해쉬함수를 이용한 안전한 일회용 패스워드 인증 스킴

윤은준*, 류은경, 유기영

*경북대학교, 컴퓨터공학과 정보보호연구실

Secure One-Time Password Authentication Scheme Using Hash Function

Eunjun Yoon*, Eunkyung Ryu, Keeyoung Yoo

*Dept. of Computer Engineering Graduate School, Kyungpook National University.

요 약

인터넷과 같이 신뢰할 수 없는 네트워크를 통한 통신에서는 비밀성과 무결성뿐만 아니라 원격의 사용자 인증이 시스템 보안에 있어서 중요한 요소이다. 패스워드 기반의 사용자 인증 방법은 비용과 효율성 측면에서 갖는 장점 때문에 가장 널리 사용되는 사용자 인증 방법이다. 본 논문에서는 최근에 Lin [5]등이 제안한 패스워드 기반의 인증 방법인 SE-OSPA 프로토콜을 분석하고, 그 결과 DoS 공격에 취약함을 보인다. 또한 DoS 공격에 대응할 수 있는 개선된 스킴을 제안한다.

I. 서론

공개된 네트워크 시스템을 통하여 안전한 통신을 하기 위해서는 사용자 인증이 보안의 가장 중요한 부분이다. 통신 상대자간 신원증명은 그들간의 새로운 연결을 시작하기 전에 서로의 신원을 확인하여야 한다. 1981년 Lamport [1]가 원격 인증 스킴을 제안한 이후로 사용자에게 편리하고 비용이 적게 들면서 효율성면에서 향상된 패스워드 기반 인증 스킴들이 지금까지 여러 가지 방법으로 제안되었다.

2000년 Sandirigama [4]등은 간단한 SAS 프로토콜을 제안하였다. 하지만 Lin [3]등은 SAS가 재전송 공격, stolen-verifier 공격 등에 취약함을 제시한 후 이러한 공격에 안전한 새로운 스킴인 OSPA 프로토콜을 제안하였다. 그럼에도 불구하고, Chen과 Ku[2]는 OSPA 프로토콜이 SAS와 마찬가지로 여전히 stolen-verifier 공격에 취약함을 보였으며 2003년 최근에 Lin [5]등은 이러한 여러 가지 공격에 안전한 SE-OSPA 프로토콜을 제안하였다.

본 논문에서는 Lin [5]등이 제안한 SE-OSPA 프로토콜이 어떤 과정으로 인해서 합법적인 사용자가 올바른 패스워드를 제시하였음에도 서버가 로그인 요청을 쉽게 거부하는 서비스 거부 공격(Denial of Service attack)에 취약한지를 기술하며, 더 나아가서 SE-OSPA 프로토콜이 서비스 거부 공격에도 안전할 수 있도록 개선된 스킴을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 패스워드 기반 인증 프로토콜들이 만족해야 할 보안 요구사항을 설명한다. 3장에서는 SE-OSPA 프로토콜을 소개하고 어떻게 서비스 거부 공격이 가능한지를 기술하며, 4장에서는 본 논문에서 제안한 SE-OSPA 프로토콜을 개선한 스킴을 기술하고 안전성을 분석한다. 최종적으로 5장에서 결론을 맺는다.

II. 패스워드 기반 인증 프로토콜에서 보안 요구사항

(1) 추측 공격(Guessing attack)에 안전해야 한다:

추측 공격은 공격자가 사용자에 의해 자주 선택되는 패스워드들에 대한 사전을 가지고 있다고 할 때 수행되는 공격이다. 공격자가 사용자와 서버간의 통신을 저장한 후, 패스워드 사전으로 과거 통신에 사용된 패스워드와 일치하는 값을 비교하여 찾아낸다.

(2) 재전송 공격(Replay attack)에 안전해야 한다:

재전송 공격은 합법적인 사용자가 과거에 통신했던 메시지를 공격자가 저장했다가 이후의 통신에 재전송하는 공격이다.

(3) 가장 공격(Impersonation attack)에 안전해야 한다:

가장 공격은 공격자가 프로토콜에 참여하여 자신을 임의의 다른 사용자로 위장하여 정당한 사용자인 것처럼 행동하는 공격이다.

