Yang의 강력한 패스워드 인증 스킴에 대한 보안 취약점 분석

김준섭, 곽진
순천향대학교 정보보호학과
e-mail : jskim0911@sch.ac.kr, jkwak@sch.ac.kr

Security Vulnerability Analysis for Yang's Strong Password Authentication Scheme

Jun-Sub Kim, Jin Kwak
Dept of Information Security Engineering, Soonchunhyang University

요 약

현재까지 많은 강력한 패스워드 인증 프로토콜들이 제안되고 있으나 이 프로토콜들은 여러 보안 취약점이 존재한다. 2010년 Yang 등은 Ku가 제안한 프로토콜이 훔친 검증자 공격에 취약하다는 것을 지적하며 SPAS를 제안하였다. 하지만 SPAS는 Ku의 프로토콜과 마찬가지로 훔친 검증자 공격에 대한 취약성을 가지고 있다. 따라서 본 논문에서는 SPAS를 분석하고 SPAS가 훔친 검증자 공격에 안전하지 못함을 증명한다.

1. 서론

사용자 인증은 개방형 네트워크에서 안전한 통신을 보장하기 위한 중요한 보안 기술이다. 클라이언트와 서버 간의 통신에서 공격자가 변경하거나 도청하더라도 인증 메시지에 대한 안전성과 기밀성을 보장할 수 있어야 한다. 이러한 인증 방식으로 패스워드 인증 프로토콜을 가장 널리 사용하고 있다.

1981년 Lamport가 일회용 패스워드 인증 방식을 제안하였다[1]. 이 방식은 높은 오버헤드와 패스워드 재설정에 대한 문제로 인하여 실제 구현에 대한 어려움이 있다. 이러한 문제를 해결하기 위해 Shimizu는 CINON(chained one-way data verification method) 방식을 제안하였다[2, 3]. 하지만 CINON 방식은 난수를 메모리 장치 등에 저장하여 안전성을 제공하지만, 이는 휴대의 불편함과 하드웨어의 고비용에 대한 문제점이 발생하였다. 이후 Hailer는 Lamport 방식을 개선하여 효율적인 프로토콜인 S/KEY 방식[4]을 제안하였지만, Mitchell은 Hailer의 프로토콜이 재전송 공격에 취약하다는 것을 증명하였다[5]. Lamport와 S/KEY 방식의 취약점을 해결하기 위해 Shimizu는 PERM(Privacy Enhanced information Reading end writing Management method)이라고 불리는 개선된 일회용 패스워드 인증 방식을 제안하였다[6]. 하지만 PERM 방식은 중간자 공격과 위장 공격에 취약하다.

2000년 Sandirigama 등은 이전 방식보다 우수하고 단순한 강력한 패스워드 인증 프로토콜인 SAS(Simple and Secure) 프로토콜을 제안하였다[7]. 하지만 Lin 등은 SAS 프로토콜이 재전송 공격과 서비스 거부 공격에 대한 취약성을 지적하며, OSPA(Optimal Strong Password Authentication) 프로토콜을 제안하였다[8]. 그럼에도 불구하고 Chen과 Ku는 SAS와 OSPA 프로토콜이 훔친 검증자 공격에 취약하다는 것을 증명하였다[9]. 2003년 Lin 등은 OSPA 프로토콜의 안전성을 강화한 SE-OSPA(Security Enhancement for Optimal Strong Password Authentication) 프로토콜을 제안하였다[10]. 그러나 Ku 등은 SE-OSPA 프로토콜이 재전송 공격과 서비스 거부 공격에 대한 취약성을 지적하며[11], Ku는 스마트카드를 사용하지 않는 해시 기반의 강력한 패스워드 인증 프로토콜을 제안하였다[12]. 이후 2010년 Yang 등은 Ku의 프로토콜이 훔친 검증자 공격에 대한 취약성을 지적하며, SPAS(Strong Password Authentication Scheme)를 제안하였다[13]. 하지만 SPAS는 Ku의 프로토콜과 마찬가지로 훔친 검증자 공격에 대한 취약성을 가지고 있다. 따라서 본 논문에서는 SPAS가 훔친 검증자 공격에 안전하지 못함을 증명한다.

본 논문의 구성은 다음과 같다. 2장에서는 SPAS를 분석하고, 3장에서는 SPAS가 훔친 검증자 공격에 안전하지 못함을 증명한다. 마지막으로 4장에서는 결론을 맺는다.

2. 강력한 패스워드 인증 프로토콜 분석

본 장에서는 Yang 등이 제안한 SPAS에 대하여 분석하

고, 3장에서는 SPAS가 훔친 검증자 공격에 안전하지 못함을 증명한다. SPAS에서 사용한 시스템 파라미터는 <표 1>과 같다.

