Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.609

해시 기반 인증자 안전성 고찰

변 진 욱†‡
평택대학교 정보통신학과

A Brief Consideration on the Security of Hash-Based Authenticator

Jin Wook Byun†‡
Pyeongtaek University, Department of Information and Communication

요 약

인증된 키 교환 프로토콜에서 두 참여자는 주고받은 공통된 값과 공통의 세션 키를 이용하여 해시 기반 인증자(hash-based authenticator)를 만들고 이를 통해 참여자들의 인증을 유도한다. 본 짧은 논문에서는 이러한 해시 기반 인증자의 입력을 부주의하게 설계하면 전체적인 프로토콜의 안전성을 보장하지 않을 수 있음을, Tsai 기타 등등이 2013년에 제안한 프로토콜을 통해, 보인다.

ABSTRACT

Authenticated key exchange protocol achieves its authentication by using hash-based authenticator with input of common message and session key that agrees between participants. In the letter, we show that this approach cannot satisfy the entire security, through a recent example protocol that is proposed by Tsai et al, 2014, if the input of authenticator has been insecurely designed.

Keywords: Authenticator, Authenticated Key Exchange, Security Analysis

I. 서 론

인증된 키 교환 프로토콜에서 참여자들의 인증을 유도할 때 일방향 해시함수를 적용한 인증자 값을 이용한다. 또한 참여자들 사이에 주고받은 메시지, 공통의 세션 키들이 인증자의 입력으로 주로 활용된다. 인증자의 입력 값들이 구체적으로 어떻게 구성되느냐에 따라 전체적인 프로토콜이 안전할 수 있고 안전하지 않을 수 있다. 본 짧은 논문에서는 일방향 해시기반의 인증자의 입력 값이 부주의하게 잘못 설계되면 전체적인 프로토콜이 안전하지 않을 수 있음을 보인다. 이를 위해 최근에 유명 저널에 소개된 Tsai 등이 제안한 프로토콜 (TLW 프로토콜[2]) 을 하나의 반면교사로 삼고 해시 기반 인증자 설계의 중요성 및 그 안전성 영향에 대해 고찰해보려 한다.

Received(03. 31. 2016), Modified(06. 10. 2016), Accepted(06. 10. 2016)
† 주저자, jwbyun@ptu.ac.kr
‡ 교신저자, jwbyun@ptu.ac.kr(Corresponding author)

II. 안전성 모델 및 정의

BPR[1] 모델을 기반으로 하여 설계된 TLW 프로토콜의[2] 안전성 모델은 다음과 같다. 먼저 두 개의 참여자, U와 S가 존재하고 t번째 세션을 U^t, S^t로 각각 정의한다. 참고문헌 [2]에 정의된 공격자 A의 질의 능력 및 안전성 관련 정의를 간략히 요약하여 정리하면 다음과 같다.

- Send(U^t,m): A가 메시지 m을 U^t에게 보내는 것을 모델링한 것으로, 답변으로 U^t가 보낼 다음 메시지를 출력한다.
- Reveal(U^t): U^t가 세션 키를 만들었다면 그 세션 키를 출력하여 반환한다.
- Corrupt(U,a): a가 1이라면 사용자 U의 패스

워드를 출력하여 반환하고 2라면 서버 S의 롱텀 키 값을 반환한다.

- Execute(U^t,S^j): U^t,S^j사이의 교환된 메시지들 값을 출력한다.
- Test(U^t): A의 세션 키 이점을 측정하기 위한 질의로, 동전 던지기를 통해 랜덤 비트 b값을 정한다. $b=1$이면 실제 키를 출력하고 $b=0$이면 랜덤 키를 출력한다.