(4) Stolen-verifier 공격에 안전해야 한다:

Stolen-verifier 공격은 서버로부터 패스워드 확인자를 훔친 공격자가 인증 프로토콜에서 합법적인 사용자로 가장하여 훔친 패스워드 확인자를 직접 사용하는 공격이다.

(5) 서비스 거부 공격(DoS attack)에 안전해야 한다:

서비스 거부 공격은 서버의 정상적인 사용을 방해하고 제지하는 공격이다. 예를 들면, 공격자가 특정한 사용자의 재등록 전까지 모든 로그인 요청을 서버가 거부하도록 하는 공격이다.

Ⅲ. SE-OSPA 프로토콜에 대한 DoS 공격

이 장에서는 본 논문에서 사용할 용어들을 정의하고, SE-OSPA 프로토콜을 소개하고 인증 단계에서 이루어지는 서비스 거부 공격 과정을 기술한다.

3.1. 용어 정의

- ID_i : 사용자 i의 식별자
- P : 사용자 패스워드
- $h(\cdot)$: 일방향 해쉬 함수
- $\oplus$: 배타적 논리합 연산
- N : 랜덤 넌스
- N' : 다음 로그인을 위한 랜덤 넌스
- x : 서버의 비밀키 값

3.2. 프로토콜

SE-OSPA 프로토콜은 사용자 아이디와 패스워드를 설정하는 등록 단계와 인증 단계로 구성되며 프로토콜의 수행 절차는 다음과 같다.

등록 단계:

새로운 사용자 i가 서비스 접근을 위해 서버와 함께 안전한 등록을 하기를 원한다고 가정하자.

(1) 사용자 i는 패스워드 $h^2(P\oplus N)$을 계산하고 안전한 채널을 통하여 자신의 식별자 ID_i와 함께 서버에게 보낸다.

(2) 서버는 사용자 i의 식별자 ID_i가 증명되면 데이터베이스에 패스워드 확인자(verifier) $h^2(P\oplus N)$을 저장한 후 서버는 자신의 비밀키 값인 x를 이용하여 $K=h^2(P\oplus N)\oplus h(x\|ID_i)$를 계산하여 사용자 i의 스마트 카드에 N과 K값을 저장하여 발급한다.

인증 단계:

만일 사용자 i가 로그인하기를 원한다면, 입력장치에 스마트카드를 입력한다. 그 후 자신의 아이디 ID_i와 패스워드 P를 입력하면 스마트 카드는 다음과 같은 연산을 수행하여 사용자 i의 인증을 수행하게 된다.

(1) $c_1=K\oplus h^2(P\oplus N)=h(x\|ID_i)$을 계산한다. 여기서 K는 스마트 카드에 저장되어 있다.

(2) $c_2=c_1\oplus h(P\oplus N)$을 계산한다.

(3) $c_3=h(P\oplus N)\oplus h^2(P\oplus N')$을 계산한다.

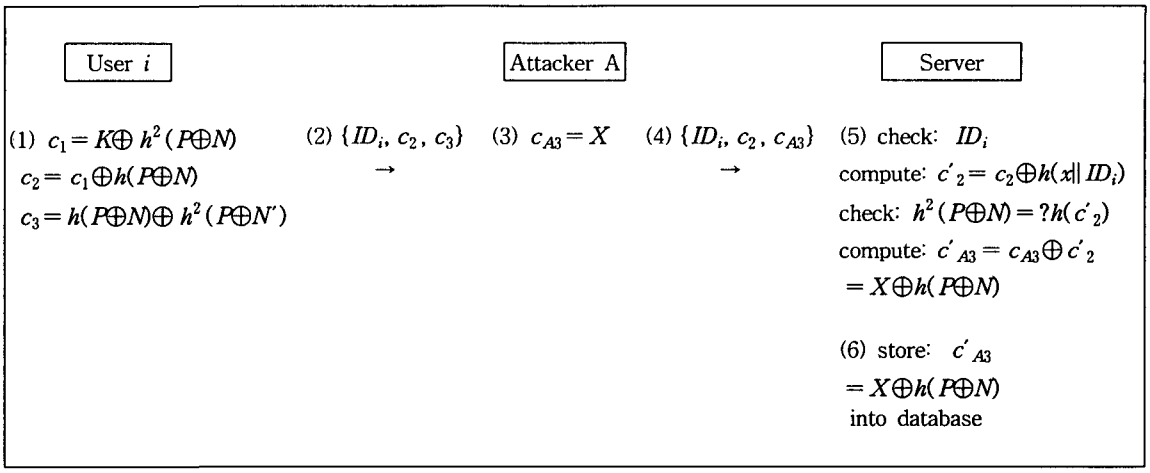

그림 1 인증 단계에서 공격자 A의 서비스 거부 공격 과정

여기서 $h^2(P \oplus N')$은 이후의 로그인 과정에 사용되는 다음번 패스워드 확인자이다.

