약한 키를 가지는 대화식 영지식 증명의 안전성 강화 방법

양 대 헌

ETRI, 정보보호연구본부

A Method to Enhance the Security of ZKIP with Weak Keys

DaeHun Nyang

Information Security Technology Division, ETRI

요 약

본 논문에서는 약한 키를 가지는 대화식 영지식 증명을 이용한 인증 프로토콜의 안전성을 강화하는 방법을 제시한다. 일반적으로 대화식 영지식 증명을 이용한 인증 프로토콜은 충분히 길고 랜덤한 비밀키를 가정하고 그 비밀키에 대한 영지식 증명을 수행하게 된다. 하지만 때에 따라서 충분히 길지 않거나 랜덤하지 않은 비밀키가 선택될 수 있다. 즉, 좋지 않은 난수 발생기를 써야 하는 경우, 또는 패스워드처럼 의도적으로 약한 키를 사용하는 경우가 생기며, 대화식 영지식 증명은 이에 적합하지 않다고 알려져 있다. 본 논문에서는 비밀 동전 던지기(Secret Coin Tossing)라는 개념을 제시해서, 일반적인 영지식 증명을 이용한 인증 프로토콜을 약한 키를 가지는 영지식 증명 기반 인증 프로토콜로 쉽게 변환할 수 있는 프레임웍을 제안한다. 또한, 이 프레임웍을 이용해서 설계된 인증 프로토콜이 ideal cipher model에서 안전함을 보인다.

I. 서론

대화식 영지식 증명은 암호학에서 가장 유용한 툴 중의 하나가 되었고, 수 많은 암호 프로토콜들이 대화식 영지식 증명에 기초하고 있다. 대화식 영지식 증명이 가장 유용하게 쓰이는 분야중의 하나가 인증 프로토콜 분야인데, 많은 좋은 프로토콜들이 제안되어왔다[2][3][4].

대화식 영지식 증명에서 증명하려는(동시에 아무 지식도 노출시키지 않으려는) 비밀은 예외 없이 길고 랜덤한 수이어야 하며, 이는 대화식 영지식 증명의 광범위한 사용을 제한한다. 즉, 아무리 잘 설계된 대화식 영지식 증명 프로토콜이라 하더라도 그것이 증명하고 있는 비밀의 랜덤성과 충분한 길이가 보장되지 않는다면 오프라인 사전 공격(Offline Dictionary Attack or Guessing Attack)에 쉽게 깨질(is broken) 수 있다. 이 논문에서는 일반적인 대화식 영지식 증명에 기반한 인증 프로토콜에 약한 키가(weak key)가 사용되는 경우 어떻게 이런 오프라인 사전 공격이 가능한지에 대해 알아보고, 이들을 체계적으로 막을 수 있는 프레임웍을 제시한다. 약한 키를 가지는 대화식 영지식 증명의 안전한 사용을 위해서 비밀 동전 던지기(Secret coin tossing)이라는 개념을 제안하고, 이를 수용한 특별한 형태의 영지식 증명에 기반한 인증 프로토콜 프레임웍을 보인다. 또한 이 프레임웍을 적용할 수 있는 재미있는 응용분야의 하나인 패스워드에 기초한 인증 및 키 교환 프로토콜로의 적용에 대해서도 살펴본다.

이 프레임웍을 이용해서 기존의 또는 앞으로 발표될 좋은 특징을 가지는 대화식 영지식 증명 프로토콜을 쉽게 패스워드를 이용한 인증 및 키 교환 프로토콜로 변환할 수 있다. 또한 약한 키를 가지는 대화식 영지식 증명 프로토콜을 안전하게 사용할 수 있다.

