제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

Cho의 원격 인증스킴에 대한 보안 취약점 분석

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

Security Vulnerability Analysis for Cho's Remote Authentication Scheme

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

요 약

현재까지 사용되는 인증 기술에서는 패스워드 기반의 인증스킴이 주로 사용되고 있다. 공개된 네트워크상에서의 인증스킴의 안전성 보장을 위하여 많은 인증스킴이 연구 및 제안되고 있지만, 이러한 인증스킴들은 아직까지 여러 보안 취약점의 문제를 갖고 있다. 2010년 Cho는 Lee 등의 인증스킴을 분석하여 보안이 개선된 원격 인증스킴을 제안하였지만, 이 인증스킴 또한 여전히 공격자에 의한 DoS 공격과 훔친 검증자 공격에 대한 취약점을 가지고 있다. 따라서 본 논문에서는 Cho의 원격 인증스킴에 대해 분석하고, DoS 공격과 훔친 검증자 공격에 대해 안전하지 못함을 증명한다.

1. 서론

공개된 네트워크를 통한 다양한 통신 환경에서 패스워드 기반의 사용자 인증 기술은 기술 비용의 이점과 사용자의 편리성으로 인해 가장 보편적으로 사용되고 있다. 사용자 인증기술에서는 보안이 중요하기 때문에 오늘날까지 다양한 연구가 지속적으로 이루어지고 있다.

일반적인 네트워크에서 원격으로 접속을 하는 방법으로는 원격 응용 프로그램이 사용자의 ID와 패스워드를 요구하게 된다. 이러한 역할을 수행하는 네트워크 서버는 서버가 제한된 접근 권한을 적용하는 방식으로, 네트워크 및 리소스에 접근할 권한이 있는 사용자의 ID를 식별하여 접근의 허용여부를 판단한다. 과거에는 공개된 네트워크에서 전송되는 메시지와 패스워드를 보호하기 위해 대칭키 암호나 공개 키 암호 등을 통해 암호화 하였다[1-3]. 하지만 이러한 방식은 추가적인 키를 교환하는데 있어 암호화 이외에 다른 방식으로는 보호하지 않았다. 또한 안전하지 않은 네트워크를 통해 전송되는 메시지는 공격자에 의해 비교적 쉽게 접근할 수 있으며, 사용자가 전송하는 패스워드는 도청공격에 취약하다[4-5]. 하지만 2000년 Peyravian과 Zunic은 암호화키를 이용하는 방식이 아닌, 해시함수를 이용한 스킴을 제안하였다. 이 해시함수 기반의 인증스킴은 공개된 네트워크상에서 패스워드의 안전성을 높이고 패스워드를 변경할 수 있는 인증스킴으로, 추가적인 키의 변경을 요구하지 않아도 안전하게 메시지를 보호하고 패스워드를 변경할 수 있다[6]. 하지만 이 스킴은 패스워드 추측 공격에 대한 취약점이 발견되면서 이를 보완하기 위해 2002년 Lee 등은 Peyravian과 Zunic의 인증스킴에서 추측 공격에 대한 취약점을 보완하여 해시함수 기반의 새로운 인증스킴을 발표하였다[7]. 그러나 Lee 등이 발표한 스킴은 패스워드 검증자를 변경시키면서, 새로운 패스워드 검증자가 등록되는 과정에서 이에 대한 무결성 검증을 하지 않는다. 따라서 이 스킴은 공격자가 위조된 메시지를 변경하여 보낼 경우, 메시지가 그대로 검증테이블에 저장되어 이 후 로그인 요청을 하더라도 서버에서는 사용자를 거부한다.

2010년 Cho는 2002년 발표된 L-L-H의 인증스킴을 분석하여 패스워드 검증자에 대한 무결성 검사를 통해 공격자의 메시지를 거부함으로써 안전한 원격 인증스킴을 제안하였다. 또한 세션마다 안전한 패스워드 검증자 변경이 가능하고, 이에 대한 무결성을 제공하면서 DoS 공격에 안전하다고 주장하고 있다[8]. 하지만 Cho가 제안한 원격 인증스킴은 훔친 검증자 공격과 DoS 공격에 대한 취약점을 가지고 있다. 따라서 본 논문에서는 Cho가 제안한 원격 인증스킴에 대한 취약점을 증명한다.