(4) 로그인 요청으로 서버에게 메시지 $\{ID_i, c_2, c_3\}$를 보낸다.

서버는 사용자 i로부터 로그인 요청 메시지 $\{ID_i, c_2, c_3\}$를 받은 상태에서, 로그인 사용자 신원을 확인하기 위해서 다음과 같은 연산을 수행한다.

(1) 서버는 ID_i의 유효성을 확인한다. 만약 ID_i의 형식이 정확하지 않다면, 서버는 사용자 i와의 현재 접속을 종료하게 된다.

(2) 서버는 $h(x \| ID_i)$를 계산한 후 이 값을 이용하여 $c'_2 = c_2 \oplus h(x \| ID_i) = h(P \oplus N)$을 계산하고 저장된 패스워드 확인자 $h^2(P \oplus N) = ?h(c'_2)$인지를 확인하고, 만약 비교값이 같으면 서버는 사용자 i의 로그인 요청을 받아들여 접근 권한을 부여하고 그렇지 않으면 로그인 요청을 거절한다.

(3) $h^2(P \oplus N')$를 계산하고 다음번 로그인을 위해 기존의 패스워드 확인자 $h^2(P \oplus N)$을 다음번 패스워드 확인자 $h^2(P \oplus N')$로 업데이트 한다.

3.3 서비스 거부 공격

SE-OSPA 프로토콜은 인증 단계에서 서버가 임의의 사용자의 로그인 요청을 쉽게 거부할 수 있도록 공격자가 서비스 거부 공격을 할 수 있다. 비록 사용자가 올바른 패스워드를 제공하였다 할지라도, 그 사용자는 재등록을 해야만 한다. 다음과 같은 과정으로 공격자는 쉽게 서비스 거부 공격을 할 수 있다.

(1) N번째의 임의의 인증 절차에서 사용자 i는 서버에게 메시지 $\{ID_i, c_2, c_3\}$를 보낸다.

(2) 공격자 A는 사용자 i가 서버에게 보내는 메시지 $\{ID_i, c_2, c_3\}$를 가로채기한다.

(3) 공격자 A는 c_3를 c_{A3}로 다음의 예와 같이 임의의 값으로 수정을 한다:

$$c_{A3} = X$$

(4) 공격자 A는 서버에게 수정된 c_{A3}를 포함한 메시지 $\{ID_i, c_2, c_{A3}\}$를 보낸다.

(5) 서버는 공격자 A가 보낸 ID_i의 형식이 올바른가를 검사한다. 만약 이 검사를 통과하지 못한다면, 서버는 현재 접속을 종료하게 된다. 하지만 공격자 A는 사용자 i의 ID_i를 수정하지 않았기 때문에 이 과정을 통과하게 된다. 서버는 $h(x \| ID_i)$를 계산한 후 이 값을 이용하여 $c'_2 = c_2 \oplus h(x \| ID_i) = h(P \oplus N)$을 계산하고 저장된 패스워드 확인자 $h^2(P \oplus N)$와 $h(c'_2)$가 같은지를 검사하여 통과되면 서버는 공격자 A의 로그

