Keystroke Dynamics를 위한 안전한 패스워드 인증기법의 보안 분석*

송현수, 권태경

세종대학교 정보보호연구실

*Security Analysis of Secure Password Authentication for Keystroke Dynamics**

Hyun-Soo Song, Taekyoung Kwon

Information Security Lab, Sejong University.

요 약

오늘날 패스워드 인증과 키 분배는 컴퓨터 환경에서 중요하다. 패스워드 기반의 시스템은 패스워드를 사용자가 기억하기 쉽다는 장점 때문에 널리 사용 되고 있다. 하지만, 패스워드는 작은 공간에서 선택되어지기 때문에 패스워드 추측 공격을 포함한 다양한 공격에 취약점을 나타낸다. 본 논문에서는 최근에 제안된 새로운 패스워드 인증 기법을 분석하고, 서버 위장 공격, 서버 속임 공격과 패스워드 추측 공격에 취약하다는 것을 보인다. 또한, 패스워드 기반의 기법을 설계할 때는 주의해야 한다는 점에 대해 논하고, IEEE 1363.2와 같은 표준을 사용해 CK 프로토콜을 강하게 하는 법에 대해 간단히 보인다.

I. 서론

패스워드 기반의 인증과 키 분배는 컴퓨터 환경에서 매우 중요하다. 패스워드 기법은 패스워드가 작은 공간에서 선택되어 지기 때문에 여러 공격들에 취약하다[1].

검증자 기반의 프로토콜은 패스워드가 사용자에 의해 유지되고 서버에 의해서 검증되기 때문에 비대칭 모델에서 서버 손상 공격에 대해 안전하다. 이러한 프로토콜들은 공통 세션키를 생성하고 세션키에 대한 키 검증 과정을 수행한다. A-EKE[2], B-SPEKE[7,8], SRP[12], PAK[3,10,11], AMP[9] 등이 있다.

Keystroke dynamics을 위한 안전한 인증에서[4], 효과적인 패스워드 인증 프로토콜을 제안하였다. 그들은 또한 2자간 프로토콜을 신뢰할 수 있는 서버를 통해 패스워드를 공유하는 3자간 프로토콜로 확장하였다.

우리는 CK 프로토콜의 보안 분석을 보이도록 하겠다. 이 프로토콜은 서버 위장 공격과 서버 속임 공격에 취약하다. 또한, 패스워드 추측 공격에도 약하다. 다른 말로 하면, 공격자는 오프라인 쿼리를 반복해서 합법적인 패스워드를 추측 할 수 있다[1,6]. 본 논문에서는 패스워드 기반의 기법을 설계할 때는 주의해야 한다는 점에 대해 논하고, IEEE 1363.2와 같은 표준을 사용해 기법을 강하게 하는 법에 대해 간단히 보인다.

이 논문에서는 다음의 순서를 따르고 있다. 2장에서는 CK 프로토콜의 패스워드 기반의 인증 기법을 설명하고, 3장에서는 CK 프로토콜의 보안을 분석하고 새로운 공격을 보이도록 하겠다. 4장에서는 실험을 통해 패스워드 추측 공격의 가능성을 시험 한다. 마지막으로 5장에서는 결론으로 구성된다.

* 본 연구는 서울시 산학연 협력사업의 지원에 의하여 이루어진 것임.

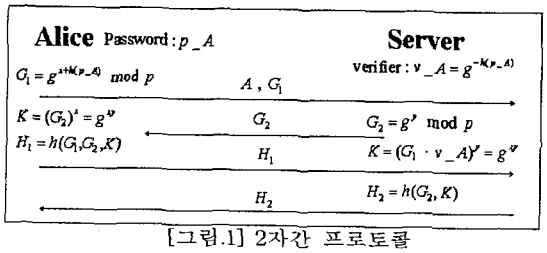
II. CK 프로토콜

p, q는 충분히 큰 소수이고 $p=2q+1$을 만족한다. 이 기법에서는 다음의 파라미터를 사용한다.