본 논문의 구성은 다음과 같다. 2장에서는 Cho가 제안한 원격 인증스킴을 분석하고 3장에서는 Cho의 인증스킴이 DoS 공격과 훔친 검증자 공격에 안전하지 못함을 증명한다. 마지막으로 4장에서는 결론을 맺는다.

2. Cho의 원격 인증스킴

본 장에서는 Cho가 제안한 원격 인증스킴에 대하여 분석한다. <표 1>은 원격 인증스킴의 시스템 파라미터를 나

타낸다.

<표 1> 시스템 파라미터

기호	의미
$h()$	일방향 해시 함수
T	타임스탬프
X_s	서버의 비밀키
ID	사용자의 ID
A_s	서버의 인증값
P	사용자의 패스워드
r_c	사용자의 랜덤값
r_s	서버의 랜덤값
$A \rightarrow B: X$	X가 A에서 B로 전송

2.1 등록 단계

① $U \rightarrow S: ID, r_c$

사용자 U는 ID와 랜덤값 r_c를 선택하여 $h(P \| r_c)$를 생성한 후 서버 S에게 전송한다.

② $S \rightarrow U$: 스마트카드$\{A_s\}$

서버 S는 사용자의 ID와 검증자 $h(P \| r_c)$를 저장한다. 그리고 A_s를 계산하여 스마트카드에 저장한 후 사용자에게 스마트카드를 발급한다.

$$A_s = h(ID \oplus X_s) \oplus h(P \| r_c)$$

2.2 인증 및 검증자 업데이트 단계

① $U \rightarrow S: \{ID, T, c_3\}$

사용자 U는 아래와 같은 c_1, c_2, c_3를 계산한 후 서버에게 $\{ID, T, c_3\}$를 전송한다.

$$c_1 = A_s \oplus h(P \| r_c) = h(ID \oplus X_s)$$
$$c_2 = ID \oplus T$$
$$c_3 = h(c_1 \oplus c_2) = h(h(ID \oplus X_s) \oplus ID \oplus T)$$

② $S \rightarrow U: \{r_s \oplus h(P \| r_c)\}$

서버 S는 사용자 U로부터 받은 T를 이용하여 시간 유효성 값과 c_3를 검증하여, 사용자 U를 인증하게 된다. 그리고 자신의 랜덤값 r_s를 생성하여 $r_s \oplus h(P \| r_c)$을 계산한 후 사용자 U에게 전송한다.

③ $U \rightarrow S: \{c_4, c_5\}$

사용자 U는 서버 S로부터 받은 $r_s \oplus h(P \| r_c)$와 패스워드 검증자 $h(P \| r_c)$를 이용하여 r_s를 계산한다. 이 후 다음 세션을 위한 랜덤값 r_c'을 선택하여 다음 세션을 위한 패스워드 검증자 $h(P \| r_c')$을 계산한 후, c_4와 c_5를 계산하여, $\{c_4, c_5\}$를 서버 S에게 전송한다.

$$c_4 = h(c_1) \oplus h(P \| r_c') \oplus r_s$$
$$c_5 = h(P \| r_c) \oplus h(P \| r_c')$$

④ 서버 S는 사용자 U로부터 받은 c_4와 c_5를 이용하여 다음과 같은 검증 과정을 수행한다.

$$c_4' = c_4 \oplus h(h(ID \| X_s)) \oplus r_s = h(P \| r_c')$$
$$c_5' = c_5 \oplus h(P \| r_c) = h(P \| r_c')$$

각 c_4'와 c_5'에서 계산된 다음 세션을 위한 패스워드 검증자에 대한 무결성을 검증한다. 무결성이 검증되면 현재 세션을 위한 $h(P \| r_c')$이 동일한 값인지를 확인하여 기존의 패스워드 검증자인 $h(P \| r_c)$를 $h(P \| r_c')$로 업데이트한다.

3. 취약점 분석

2장에서 분석한 Cho의 원격 인증스킴은 DoS 공격에 대한 취약성을 보완하여 재전송 공격이나 위장 공격, 추측 공격에 안전하다고 제안되었다. 하지만 Cho의 원격 인증스킴은 DoS 공격과 훔친 검증자 공격에 대한 취약점을 가지고 있다.

따라서 본 장에서는 Cho의 원격 인증스킴이 DoS 공격과 훔친 검증자 공격에 안전하지 못함을 증명한다.