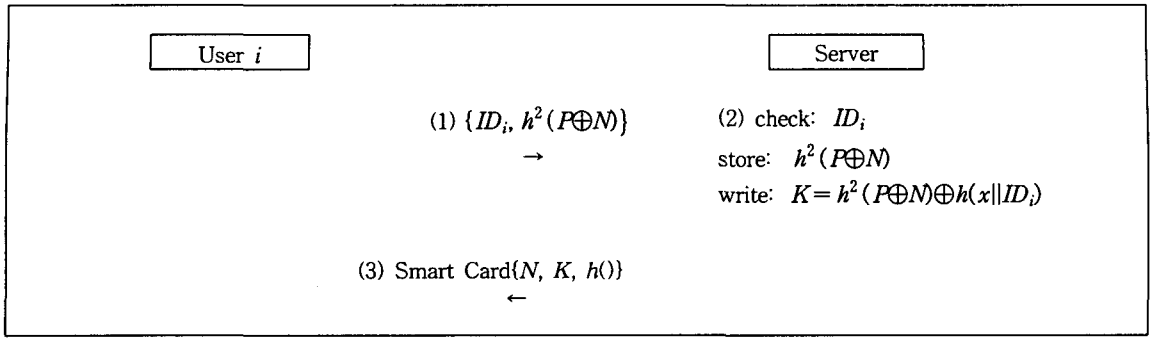

그림 2 제안한 스킴의 등록 단계

인 요청을 받아들여 접근 권한을 부여하고 그렇지 않으면 로그인 요청을 거절한다. 하지만 공격자 A는 사용자 i의 c_2를 수정하지 않았기 때문에 이 과정을 통과하게 된다. 서버는 다음과 같이 c'_{A3}를 계산한다:

$$c'_{A3} = c_{A3} \oplus c'_2 = X \oplus h(P \oplus N).$$

(6) 서버는 다음번 로그인을 위해 기존의 패스워드 확인자 $h^2(P\oplus N)$을 다음번 패스워드 확인자 즉 공격자 A가 조작한 c'_{A3}로 업데이트 한다.

다음번 인증 절차에서 사용자 i는 로그인 요청을 위해 서버에게 메시지 $\{ID_i, c_2, c_3\}$를 보내면 서버가 위 (5)(6)번 과정에서 공격자가 조작한 패스워드 확인자 c'_{A3}와 $h(c'_2)$가 같은지를 검사하는 과정에서 다음과 같이 패스워드가 일치하지 않게 되어 서버로부터 로그인 요청을 거부당하게 된다:

$$X \oplus h(P \oplus N) \neq h^2(P \oplus N').$$

결론적으로 SE-OSPA 프로토콜은 현재 사용자 패스워드 $h^2(P\oplus N)$에 대한 무결성 검사는 이루어지지만, 다음번 패스워드 확인자 $h^2(P\oplus N')$에 대한 무결성 검사를 하지 않고 기존의 패스워드 확인자를 다음번 패스워드 확인자로 업데이트 하기 때문에 서비스 거부 공격에 취약하다. 공격자 A의 서비스 거부 공격 과정은 그림 1과 같이 수행된다.

Ⅳ. 제안한 프로토콜

이 장에서는 서비스 거부 공격에 안전한 개선된 스킴을 제안하며 제안한 스킴의 여러 가지 공격에 대한 안전성을 분석한다.

4.1 프로토콜

본 논문에서 제안한 스킴은 사용자 아이디와 패스워드를 설정하는 등록 단계와 인증 단계로 구성되며 프로토콜의 수행 절차는 다음과 같다.

등록 단계:

새로운 사용자 i가 서비스 접근을 위해 서버와 함께 안전한 등록을 하기를 원한다고 가정하자.

(1) 사용자 i는 패스워드 $h^2(P\oplus N)$을 계산하고 안전한 채널을 통하여 자신의 식별자 ID_i와 함께 서버에게 보낸다.

(2) 서버는 사용자 i의 식별자 ID_i가 증명되면 데이터베이스에 패스워드 확인자 $h^2(P\oplus N)$을 저장한 후 서버는 자신의 비밀키 값인 x를 이용하여 다음과 같이 K를 계산하여 사용자 i의 스마트 카드에 N과 K값을 저장하여 발급한다.:

$$K = h^2(P \oplus N) \oplus h(x \| ID_i).$$

본 논문에서 제안한 스킴의 등록 단계는 그림 2와 같이 수행된다.