II. 영지식 증명과 약한 키

만약 대화식 영지식 증명이 증명하고 있는 비밀 지식이 작은 집합에서 선택되었고, 랜덤하지 않거나 충분히 길지 않다면, 공격자는 쉽게 공개키(또는 패스워드 확인자)를 참조 삼아(as a reference) 오프라인 사전 공격을 수행할 수 있다. 이 trivial

한 공격은 패스워드 확인자나 공개키를 서버의 안전한 저장소에 저장해 놓으므로써 쉽게 막을 수 있다. 하지만, 공개키 또는 패스워드 확인자가 사용자와 서버에게만 알려져있다 하더라도, 공격자는 둘 사이의 대화(transcript)를 보고서 오프라인 사전 공격을 수행할 수 있다. 원래의 대화형 영지식 증명 프로토콜이 soundness, completeness, simulatability를 만족한다면, 약한키 S를 사용하는 경우에도 안전한 것처럼 보인다. 하지만, 공격자는 시험수 A 질문수 c 그리고 목격자수 B를 이용해서 쉽게 S에 사전공격을 수행할 수 있다. 좀더 명확히 말하면, B와 A를 이용하면 c로 마스킹된 공개키값을 얻을 수 있고, 알려진 정보 A, B, c를 이용해서 공개키를 추측하므로써 사전공격을 수행할 수 있게된다. 이는 질문 수 c가 공격자에게 노출되어있기 때문인데, 전통적인 대화형 영지식 증명에서는 공개키에 해당하는 비밀키가 충분히 길고 랜덤하므로 사전공격을 수행할 수 없다.

설명을 위해서 Guillous-Quisquater의 프로토콜이 약한 키를 가지는 경우 어떻게 오프라인 사전공격이 이루어지는지 살펴보자. 우선 Guillous-Quisquater의 프로토콜은 다음과 같이 요약할 수 있다.

a. 사용자→서버: $x \equiv r^e \bmod n, r \in_R Z_n^*$
b. 서버→사용자: c, c는 $1 < c < e$ 인 랜덤수
c. 사용자→서버: $y \equiv r * f(S)^c \bmod n$
d. 서버: $x \equiv V^c * y^e \bmod n$를확인,
여기서 $V \equiv f(S)^{-e}$

V는 사용자의 공개키, n은 RSA modulus이다. 위의 프로토콜은 트랜스크립트 (x,c,y)를 가지며 이를 이용해서 누구나 다음과 같이 오프라인 사전공격을 수행할 수 있다.

Procedure DictionaryAttackGQ()
Input: (x,c,y,e,n)
Return value: Guessed password
BEGIN
For each guessed secret S′ in her dictionary do
if $x/y^e \equiv V'^c \bmod n$, 여기서 $V' \equiv f(S')^{-e} \bmod n$
then return S′
Endfor
return FAIL
END

즉, 공개키 또는 패스워드 확인자 V가 서버에 안전하게 보관된다 하더라도 위의 프로토콜은 약한 키를 가지는 경우 안전하지 않다. 지면의 제약상, 다른 프로토콜들에 대한 공격방법은 생략하지만, Schnorr의 프로토콜, Feige-Fiat-Shamir의 프로토콜 등에도 위의 공격이 가능하다.

III. 비밀 동전 던지기

앞서 언급한 약점은 비밀 동전 던지기(Secret Coin Tossing)라는 개념을 이용해서 극복할 수 있다. II장의 추측공격이 가능한 주요한 이유는 마스킹된 공개키 또는 마스킹된 패스워드 확인자가(비록 마스킹된 채로 노출되기는 하지만) 노출된다는 것이다. 따라서 만약 이것을 노출시키지 않는다면 오프라인 사전공격을 막을 수 있다.

일반적인 대화식 영지식 증명 프로토콜에 기반한 인증 프로토콜이 공개된 동전 던지기를 하는 것은 앞서 살펴본 바와같이 증명하고자 하는 비밀수의 랜덤성과 충분한 길이에 안전성을 두고 있다. 약한 키를 가지는 대화형 영지식 증명 프로토콜의 설계를 위해서 비밀 동전 던지기라는 개념을 제시한다. 비밀 동전 던지기는 대화하는 두 주체만 동전 던지기의 결과를 알 수 있고, 그 이외에는 결과를 알 수 없는 시행이다. 따라서, 대화식 영지식 증명 프로토콜에서 공개된 동전 던지기를 하는 대신 비밀 동전 던지기를 수행하므로써, 마스킹된 패스워드 확인자나 마스킹된 공개키가 노출되는 것을 막을 수 있다. 이렇게, 전통적인 대화식 영지식 증명의 공개된 동전 던지기 부분을 비밀 동전 던지기로 대체하므로써 약한 키에 대한 영지식 증명을 원래의 프로토콜이 가지는 좋은 성질(completeness, soundness, simulatability)을 잃지 않고 수행할 수 있게 된다.