A, B	사용자의 식별자
p_A, p_B	사용자의 패스워드
v_A, v_B	패스워드를 사용하여 만든 사용자의 검증값
Z_p^*	곱셈군
g	위수가 q인 Z_p^*상의 원소
Z_q	Z_p^*의 서브그룹
x, y	랜덤값
K	세션키
$h()$	일방향 해쉬 함수

Alice 또는 Bob은 패스워드 p_A, p_B를 각각 선택한다. 그리고 서버는 패스워드를 사용해서 만든 검증 값 v_A, v_B을 저장한다.

2.1 2자간 CK 프로토콜



[그림.1] 2자간 CK 프로토콜

2자간 CK 프로토콜은 그림 1에 나타나 있고 그 과정은 다음과 같다.

Alice가 서버와 통신하고 할 때,

가. Alice는 랜덤값 $x \in_R Z_q$을 선택한 후, G_1을 계산하여 서버에게 G_1과 A를 보낸다.

나. 서버는 Alice의 요청을 받은 후에 랜덤값 $y \in_R Z_q$를 선택하여 G_2를 Alice에게 보낸다.

다. Alice와 서버는 x, y를 사용해 공통의 세션키를 계산한다.

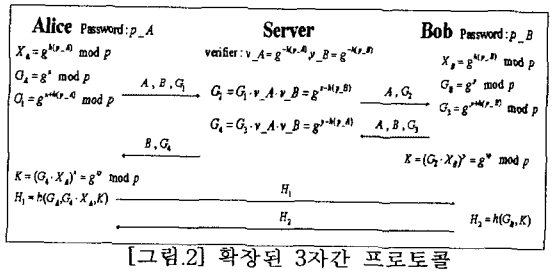
라. Alice는 H_1을 계산하여 서버에게 보낸다.

라. 서버는 $h(G_1, G_2, K)$를 계산한 후 H_1과 비교하여 검증한다.

마. 서버는 H_2를 계산하여 Alice에게 보낸다.

바. Alice는 $h(G_2, K)$를 계산한 후 H_2와 비교하여 검증 한다. 이 과정을 성공할 경우, Alice는 서버와의 공통의 세션 키를 수락한다.

2.2 3자간 CK 프로토콜



[그림.2] 확장된 3자간 프로토콜

CK 프로토콜은 3자간 프로토콜로 확장가능하다. 3자간 프로토콜은 그림 2에 나타나 있고 그 과정은 다음과 같다.

Alice가 Bob과 통신하자고 할 때,

가. Alice는 자신의 패스워드를 사용하여 X_A를 계산한다. 랜덤값 x를 선택하여 G_1을 계산한 후 서버에게 A, B, G_1을 보낸다.

나. 서버는 Alice의 요청을 받은 후에 G_2를 계산하여 A, G_2를 Bob에게 보낸다.

다. Bob은 X_B를 계산한 후 랜덤값 y를 선택하여 G_3을 계산한다. 서버의 요청을 받은 Bob은 서버에게 A, B, G_3를 보낸다.

라. Bob은 공통의 세션키 K를 계산한다.

마. 서버는 G_4를 계산하여 Alice에게 B, G_4를 보낸다.

바. Alice는 공통의 세션키 K와 H_1을 계산한 후에 Bob에게 H_1을 보낸다.

사. Bob은 $h(G_A, G_B, K)$를 계산한 후 H_1과 비교하여 검증한다.

아. Bob은 H_2를 계산한 후 Alice에게 보낸다.