공격자 A는 위에서 정의한 질의를 통해 다항식 시간 T 동안 인증된 키 교환 프로토콜을 수행한다고 가정하자. 건전한(freshness) 세션에 대해 Test 질의를 수행하면 답변으로 키 값을 얻게 되고, 이에 대해 실제 키인지 랜덤 키인지 구별하는 의미에서 b 값에 대한 추측 값 b'을 추측한다. 세션 키 이점은 아래와 같이 정의된다.

$$Adv_{sk}^{ake}(A,T,k)=2\Pr[b=b']-1$$

다항식 공격자 A에 대해 세션 키 이점이 무시할 수 있는 확률로 작을 때 키 교환 프로토콜 P가 안전하다고 정의한다. 건전한 세션이란 같은 세션 키를 형성한 U^t,S^t에 대해 Reveal질의가 허용되지 않아야 하고 공격자에 의해 Corrupt 질의가 발생되더라도 그 후 Send(U^t,m), Send(S^t,m) 질의가 없어야 한다.

III. Tsai 등의 프로토콜 및 안전성 분석

먼저 타원형 곡선 E가 큰 소수 p에 대한 Z_p 위에서 정의된다. 생성자 P에 대해 서버의 공개키는 $P_s=xP$이고 개인키는 x이다. h,h_1은 일방향 해시 함수이다. 인증의 중요부분인 로그인 단계에 대해서 동작과정을 Fig. 1에 나타내었다.

3.1 등록단계

- 1단계: 사용자 U_i는 본인의 아이디, 패스워드, 생체정보, (ID_i,pw_i,f_i)를 입력한다. 랜덤한 r에 대해 $h(pw_i\|r\|f_i)$가 계산되고 ID_i와 $H=h(pw_i\|b\|f_i)$가 서버 S에게 전달된다.
- 2단계: H,ID_i를 받은 S는 개인키 x를 활용하여 $V=h(ID_i\|x)\oplus H$를 계산 후 U_i에게 전달한다.
- 3단계: U_i의 스마트카드에 {V,b}가 안전하게 저장된다.

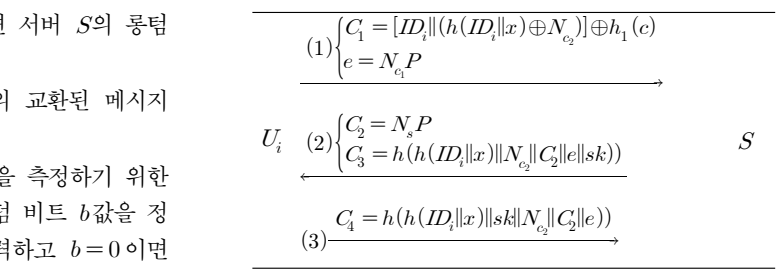

Fig. 1. The login authentication process of TLW protocol

3.2 로그인 단계

- 1단계: U_i는 자신의 ID_i,pw_i,f_i를 입력한다. U_i는 자신의 스마트카드에 V,b를 가지고 있으므로 V와 $H=h(pw_i\|b\|f_i)$를 배타적 결합하여 $h(ID_i\|x)$ 값을 복원하고 랜덤한 N_{c_1}을 선택하여 $e=N_{c_1}P$, $c=N_{c_1}P_s$를 계산한다. 그 후 랜덤한 N_{c_2}값을 선택하여 $C_1=[ID_i\|h(ID_i\|x)\oplus N_{c_2})]\oplus h_1(c)$를 계산하여 S에게 (C_1,e)를 전달한다.
- 2단계: (C_1,e)를 받은 S는 자신의 개인키 x를 이용하여 $h_1(xe)=h_1(c)$를 만든 후 C_1과 배타적 결합하여 $ID_i\|h(ID_i\|x)\oplus N_{c_2}$를 복원한다. S는 고정된 길이의 ID_i를 파악 후 제거하고, $h(ID_i\|x)$를 배타적 결합하여 N_{c_2}값을 복원한다. S는 $C_2=N_sP$를 계산하고 공통의 키 $sk=h(e,C_2,N_sN_{c_1}P)$를 형성한다. 그 후 $C_3=h(h(ID_i\|x)\|N_{c_2}\|C_2\|e\|sk)$를 만들어 C_2와 함께 U_i에게 (C_2,C_3) 최종 전달한다.
- 3단계: (C_2,C_3)를 받은 후 U_i는 랜덤 값 N_{c_1}을 통해 $N_sN_{c_1}P$를 만들고 $sk=h(e,C_2,N_sN_{c_1}P)$를 형성한다. 또한 $C_3'=h(h(ID_i\|x)\|N_{c_2}\|C_2\|e\|sk)$를 계산하여 받은 C_3와 비교하여 맞으면 U_i가 S를 인증하고 $C_4=h(h(ID_i\|x)\|sk\|N_{c_2}\|C_2\|e)$를 계산하여 U_i에게 전달한다. 틀리면 로그인 단계가 실패한다.
- 4단계: C_4를 받은 후 S는 자신의 C_4'을 계산하고 받은 C_4와 맞는지 비교 후 U_i를 인증하고, 틀린 경우는 로그인 단계가 실패하여 프로토콜이 멈춘다.