이 프로토콜이 끝난 후, 서버는 사용자가 비밀수를 알고 있음을 높은 확률로 확신할 수 있다. 하지만, 이는 사용자가 서버의 공개키 또는 패스워드 확인자에 대한 지식을 확인 할 수 없다는 점에서 일방향성을 띤다. 전통적인 대화식 영지식 증명에서는 공개키가 엔트로피가 높은 비밀키와 대응되므로 이런 일방향성이 안전성 취약점이 되지 않지만, 약한키를 가지는 대화식 영지식 증명의 경우 안전성에 위협이 된다. 따라서 서버의 공개키 또는 패스워드 확인자에 대한 지식을 사용자가 먼저 확인하고 나서 앞서 기술한 비밀 동전 던지기를 이용한 영지식 증명을 수행하여야 한다.

비밀 동전 던지기 그리고 사용자의 공개키 또는 패스워드 확인자에 대한 서버의 지식 확인을 위해서 EKE의 변형된 형태를 사용한다. EKE는 원래 패스워드에 기초한 인증 프로토콜을 위해 설계되었고, [1]에서 그 안전성의 일부분이 처음으로 증

명되었다. 다음의 프로토콜이 이 논문에서 제안하는 인증 프로토콜 프레임웍을 위해 변형된 EKE이다. 여기서 모든 연산은 유한 순환 그룹 G = <g>에서 행해진다. 이 그룹은 $G=Z_p^*$ 이 될 수도 있고, 이 그룹의 소수차 서브그룹(prime order subgroup)일 수도 있다. 또한 타원 곡선 그룹이 될 수도 있다. 표기는 multiplicative group 표기를 사용하겠다.

- 변형된 EKE

a. 사용자가 서버에게 자신의 ID와 $X=V(g^x)(x\in_R G)$를 보낸다. $V(x)(V^{-1}(x))$는 x 를 키 V로 대칭키 암호(복호)화 하는 것을 의미한다.

b. 서버는 $y\in_R G$ 를 선택하고, 다음을 계산해서 $(auth=H(K'||1), Y)$ 를 사용자에게 보낸다.

$$K\equiv[V^{-1}(X)]^y, Y=V(g^y)$$
$$K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$$

여기서 K는 임시 세션키를 생성하는데, Y는 키 교환을 위해, 그리고 K'은 K의 유효성을 검증하는데 사용된다.

c. 사용자는 다음을 계산해서 $H(K'||1)=auth$ 인지 확인한다. 만약 성공한다면, 사용자는 서버가 V를 알고 있음을 확신할 수 있다. $K\equiv[V^{-1}(Y)]^x, K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$

d. 프로토콜이 성공적으로 끝난다면, 사용자와 서버 모두 임시 세션키 $TSK=H(K'||0)$을 갖게 된다.

위의 프로토콜은 [1]의 "AddSCA(EKE2)"를 패스워드 대신 패스워드 확인자 또는 공개키에 대한 인증으로 변형한 것이다. 따라서 위의 프로토콜도 패스워드 확인자에 대한 인증에 대해서 ideal cipher 모델에서 안전하다. 이에 대한 증명을 [1]를 참고하라.