<표 1> 시스템 파라미터

기호	의미
U	사용자
S	서버
ID	사용자의 식별자
P	사용자의 패스워드
N	현재 세션을 위한 랜덤 넌스
T	타임스탬프
X_s	서버의 비밀키
r	임의의 랜덤 넌스
$K_u^{(T)}$	스토리지 키
$sv^{(N)}$	봉인된 검증자
$\oplus$	배타적 논리합 연산
$\|\|$	연접 연산
$A \rightarrow B$: X	X가 A에서 B로 전송

SPAS는 등록 단계와 인증 단계로 구성되어 있으며, 구성은 다음과 같다.

[등록 단계]

① 사용자 U는 서버 S에 등록을 하기 위해 등록 요청 메시지를 전송한다.

② $S \rightarrow U$: $\{N, T\}$

서버 S는 타임스탬프 T, 현재 세션을 위한 랜덤 넌스 N을 사용자 U에게 전송한다.

③ $U \rightarrow S$: $\{h^2(S||P||N||T)\}$

사용자 U는 현재 세션을 위한 패스워드 검증자 $h^2(S||P||N||T)$를 계산하여 서버 S에게 전송한다.

④ 서버 S는 사용자의 스토리지 키 $K_u^{(T)}$와 봉인된 검증자 $sv^{(N)}$을 계산한 후 $sv^{(N)}$, N, T를 저장한다.

$K_u^{(T)}=h(ID||h(X_s||T))$

$sv^{(N)}=h^2(S||P||N||T) \oplus K_u^{(T)}$

[인증 단계]

① 사용자 U는 서버 S에 인증을 하기 위해 로그인 요청 메시지를 전송한다.

② $S \rightarrow U$: $\{r, T\}$

서버 S는 랜덤 넌스 r, 타임스탬프 T를 사용자 U에게 전송한다.

③ $U \rightarrow S$: $\{c_1, c_2, c_3\}$

사용자 U는 다음과 같이 c_1, c_2, c_3을 계산한 후 메시지 $\{c_1, c_2, c_3\}$을 서버 S에게 전송한다.

$c_1=h^2(S||P||N||T) \oplus h(S||P||N||T)$

$c_2=h(S||P||N||T) \oplus h^2(S||P||N+1||T)$

$c_3=h(h^2(S||P||N+1||T)||r)$

④ 서버 S는 $K_u^{(T)}=h(ID||h(X_s||T))$를 계산한 후 $sv^{(N)}$과 $K_u^{(T)}$를 연산하여 사용자 U의 패스워드 검증자 $h^2(S||P||N||T)$를 계산한다.

$sv^{(N)} \oplus K_u^{(T)}=h^2(S||P||N||T)$

⑤ 서버 S는 c_1과 $h^2(S||P||N||T)$를 연산하여 $h(S||P||N||T)$를 계산한 후 c_2와 $h(S||P||N||T)$를 연산하여 다음 세션을 위한 패스워드 검증자 $h^2(S||P||N+1||T)$를 계산한다.

$u_1=c_1 \oplus h^2(S||P||N||T)=h(S||P||N||T)$

$u_2=c_2 \oplus h(S||P||N||T)=h^2(S||P||N+1||T)$

⑥ 서버 S는 $h(u_1)$와 현재 세션을 위한 패스워드 검증자 $h^2(S||P||N||T)$, $h(u_2||r)$와 c_3에 대한 무결성을 각각 검증한다.

$h(u_1)=h^2(S||P||N||T)$

$h(u_2||r)=h(h^2(S||P||N+1||T)||r)$

⑦ 현재 세션을 위한 패스워드 검증자 $h^2(S||P||N||T)$와 c_3에 대한 무결성이 검증되면 다음 세션을 위한 패스워드 검증자 $h^2(S||P||N+1||T)$와 사용자의 스토리지 키 $K_u^{(T)}$를 연산하여 다음 세션을 위한 봉인된 검증자 $sv^{(N+1)}$를 계산한다. 이후 사용자 U의 다음 로그인을 위해 $sv^{(N)}$을 $sv^{(N+1)}$으로 업데이트하고 $N=N+1$을 설정한다.

3. 훔친 검증자 공격에 대한 취약점

공격자 A는 사용자 U의 $n-1$번째 로그인 후에 패스워드 검증자 $h^2(S||P||N||T)$를 훔쳤다고 가정한다. 사용자

U가 서버 S로부터 n번째 로그인을 하는 동안 공격자 A는 서버 S로부터 사용자 U에게 전송하는 메시지 $\{r, T\}$를 도청하고, 사용자 U로부터 서버 S에게 전송하는 메시지 $\{c_1, c_2, c_3\}$을 차단하고 복사한다. 공격자 A는 $h^2(S||P||N||T)$와 c_1을 연산하여 $h(S||P||N||T)$를 계산한다. 이후 공격자 A는 P_A, N_A+1을 선택하고 $c_{A2}=h(S||P||N||T)\oplus h^2(S||P_A||N_A+1||T)$, $c_{A3}=h(h^2(S||P_A||N_A+1||T)||r)$를 계산한 후 메시지 $\{c_1, c_2, c_3\}$을 $\{c_1, c_{A2}, c_{A3}\}$로 교환하여 전송한다.

