = K_B.$$

올바른 사용자는 공격자와 동일한 세션키를 공유했으므로 공격자 A가 자신과 동일한 그룹의 구성원이라고 신뢰하므로 그룹 구성원에게만 알려줄 수 있는 정보를 공격자에게 제공하게 된다. 이외에도 같은 그룹 구성원으로 인정하기 때문에 발생하는 다양한 문제점이 야기될 수 있다.

올바른 사용자의 비밀키 정보가 노출되면 이를 기반으로 올바른 사용자를 가장하는 위장공격이 수행가능하다. 또한 기본적으로 가정이 되는 비밀키를 제공하는 내부 공격자가 존재한다면 그 내부 공격자와 함께 공모공격을 수행하여 위와 같이 공격 대상이 되는 사용자와 동일한 세션키를 공유할 수 있다. 결과적으로 상기 기술한 문제점은 위장공격과 공모공격에 대한 안전성 모델의 변경을 요구하게 된다. 결과적으로 [2]에서는 두 공격에서 공격대상 그룹의 구성원은 비밀정보가 노출되지 않는다고 가정하에서 두 공격에 대한 안전성을 분석하였고 이러한 가정의 비약에서 실제 안전성이 올바르게 분석되지 않는 결과를 야기하였다.

IV. 결론

본 논문은 Gu-Xue 기법의 안전성을 분석하여 공격대상 그룹 구성원의 비밀키 정보가 한 사용자의 것이라도 노출되면 다양한 취약성을 가짐을 보였다. 특히, 이러한 문제점이 공격자를 정의함에 있어 현실적이지 않은 가정을 도입함에서 기인되었음을 밝혔다. 새로운 기법을 설계하고 안전성을 분석함에 있어 공격자 모델을 올바르게 정의하는 것은 매우 중요한 문제임을 상기하게 하는 결과이다.

참고문헌

〔1〕 D. Balfanz, G. Durfee, N. Shankar, D.K. Smetters, J. Staddon, and H.C. Wong, ``Secret handshakes from pairing-based key agreements,'' Proceedings of 2003 IEEE Symposium on Security and Privacy, pp. 180-196, May 2003.

〔2〕 J. Gu and Z. Xue, "An Improved Efficient Secret Handshakes Scheme with Unlinkability," IEEE Communications Letters, vol. 15, no. 2, pp. 259-261, Feb. 2011.

〔3〕 H. Huang and Z. Cao, "A Novel and Efficient Unlinkable Secret Handshakes Scheme," IEEE Communications Letters, vol. 13, no. 5, pp. 363-365, May 2009.

〔4〕 S. Jarecki, J. Kim, and G. Tsudik, "Beyond secret handshakes: affiliation-hiding authenticated key exchange," Proceedings of CT-RSA'08, LNCS 4964, pp. 352-369, 2008.

〔5〕 S. Jarecki and X. Liu, "Unlinkable secret handshakes and key-privacy in group key management scheme," Proceedings of ACNS'07, LNCS 4521, pp. 270-287, 2007.

〔6〕 R. Su, "On the security of a novel and efficient unlinkable secret handshakes scheme," IEEE Communications Letters, vol. 13, no. 9, pp. 712-713, Sep. 2009.

〔7〕 T.-Y. Youn and Y.-H. Park, "Security analysis of an unlinkable secret handshakes scheme," IEEE Communications Letters, vol. 14, no. 1, pp. 4-5, Jan. 2010.

〈著者紹介〉

윤 택 영 (Taek-Young Youn) 종신회원
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

박 영 호 (Young-Ho Park) 종신회원
1990년 2월: 고려대학교 수학과 학사
1993년 2월: 고려대학교 수학과 석사
1997년 2월: 고려대학교 수학과 박사
2002년 3월~현재: 세종사이버대학교 부교수
〈관심분야〉 암호알고리즘, 정보보호 프로토콜, 부채널공격, 암호구현