인증 단계:

만일 사용자 i가 로그인하기를 원한다면, 입력장치에 스마트카드를 입력한다. 그 후 자신의 아이디 ID_i와 패스워드 P를 입력하면 스마트 카드

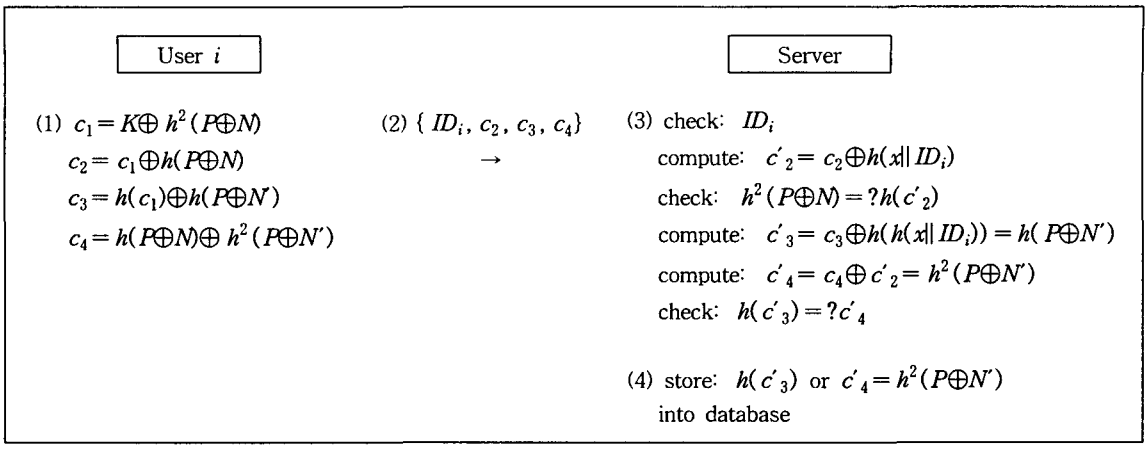

그림 3 제안한 스킴의 인증 단계

는 다음과 같은 연산을 수행하여 사용자 i의 인증을 수행하게 된다.

(1) $c_1 = K \oplus h^2(P \oplus N) = h(x \| ID_i)$을 계산한다.
(2) $c_2 = c_1 \oplus h(P \oplus N)$을 계산한다.
(3) $c_3 = h(c_1) \oplus h(P \oplus N')$을 계산한다.
(4) $c_4 = h(P \oplus N) \oplus h^2(P \oplus N')$을 계산한다.
(5) 로그인 요청으로 서버에게 메시지 $\{ID_i, c_2, c_3, c_4\}$를 보낸다.

서버는 사용자 i로부터 로그인 요청 메시지 $\{ID_i, c_2, c_3, c_4\}$를 받은 상태에서, 로그인 사용자 신원을 확인하기 위해서 다음과 같은 연산을 수행한다.

(1) 서버는 ID_i의 유효성을 확인한다. 만약 ID_i의 형식이 정확하지 않다면, 서버는 사용자 i와의 현재 접속을 종료하게 된다.
(2) 서버는 $h(x \| ID_i)$를 계산한 후 이 값을 이용하여 $c'_2 = c_2 \oplus h(x \| ID_i) = h(P \oplus N)$을 계산하고 저장된 패스워드 확인자 $h^2(P \oplus N) = ?h(c'_2)$인지를 확인하고, 만약 비교값이 같으면 서버는 사용자 i의 로그인 요청을 받아들여 접근 권한을 부여하고 그렇지 않으면 로그인 요청을 거절한다.
(3) 서버는 $c'_3 = c_3 \oplus h(h(x \| ID_i)) = h(P \oplus N')$를 계산하고 $c'_4 = c_4 \oplus c'_2 = h^2(P \oplus N')$를 계산하여 $h(c'_3) = ?c'_4$인지를 확인하고, 만약 비교값이 같으면 서버는 다음번 로그인을 위해 기존의 패스워드 확인자 $h^2(P \oplus N)$을 다음번 패스워드 확인자 $h^2(P \oplus N')$로 업데이트 한다.

본 논문에서 제안한 스킴의 인증 단계는 그림 3과 같이 수행된다.

4.2 안전성 분석

이 절에서는 본 논문에서 제안한 스킴의 여러 가지 공격에 대한 안전성을 분석한다.

· 추측 공격: 공개된 네트워크상에서 공격자가 로그인 요청 메시지 $\{ID_i, c_2, c_3, c_4\}$를 가로채기 하였다고 해도, 공격자는 c_2, c_3, c_4로부터 N, N' 그리고 서버의 비밀키 x를 알아 낼 수 없기 때문에 로그인 사용자의 패스워드 P를 유도할 수 없다. 따라서 제안한 스킴은 추측공격에 안전하다.