IV. 새로운 인증 프로토콜 프레임웍

이 장에서는 비밀 동전 던지기를 이용해서 일반적인 대화식 영지식 증명 프로토콜이 약한 키를 가지는 경우에도 안전하게 사용할 수 있는 프레임웍을 설계한다. 이 프레임웍에서 증명하려는 비밀수를 패스워드로, 공개키를 패스워드 확인자로 치환하면 이 프레임웍을 쉽게 패스워드에 기초한 인증 및 키 교환 프로토콜로 사용할 수도 있다. 이 프레임웍은 ideal cipher 모델에서 오프라인 사전 공격에 안전하다.

제안하는 프레임웍은 크게 III장의 변형된 EKE와 비밀동전던지기를 하는 대화식 영지식 증명의 두 부분으로 이루어져있다. 여기서 쓰이는 H()와 h()는 모두 일방향 해쉬함수이며, 특히 h()는 해쉬값의 상위 k 비트만을 돌려준다(k는 계산효율과 보안강도의 trade-off의 정도가 된다).

- 시스템 설정:

사용자의 공개키 또는 패스워드 확인자 V = OWF(f(S))는 서버에 비밀리에 보관된다. 여기서 S는 약한 키, f()는 S를 충분한 길이로 늘려주는 함수, OWF는 각 대화식 영지식 증명에서 사용되는 일방향 함수를 의미한다. f()가 충돌회피성, 강 또는 약 일방향성 등의 암호학적 성질을 가질 필요는 없지만, 잘 알려져있는 일방향 해쉬함수를 사용할 수 있다.

- 인증:

a. 변형된 EKE를 수행한다.

a.1 사용자는 x를 임의로 선택해서 시험수 $A=OWF(r)$와 함께 $ID_{User}, X=V(g^x)$를 서버에 전송한다. 여기서 $x\in_R G$.

a.2 서버는 $y\in_R G$를 이용해서 다음을 계산하고 $(auth=H(K'||1), Y)$를 사용자에게 전송한다.

$$K\equiv[V^{-1}(X)]^y, Y=V(G^y)$$
$$K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$$

a.3 사용자는 다음을 계산해서 $H(K'||1)=auth$ 인지 확인한다. 맞는다면 서버가 V 를 알고있다고 확신할 수 있다. $K\equiv[V^{-1}(Y)]^x, K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$

a.4 이 변형된 EKE가 성공적으로 끝나면, 각각은 공유하는 비밀키 $TSK=H(K'||0)$. 아니라면 프로토콜 수행을 중단한다.

b. 사용자는 목격자수 B를 c, r 그리고 자신이 가지고 있는 비밀수 S를 이용해서 서버에게 보낸다. 여기서 $c=h(TSK||A)$이고 c의 길이는 안전강도와 계산효율성의 trade-off파라미터가 된다.

c. 서버는 $c=H(TSK||A)$를 계산하고 사용자의 목격자수를 A, V, c를 이용해서 검증한다. 성공하면 사용자 인증이 완료된다.

d. 프로토콜 종료 후, 교환된 키는 다음과 같다.

$$SK = H(K' \| A \| B \| 2)$$

여기서 시험수 A가 영지식 증명 부분이 아닌 변형된 EKE 부분에서 전송됨을 주목해 보면, 사용자가 시험수를 결정할 당시에는 질문수 c를 전혀 예측할 수 없음을 알 수 있다. 이 불예측성은 서버가 랜덤하게 질문수를 선택해서 사용자에게 전송하는 것과 같은 효과를 가진다.

V. 안전성 증명

이 논문에서 제안한 인증 프레임웍으로 만들어진 프로토콜에 대한 오프라인 사전공격의 가능성을 평가하는데는 [1]에서 소개된 adversary 모델을 사용한다. 여기서는 중요한 표기법을 간략하게 소개한다. 자세한 내용은 [1]를 참조하기 바란다. 자세한 증명은 지면 관계상 생략한다. 공격자(adversary) A는 서버 또는 클라이언트 오라클 ($\Pi_U^i, U \in \{Client, Server\}, i \in N, \ 1 \le N \le \sqrt{|G|}/q$) 에 다음과 같은 여섯 가지 타입의 질의를 수행할 수 있다: Send(U, I, M), Reveal(U,i), Corrupt(U, pw), Execute(A,i,B,j), Test(U, i), Oracle(M). 여기서 $q_{se}, q_{re}, q_{co}, q_{ex}, q_{or}$ 은 각각 Send, Reveal, Corrupt, Execute, Oracle 질의의 수를 의미한다. 또한, t는 공격자의 수행시간을 뜻한다.