3.3 TLW 프로토콜 안전성 분석

TLW 프로토콜은 CDH 문제에 기반하여 세션 키의 안전성이 보장됨을 증명하였다[2]. 하지만, 공격자가 자신 스스로 인증자를 교묘히 조작하여 전달한 후 프로토콜의 실패 결과를 통해 세션 키의 정보를 유추하는 악의적인 행동을 증명과정에서 간과하였다. 이로 인해 인증자가 불안전하게 설계되었음에도 불구하고 전체적인 프로토콜의 세션 키 안전성이 보장됨이 증명되는 모순된 결과를 낳았다. 아래 정리를 통해 TLW 프로토콜은 BPR 안전성 모델 관점에서 세션 키 안전성을 보장하지 않음을 보인다.

정리 1. Execute, Corrupt질의를 할 수 있는 공격자A에 대해 TLW 프로토콜의 세션 키 이점은 무시할 수 없을(non-nelgigible) 정도로 크다.

증명. 공격자 A는 안전성 정의에 허용된 모든 질의를 할 수 있다. 하지만, 공격할 해당 세션이 건전해야 하며, Corrupt질의가 끝난 후에는 Send 질의를 할 수 없고, 또한 해당 세션에 Reveal 질의도 할 수 없다. A는 Send 질의와 Reveal 질의 없이 단지 Corrupt질의와 Execute질의를 통해 세션 키 이점을 얻어 낸다.

- 먼저, $Execute$ 질의를 수행하여 U^i와 S^j로부터 발생한 메시지 $[(C_1,e),(C_2,C_3),C_4]$를 얻는다.

$$\begin{cases} C_1=[ID_i\|h(ID_i\|x)\oplus N_{c_2}]\oplus h_1(c), \quad e=N_{c_1}P \\ C_2=N_sP \\ C_3=h(h(ID_i\|x)\|N_{c_2}\|C_2\|e\|sk)) \\ C_4=h(h(ID_i\|x)\|sk\|N_{c_2}\|C_2\|e) \end{cases}$$

- A는 Corrupt 질의를 통해 x를 얻는다
- A는 x를 이용해 공개된 값 e와 함께 $h_1(xe)$를 계산하고, $C_1\oplus h_1(c)$ 연산을 통해 ID_i를 파악한 후 $h(ID_i\|x)\oplus N_{c_2}$를 끄집어 낸다. 그 후 $h(ID_i\|x)$를 배타적 결합해 결국 N_{c_2}를 유도한다.
- 세션키 이점을 측정하기 위해 Test질의를 요청하고, b가 1인 경우 실제 sk를 받게 되고, b가 0인 경우에는 랜덤 sk를 받게 된다. 받은 세션 키를 $\widetilde{sk}$라 했을 때 실제 키인지 랜덤 키인지 다음 전략을 통해 높은 확률로 알 수 있다.