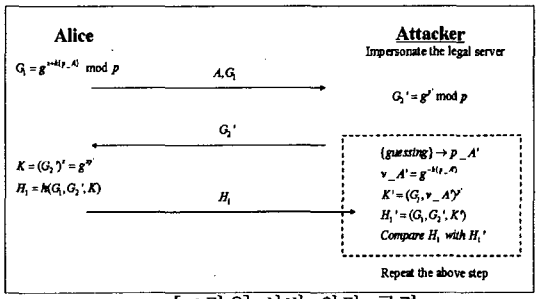
자. Alice는 $h(G_4, X_A, K)$계산한 후 H_2와 비

교하여 검증 한다. 이 과정을 성공할 경우, Alice와 Bob은 공통의 세션키를 수락한다.

III. CK 프로토콜의 보안 분석

이번 장에서는 앞에서 보았던 2자간 프로토콜과 3자간 프로토콜에 대한 새로운 공격 방법을 보인다.

3.1 2자간 프로토콜에 대한 서버 위장 공격



[그림.3] 서버 위장 공격

2자간 프로토콜에서 서버 위장 공격은 그림 3에 나타나 있고 그 과정은 다음과 같다.

1. 공격자는 서버에 DoS 공격을 해서 합법적인 서버로 위장한다.

2. 서버로 위장한 공격자는 G_1과 A를 얻는다.

3. 공격자는 랜덤값 $y' \in_R Z_q$를 선택하여 위조된 값 G_2'을 Alice에게 보낸다. Alice는 G_2'이 공격자가 보낸 것인지 서버가 보낸 것인지 알 수 없다.

4. Alice는 공통의 세션키를 계산한다. 그리고 H_1을 계산하여 공격자에게 보내준다.

5. 공격자는 패스워드 추측 공격을 통해서 Alice의 합법적인 패스워드를 찾을 수 있다.

자세한 공격 방법은 다음과 같다.

• p_A'을 패스워드 추측 값이라 하자.

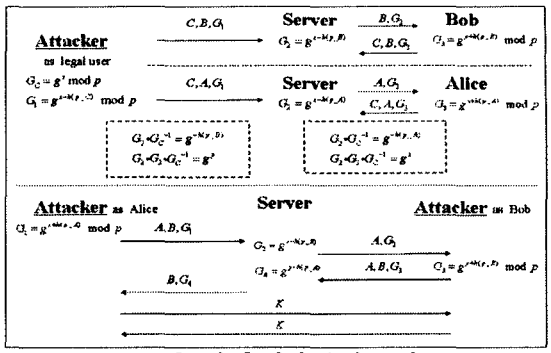
$$\{guessing\} \rightarrow p\_A'$$

• 추측한 패스워드 p_A'를 선택하여 검증값 $v_A' = g^{-h(g_A')}$을 계산한다.

• H_1과 $H_1' = (G_1, G_2', K')$을 비교한다.

• Alice의 합법적인 패스워드를 찾을 때까지 위의 과정을 반복한다.

3.2 3자간 프로토콜에서 서버 속임 공격



[그림.4] 서버 속임 공격

이 장에서는 3자간 프로토콜의 취약점을 보인다. 그림 4와 같이 3자간 프로토콜은 서버 속임 공격에 취약하다. 공격자는 다음의 과정을 수행한다.

가. 공격자는 합법적인 사용자로서 3자간 프로토콜에 참여한다.

나. 공격자는 랜덤값 z를 선택한 후, G_1을 계산하여 서버에게 G_1과 C, B를 보낸다.

다. 공격자는 서버와 Bob의 통신을 도청하여 G_2, G_3 값을 얻는다.

라. 공격자는 다음의 계산을 통해 Bob의 G_B와 검증값을 얻을 수 있다.

$$G_2 \cdot G_C^{-1} = g^{z-h(p\_B)} \cdot g^{-z} = g^{-h(p\_B)}$$

$$G_2 \cdot G_3 \cdot G_C^{-1} = g^{z-h(p\_B)} \cdot g^{y+h(p\_B)} \cdot g^{-z} = g^{y}$$

마. 공격자는 Alice의 G_A와 검증값을 얻기 위해 가-라의 Alice와 통신과정을 수행한다.