서버 S는 $sv^{(N)}$와 $K_u^{(T)}$를 연산하여 현재 세션을 위한 패스워드 검증자 $h^2(S||P||N||T)$를 계산한다. 서버 S는 $h^2(S||P||N||T)$와 c_1을 연산하여 $u_3=h(S||P||N||T)$를 계산한 후 c_2와 $h(S||P||N||T)$를 연산하여 다음 세션을 위한 패스워드 검증자 $u_4=h^2(S||P_A||N_A+1||T)$를 계산한다. 이후 $h(u_3)$와 현재 세션을 위한 패스워드 검증자 $h^2(S||P||N||T)$, $h(u_4||r)$와 c_{A3}에 대한 무결성을 각각 검증한다. 현재 세션을 위한 패스워드 검증자 $h^2(S||P||N||T)$와 c_{A3}에 대한 무결성이 검증되기 때문에 서버 S는 다음 세션을 위한 패스워드 검증자 $h^2(S||P_A||N_A+1||T)$와 사용자의 스토리지 키 $K_u^{(T)}$를 연산하여 다음 세션을 위한 봉인된 검증자 $sv^{(N+1)}$를 계산하고 사용자 U의 다음 로그인을 위해 $sv^{(N)}$을 $sv^{(N+1)}$으로 업데이트하고 $N=N+1$을 설정한다.

이후 사용자 U가 다음의 로그인을 하기 전에 공격자 A는 사용자 U로 위장하기 위하여 $c_{A1}=h^2(S||P_A||N_A+1||T)\oplus h(S||P_A||N_A+1||T)$, $c_{A2}=h(S||P_A||N_A+1||T)\oplus h^2(S||P_A||N_A+2||T)$, $c_{A3}=h(h^2(S||P_A||N_A+2||T)||r)$를 계산하여 전송하면 서버 S로부터 인증에 성공할 수 있다. 따라서 SPAS는 훔친 검증자 공격에 취약하다.

4. 결론

본 논문에서는 Yang 등이 제안한 SPAS의 안전성을 분석하였다. 분석한 결과 SPAS는 Ku의 프로토콜과 마찬가지로 서버로부터 패스워드 검증자를 훔친 공격자가 인증 단계에서 합법적인 사용자로 위장하여 서버로부터 인증을 받을 수 있는 훔친 검증자 공격에 취약하다.

참고문헌

[1] L. Lamport, “Password Authentication with Insecure Communication,” Communication of ACM, Vol. 24, no. 11, pp. 770-772, Nov. 1981.

[2] A. Shimizu, “A dynamic password authentication method by one-way function,” IEICE Transactions on Communications, Vol. J73-D-I, no. 7, pp. 630-636, Jul. 1990.

[3] A. Shimizu, “A dynamic password authentication method by one-way function,” System and Computers in Japan, Vol. 22, no. 7, pp. 32-40, Jul. 1991.

[4] N. M. Hailer, “The S/KEY™ one-time password system,” in Proceedings of the Internet Society Stmposium on Network and Distributed System Security, pp. 151-158, 1994.

[5] C. J. Mitchell and L. Chen, “Comments on S/KEY user authentication scheme,” ACM Operating Systems Review, Vol. 30, no. 4, pp. 12-16, 1996.

[6] A. Shimizu, T. Horioka, and H. Inagaki, “A password authentication method for contents communication on the internet,” IEICE Transactions on Communications, Vol. E81-B, no. 8, pp. 1666-1673, Aug. 1998.

[7] M. Sandirigama, A. Shimizu, and M. T. Noda, “Simple and Secure Password Authentication Protocol,” IEICE Transactions on Communications, Vol. E83-B, no. 6, pp. 1363-1365, Jun. 2000.

[8] C. L. Lin, H. M. Sun, and T. Hwang, “Attacks and Solutions on Strong-Password Authentication,” IEICE Transactions on Communications, Vol. E84-B, no. 9, pp. 2622-2627, Sep. 2001.

[9] C. M. Chen and W. C. Ku, “Stolen-Verifier Attack on Two New Strong-Password Authentication Protocols,” IEICE Transactions on Communicatioins, Vol. E85-B, no. 11, pp. 2519-2521, Nov. 2002.

[10] C. W. Lin, J. J. Shen, and M. S. Hwang, “Security Enhancement for Optimal Strong-Password Authentication Protocol,” ACM SIGOPS Operating Systems Review, Vol. 37, no. 2, pp. 7-12, Apr. 2003.

[11] W. C. Ku, H. C. Tsai, and S. M. Chen, “Two simple attack on Lin-Shen-Hwang's strong-password authentication protocol,” ACM SIGOPS Operating Systems Review, Vol. 37, no. 4, pp. 26-31, Oct. 2003.

[12] W. C. Ku, “A Hash-Based Strong-Password Authentication Scheme without Using Smart Cards,” ACM Operating System Review, Vol. 38, no. 1, pp. 29-34, Jant. 2004.

[13] Jingbo Yang and Pingping Shen, “A Secure Strong Password Authentication Protocol,” 2010 2th International Conference on Software Technology and Engineering, Vol. 2, pp. 355-357, Oct. 2010.