▷ 1 단계: A는 이미 $h(ID_i\|x),N_{c_2},C_2,C_3,e$ 값을 Execute 질의를 통해 얻었다.

▷ 2 단계: 받은 $\widetilde{sk}$가 실제 키인지 랜덤 키인지 구분하기 위해 직접 $\widetilde{C_3}$값을 $\widetilde{sk}$를 활용하여 다음 조건식을 통해 받은 C_3와 비교하여 판단한다.

$$\begin{aligned} &If \quad \widetilde{C_3}(=h(h(ID_i\|x)N_{c_2}\|C_2\|e\|\widetilde{sk}))==C_3 \\ &\quad output \quad b'=1 \\ &Else \\ &\quad output \quad b'=0 \end{aligned}$$

A가 정확히 $b=b'$ 할 확률은 명확히 1이므로 다음의 이점을 쉽게 얻을 수 있다.

$$Adv_{p,sk}^{pake}(A,T',k)=2\Pr[b=b']-1=1$$

T_e,T_c,T_h가 각각 Execute, Corrupt, Hash 질의 시 걸리는 시간이라했을때 총 $T'\geq T+T_e+T_c+2T_h$의 시간이 소요된다. □

IV. 인증자 설계의 문제 및 대처방안

4.1 해시 인증자의 재 설계

공격자 A가 C_3에 입력되는 입력 값들을 계산하지 못하도록 CDH 문제를 입력으로 하여 아래와 같이 설계할 수 있다.

$$\begin{cases} C_3=h(h(ID_i\|x)\|N_{c_2}\|C_2\|e\|N_{c_1}N_sP\|sk) \\ C_4=h(h(ID_i\|x)\|sk\|N_{c_2}\|C_2\|e\|N_{c_1}N_sP) \end{cases}$$

정당한 참여자만이 본인이 선택한 N_{c_1},N_s값을 알 수 있고, $N_{c_1}N_sP$값을 구할 수 있으므로 A는 가능한 $p-1$개의 $\widetilde{C_3}$ 중 검증 가능한 $\widetilde{C_3}$를 선택할 수 없게된다. 그러므로 정리 1의 2단계의 조건식을 통해 주어진 $\widetilde{sk}$값이 실제인지 랜덤인지 확인할 수 없다.

4.2 안전한 인증자 컴파일러 적용

CDH의 인증자에 CDH 값을 입력으로 하지 않고 인증자를 안전하게 재설계 할 수도 있다. Bellare 등은 형성된 세션 키를 바탕으로 안전하게 인증자를 설계하여 인증된 키 교환으로 만드는 해시함수 기반 인증자 컴파일러를 설계하였다[1]. 주된 아이디어는 먼저 공통의 키 sk'를 만들고 이 키를 기반으로 하여 인증자 $h_1=h(sk'\|1)$과 $h_2=h(sk'\|2)$를 교환하여 상호 인증을 수행한다. 세션 키 sk는 h_1,h_2와 공통의 키 sk'와 독립적으로 $sk=h(sk'\|0)$를 형성한다. 여기서 h는 랜덤오라클이며 입력 값이 틀리면 랜덤

하게 뽑힌 값으로 출력 값이 시뮬레이션 되므로 충돌 확률을 제외한다면 h는 독립적인 출력 값을 가진다. 안전하게 C_3, C_4, sk, sk' 를 설계하면 다음과 같다.

$$\begin{cases} C_3 = h(sk' \| 1) \\ C_4 = h(sk' \| 2) \\ sk = h(sk' \| 0) \\ sk' = h(e, C_2, N_{c_2} N_s P) \end{cases}$$

무엇보다도 CDH 문제에 기반한 $N_{c_2} N_s P$값을 계산할 수 없으므로 sk'를 만들 수 없다. 이로 인해 정리 1의 2단계의 조건식을 통해 주어진 $\widetilde{sk}$값이 실제인지 랜덤인지 확인할 수 없다.