바. 공격자는 A, B, G_A, G_B, v_A, v_B를 사용해 서버를 속일 수 있다. 공격자는 Alice와 Bob으로 위장하여 서버를 통해 통신한다.(그림 4)

3.3 3자간 프로토콜에서 패스워드 추측 공격

공격자는 서버 속임 공격에서 얻어진 값을 가지고 Alice와 Bob의 합법적인 패스워드를 알아 낼 수 있다. 다른 말로 하면, 공격자는 속임 공격을 후에 오프라인 패스워드 추측 공격을 한다. 자세한 공격 과정은 다음과 같다.

• p_A'을 패스워드 추측 값이라 하자.

$$\{guessing\} \rightarrow p\_A'$$

• 추측한 패스워드 p_A'를 선택하여 검증값 $v_A' = g^{-h(g_A')}$을 계산한다.

• v_A과 p_A'을 비교한다.

• Alice와 Bob의 합법적인 패스워드를 찾을 때까지 위의 과정을 반복한다.

IV. 구현

본 논문에서는 CK 프로토콜과 패스워드 추측 공격을 구현해 보았다.

4.1 구현 환경

구현 환경은 다음과 같다.

1. 하드웨어 환경

• 노트북3대 : CPU-Intle PentiumM 1.0GHz
RAM-768MB

• 통신 채널 : 100BaseT 이더넷

2. 소프트웨어 환경

• 시스템 : 마이크로소프트 윈도우XP

• 언어 : C++(비쥬얼 스튜디오 6.0)

• 암호 라이브러리 : OpenSSL

4.2 구현 시나리오

이 실험에서는, 패스워드 공간을 2^{10}으로 제한한다. 실생활에서 사용되어지는 패스워드 공간은 2^{40}이다. 대상 패스워드는 주어진 공간에서 랜덤하게 선택 되어지는 정수로 설정한다.

가. 2자간 프로토콜 공격시나리오

공격 2자간 프로토콜에서 패스워드 추측 공격
대상 패스워드 p_A: $0 \le p\_A \le 1023$
프로토콜 시작: 그림 3 참고
ㄱ. Alice는 공격자에게 A, G_1을 보낸다.
ㄴ. 공격자는 Alice에게 G_2'을 보낸다.
ㄷ. Alice는 공격자에게 H_1을 보낸다.
오프라인 추측:
ㄹ. For i from 0 to 1023 :
ㄹ-1 $v_A' = g^{-h(g_A')}$을 계산한다.
ㄹ-2 $K' = (G_1, v_A')^{y'}$을 계산한다.
ㄹ-3 $H_1' = (G_1, G_2', K')$을 계산한다.
ㄹ-4 만약 $H_1' = H_1$이면 $i = p\_A$
ㅁ. 공격자는 p_A를 얻는다.

2^{10}의 패스워드 공간을 검색하는데 걸리는 시간은 16.047초이었고, 대상 패스워드를 찾는데 소요되는 시간의 평균은 3.343초다.

나. 3자간 프로토콜 공격시나리오

공격 3자간 프로토콜에서 패스워드 추측 공격
대상 패스워드 p_B: $0 \le p\_B \le 1023$
프로토콜 시작: 그림 4 참고
ㄱ. 공격자는 서버에게 C, B, G_1을 보낸다.
ㄴ. 서버는 Bob에게 C, G_2을 보낸다.
ㄷ. 서버는 공격자에게 G_2을 보낸다.
ㄹ. Bob은 서버에게 C, B, G_3을 보낸다.
ㅁ. 서버는 공격자에게 B, G_4을 보낸다.
ㅂ. 공격자는 Bob에게 H_1을 보낸다.
ㅅ. Bob는 공격자에게 H_2을 보낸다.
오프라인 추측:
ㅇ. $g^{-h(p_B)} = G_2 \cdot G_c^{-1}$을 계산한다.
ㅈ. For i from 0 to 1023 :
ㅈ-1 $v_B' = g^{-h(i)}$을 계산한다.
ㅈ-2 만약 $v_B' = g^{-h(p_B)}$이면 $i = p\_B$
ㅊ. 공격자는 p_B를 얻는다.