정리1: 공격자는 ideal cipher 모델에서 앞서 제시한 프레임웍으로 생성된 변형된 GQ 프로토콜에 대해 오프라인 사전공격을 다음의 확률보다 더 높은 확률로 성공할 수 없다.

$$Adv_{P,PW,SK}^{ake-fs} \le \frac{q_{se}}{N} + q_{se} q_{or} \, Adv_{G,g}^{dh}(t', q_{or}) + \frac{O(q^2)}{|G|} + \frac{O(1)}{\sqrt{|G|}}$$

여기서 $t' = t + O(q_{se} + q_{or}), \ q = q_{se} + q_{re} + q_{co} + q_{ex} + q_{or}$.

증명 스케치: 알고리즘 A* 가 변형된 GQ 프로토콜에 대해서 오프라인 사전 공격을 $Adv_{P,PW,SK}^{ake-fs}$ 보다 큰 확률로 수행할 수 있다고 가정하자. 변형된 GQ 프로토콜을 GQ*이라하고, [1]에서 AddSCA (EKE2)가 안전함이 증명되었다는 사실을 이용한다. 만약 $Adv_{P,PW,SK}^{ake-fs}$보다 큰 확률로 GQ*에 사전공격을 할 수 있는 A*가 존재한다면 AddSCA (EKE2)를 $Adv_{P,PW,SK}^{ake-fs}$보다 높은 확률로 공격할 수 있는 알고리즘 A+가 존재함을 보인다. [1]에서 AddSCA(EKE2)는 $Adv_{P,PW,SK}^{ake-fs}$보다 높은 확률로 공격당할 수 없음을 증명했으므로, 모순을 이끌어 낼 수 있다. ■

VI. 결론

대화식 영지식 증명은 충분히 길고 랜덤한 비밀수를 보호하는 인증 프로토콜을 설계하는데 매우 강력한 도구이지만, 약한 키를 보호하는데 응용하는 방법에 대해서는 많은 연구가 이루어지지 않았다. 따라서 약한 키를 보호하는데 사용하는 프로토콜들은 주로 ad hoc 설계에 의존해 왔다. 이 논문에서는 어떤 영지식 증명을 약한 키를 증명하는데 사용할 수 있는 체계적인 방법을 프레임웍 형태로 제시하였다. 이렇게 하므로써, 약한키를 쓸 수밖에 없는 환경에서도 영지식 증명을 이용해서 인증을 하거나 키 교환을 할 수 있게 되었다. 특히 유용한 분야로 패스워드를 이용한 인증과 키 교환 프로토콜 설계가 있는데, 적당한 대화형 영지식 증명 프로토콜을 쉽게 패스워드에 기초한 인증 및 교환 프로토콜로 변환할 수 있다.

참고문헌

[1] M. Bellare, D. Pointcheval and P. Rogaway, Authenticated key exchange secure against dictionary attacks, Proceedings of EuroCrypt 2000,Lecture Notes in Computer Science, Springer-Verlag, 2000, pp. 139-155.

[2] U. Feige, A. Fiat and A. Shamir, Zero-knowledge proofs of identity, Journal of Cryptology, Vol. 1, No. 2, 1988, pp. 77-94.

[3] L.C. Guillou and J.J. Quisquater, Protocol fitted to security microprocessor minimizing both transmission and memory, Proceedings of EuroCrypt 88,Lecture Notes in Computer Science, Springer-Verlag, 1988, pp. 123-128.

[4] C.P. Schnorr, Efficient Identification and Signatures for Smart cards, Advances in Cryptology : Proceedings of Crypto 89, Lecture Notes in Computer Science, Springer-Verlag, New York, 1989, pp. 239 251.