· 재전송 공격: 매 세션마다 사용자는 새로 생성되는 랜덤 넌스 N'와 패스워드 확인자 $h^2(P \oplus N')$를 사용하기 때문에, 공격자가 이전 세션에서 전송된 메시지를 가지고 있어도 다음 세션에서 그 메시지를 사용할 수 없으므로 재전송 공격을 수행할 수 없다.

· **가장 공격**: 공격자 A는 로그인 요청 메시지 $\{ID_i, c_2, c_3, c_4\}$를 위조한 후 서버에게 보내야 사용자 i인체 가장할 수 있다. 하지만 서버는 로그인 사용자 신원확인을 위해 인증 단계에서 다음과 같이 위조된 c_{A2}를 저장된 패스워드 확인자 $h^2(P \oplus N)$와 같은지를 검사한다:

$$c'_{A2} = c_{A2} \oplus h(x \| ID_i)$$
$$h^2(P \oplus N) \neq h(c'_{A2}).$$

이때 위조된 c'_{A2}는 위 확인 등식을 만족하지 않기 때문에 검사과정을 통과할 수 없다. 따라서 공격자는 가장 공격을 행할 수 있는 어떤 기회도 가지지 못한다.

· **Stolen-verifier 공격**: 공격자가 서버로부터 패스워드 확인자 $h^2(P \oplus N)$을 훔치고 공개된 네트워크로부터 사용자 i의 $(N-1)$번째 로그인 요청 $\{ID_i, c_2, c_3, c_4\}$를 가로채기 하였다고 해도, 훔친 패스워드 확인자 $h^2(P \oplus N)$를 이용하여 c_2, c_3, c_4로부터 $h(P \oplus N)$과 $h^2(P \oplus N')$을 유도할 수 없기 때문에 제안한 스킴은 $h(\cdot)$가 강력한 일방향 해쉬 함수임으로 stolen-verifier 공격에 대하여 안전하다.

· **서비스 거부 공격**: SE-OSPA 프로토콜에서는 다음번 패스워드 확인자 $h^2(P \oplus N')$에 대한 무결성 검사 과정을 수행하지 않기 때문에 서비스 거부 공격이 이루어진다. 제안된 스킴에서는 다음번 패스워드 확인자 $h^2(P \oplus N')$가 포함되어있는 c_3, c_4에 대한 무결성 검사를 수행하여 이 검사 과정이 통과되면, 서버는 다음번 로그인을 위해 기존 패스워드 확인자 $h^2(P \oplus N)$을 다음번 패스워드 확인자 $h^2(P \oplus N')$로 업데이트 하기 때문에 서비스 거부 공격에 대하여 안전하다.

V. 결론

본 논문에서는 SE-OSPA 프로토콜이 서비스 거부 공격에 취약함을 보였고, 서비스 거부 공격에 안전할 수 있도록 SE-OSPA 프로토콜의 개선된 스킴을 제안하였다. 또한 제안한 스킴이 기타 여러 가지 공격에도 안전함을 보였다.

본 논문에서 제안한 스킴은 기존의 SE-OSPA 프로토콜의 안전도를 저하시키지 않으면서, 기존 패스워드 확인자 기반 방식의 프로토콜보다 개선된 안전성을 가진다. 따라서 본 논문에서 제안한 스킴은 사용자 인증을 요하는 시스템에 유용하게 적용될 수 있을 것으로 기대된다.

참고문헌

[1] L. Lamport, "Password authentication with insecure communication," Communication of ACM, Vol. 24, 1981, pp. 770-772

[2] Chien-Ming Chen and Wei-Chi Ku. "Stolen-verifier attack on two new strong-password authentication protocols." IEICE Transactions on Communications, E85-B(11):2519-2521, November 2002.

[3] C. L. Lin, H. M. Sun, and T. Hwang. "Attacks and solutions on strong-password authentication." IEICE Transactions on Communications, E84-B(9):2622-2627, September 2001.

[4] M. Sandirigama, A. Shimizu, and M. T. Noda. "Simple and secure password authentication protocol (sas). IEICE Transactions on Communications," E83-B(6):1363-1365, June 2000.

[5] Chih-Wei Lin, Jau-Ji Shen, and Min-Shiang Hwang. "Security Enhancement for Oprimal Strong-Password Authentication Protocol." ACM Operating Systems Review, Volume 37 Issue 2, April 2003