4.3 세션의 건전함의 재 정의

세션의 건전성에 대해서 공격자 A가 Corrupt 질의를 원천적으로 못하는 것으로 재정의 한다면 위에서 언급한 공격을 쉽게 막을 수 있다고 반론을 재기할 수 있다. 하지만, 이는 안전성 모델을 약화시킬 뿐 아니라, 더 나아가 전방향 안전성을 전혀 보장할 수 없는 프로토콜이 설계된다. 무엇보다 Corrupt질의를 포기해서는 안 되는 가장 큰 이유는, TLW 프로토콜이 다중 인증요소(예:패스워드, 비밀키, 생체인식)를 기반으로 하는 프로토콜이므로 Corrupt질의가 반드시 정의되고 공격자에게 허용되어야 한다는 점이다. 이로인해 TLW 프로토콜이 제안된 참고문헌 [2]에서도 저자 스스로 사용자 및 서버를 대상으로 Corrupt 질의를 허용하고 있다는 사실에 주목해야 한다. 그럼에도 불구하고 프로토콜의 수정이 전혀 불가능한 상황이고 또한 공격자의 능력을 제약할 수 있는 상황이라면, 약화된 모델 하에서 TLW 프로토콜이 안전함을 보일 수 있는 것은 자명하다.

V. 결론 및 교훈

본 짧은 논문에서는 부주의한 인증자 설계가 전체 프로토콜의 안전성을 무너뜨릴 수 있음을, Tsai 등이 제안한 프로토콜을 통해 살펴보았다. Tsai 등이 제안한 프로토콜은 BPR 모델을 기반으로 저자들에 의해 안전성이 증명되었지만, 잘못 설계된 인증자를 이용한 검증 공격 행위를 고려하지 않음으로 인해, 증명 결과가 옳지 않음이 본 논문을 통해 확인되었다. 또한 TLW 프로토콜에 적합한 안전한 인증자를 설계하는 방안도 함께 제시되었다. TLW 프로토콜은 현재까지 약 27번 정도의 인용을 보이지만, 현재까지 안전성 증명에 대한 오류가 지적되지 않은 상태이며, 본 논문에서는 이러한 오류를 지적하고 인증자 설계의 중요성을 다시한번 부각시키려 하였다. 키 교환 프로토콜의 세션 키는 항상 랜덤하게 설계되어야하며, 프로토콜의 인증자 값과도 항상 독립적이어야 한다. 일반적으로 랜덤 오라클모델로 인증자 및 세션 키를 설계하면 이를 쉽게 달성할 수 있다. 하지만 랜덤오라클로 설계된 인증자라 할지라도 인증자의 입력 값 중에는 공격자가 계산하여 얻지 못하는 값이 반드시 포함되어야한다. 본 논문에서는 인증자 공격을 통해 이러한 교훈들을 다시 발견하고 상기시켰다.

References

[1] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," Proceedings of Eurocrypt'00, LNCS 1807, pp. 139-155, 2000.

[2] Jia-Lun Tsai, Nai-Wei Lo, and Txong-Chen Wu, "Novel Anonymous Authentication Scheme Using Smart Cards," IEEE Transaction on Industrial Informatics vol. 9 Issue 4, pp. 2004-2013, Nov. 2013.

〈저 자 소 개〉

변 진 욱 (Jin Wook Byun) 종신회원
2001년 2월: 고려대학교 전산학과 이학사
2003년 2월: 고려대학교 정보보호대학원 정보보호 전공, 공학 석사
2006년 8월: 고려대학교 정보보호대학원 정보보호 전공, 공학 박사
2006년 11월~2007년 12월: 영국 런던대학교, ISG 박사후 연수
2008년 03월~현재: 평택대학교 정보통신학과 부교수
〈관심분야〉 사용자 인증, 프라이버시 보호 기술, 데이터베이스 보안, 암호 프로토콜