2^{10}의 패스워드 공간을 검색하는데 걸리는 시간은 3.172초이었고, 대상 패스워드를 찾는데 소요되는 시간의 평균은 1.398초다.

V. 결론

본 논문에서는 CK 프로토콜을 분석하고 서버 위장 공격, 서버 속임 공격, 패스워드 추측 공격과 같은 다양한 공격에 취약하다는 점을 보였다. 이와 같이 패스워드 기반의 기법은 패스워드 추측 공격에 합법적인 사용자의 패스워드가 공격자에 노출될 수 있기 때문에 패스워드 기반의 기법을 설계할 때는 주의해야 한다. IEEE 1363.2와 같은 표준을 사용해 기법을 강하게 할 수 있다. 이 표준은 패스워드 추측 공격을 포함한 다양한 공격에 대해 안전하고 매우 효과적인 패스워드 인증 프로토콜이다.

예를 들면, CK 프로토콜은 $G_1 = g^{x + h(p_A)} \cdot f(p_A)$을 설정함 으로서 개선 할 수 있다($f(p\_A)$: proper subgroup). 이 개선 방법은 CK 프로토콜이 우리의 공격으로부터 안전하기 위해 IEEE 1363.2를 따른다.

[참고문헌]

[1] S.Bellovin and M.Merritt, Encrypted key exchange: password-based protocols secure against dictionary attacks, In IEEE symposium on Research in Security and Privacy, pp.77-84, 1992.

[2] S. Bellovin and M. Merritt, Augmented encrypted key exchange: a password-based protocols secure against dictionary attacks and password-file compromise, In ACM Conference on Computer and Communications Security, pp. 244-250, 1993.

[3] V. Boyko, P. MacKenzie and S. Patel, Provably secure password authenticated key exchange using Diffie-Hellman, In Eurocrypt .00, pp.156-171, 2000.

[4] Y. Choe and S. Kim, Secure Password Authentication for Keystroke Dynamics, 9th International Conference on Knowledge-Based & Intelligent Information & Engineering Systems (KES 2005), LNAI 3683, pp. 317-324, 2005.

[5] W. Diffie and M. Hellman, New directions in cryptograpy, In IEEE Transactions on Information Theory, Vol. 22, no. 6, pp. 644-654, 1976.

[6] L. Gong, M. Lomas, R. Needham and J. Saltzer, Protecting Poorly Chosen Secrets from Guessing Attacks, IEEE Journal on Selected Areas in Communications, vol.11. no. 5, pp. 648-656, 1993.

[7] D. Jablon, Strong password-only authenticated key exchange, ACM Computer Communications Review, Vol. 26, no. 5, pp. 5-26, 1996.

[8] D. Jablon, Extended password key exchange protocols immune to dictionary attacks, In WETICE.97 Workshop on Enterprise Security, pp. 248-255, 1997.

[9] T. Kwon, Authentication and Key agreement via Memorable Passwords, In Network and Distributed System Security Symposium Conference Proceedings, 2001.

[10] P. MacKenzie, More Efficient Password-Authenticated Key Exchange, In CT-RSA 2001, pp. 361-377, 2001.

[11] P. MacKenzie, The PAK suites: Protocols for Password-Authenticated Key Exchange, 2002, available from http://grouper.ieee.org/groups/1363/passwdPK\contributions.html\#Ma c02.

[12] T. Wu, Secure remote password protocol, In Network and Distributed System Security Symposium Conference Proceedings, 1998.

[13] IEEE P1363.2, http://grouper.ieee.org/groups/1363/passwdPK/index.html.