3.1 DoS 공격에 대한 취약점

공격자 A는 인증 및 검증자 업데이트 단계에서 $r_s \oplus h(P \| r_c)$를 도청하여 복사한다. 이 후 공격자 A는 사용자 U가 서버 S로 전송하는 c_4, c_5를 차단하고, $r_s \oplus h(P \| r_c)$를 이용하여 c_4*와 c_5*를 계산한다.

$$\begin{aligned} c_5^* &= c_5 \oplus r_s \oplus h(P \| r_c) \\ &= h(P \| r_c) \oplus h(P \| r_c') \oplus r_s \oplus h(P \| r_c) \\ &= h(P \| r_c') \oplus r_s \end{aligned}$$

$$\begin{aligned} c_4^* &= c_4 \oplus c_5^* \\ &= h(c_1) \oplus h(P \| r_c') \oplus r_s \oplus h(P \| r_c') \oplus r_s \\ &= h(c_1) \end{aligned}$$

그리고 계산한 c_4*를 이용하여 c_5**를 계산한다.

$$\begin{aligned} c_5^{**} &= c_5 \oplus c_4^* \\ &= h(P \| r_c) \oplus h(P \| r_c') \oplus h(c_1) \end{aligned}$$

계산한 c_5*, c_5**를 이용하여, 이전에 차단한 메시지 $\{c_4, c_5\}$를 메시지 $\{c_5^*, c_5^{**}\}$로 교환하여 서버에 전송한다.

c_5*, c_5**를 수신한 서버 S는 c_5*, c_5**를 이용하여 다음 세션을 위한 검증자 업데이트 연산을 수행한다.

$$c_4' = c_5^{*} \oplus h(c_1) \oplus r_s$$
$$= h(P \| r_c') \oplus r_s \oplus h(c_1) \oplus r_s$$
$$= h(P \| r_c') \oplus h(c_1)$$

$$c_5' = c_5^{**} \oplus h(P \| r_c)$$
$$= h(P \| r_c) \oplus h(P \| r_c') \oplus h(c_1) \oplus h(P \| r_c)$$
$$= h(P \| r_c') \oplus h(c_1)$$

서버 S는 c_4', c_5'에서 계산된 다음 세션을 위한 패스워드 검증자에 대한 무결성을 검증하는데, c_4'과 c_5'에서 계산된 패스워드 검증자 $h(P \| r_c') \oplus h(c_1)$은 동일하기 때문에 무결성을 검증하고, 현재 세션을 위한 패스워드 검증자 $h(P \| r_c')$를 $h(P \| r_c') \oplus h(c_1)$으로 업데이트한다. 이 후 사용자 U는 서버 S로부터 인증을 받으려고 하여도 서버 S에 등록된 패스워드 검증자가 다르기 때문에 인증을 받을 수 없다. 따라서 Cho의 원격 인증스킴은 DoS 공격에 취약하다.

3.2 훔친 검증자 공격에 대한 취약점

공격자 A는 $n-1$번째 인증에 성공하여 업데이트된 검증자 $h(P \| r_c)$를 훔쳤다고 가정한다. 그리고 사용자 U가 c_4, c_5를 전송할 때, 이를 차단하여 다음과 같은 연산을 수행한다.

$$c_5^{*} = c_5 \oplus h(P \| r_c)$$
$$= h(P \| r_c) \oplus h(P \| r_c') \oplus h(P \| r_c)$$
$$= h(P \| r_c')$$

그리고 계산한 $h(P \| r_c')$를 c_4와 연산하여 $h(c_1) \oplus r_s$를 계산한다.

$$c_4^{*} = c_4 \oplus h(P \| r_c')$$
$$= h(c_1) \oplus h(P \| r_c') \oplus r_s \oplus h(P \| r_c')$$
$$= h(c_1) \oplus r_s$$

공격자는 임의로 생성한 검증자와 길이가 같은 해시함수 값 $h(A)$를 이용하여, 이전에 계산한 $h(c_1) \oplus r_s$와 훔친 검증자인 $h(P \| r_c)$를 이용하여 다음과 같이 새로운 값인 c_{A4}, c_{A5}를 생성한다.

$$c_{A4} = h(c_1) \oplus r_s \oplus h(A)$$
$$c_{A5} = h(P \| r_c) \oplus h(A)$$

c_{A4}, c_{A5}를 전송받은 서버에서는 다음과 같은 검증 과정을 수행한다.

$$c_{A4}' = c_{A4} \oplus h(c_1) \oplus r_s$$
$$= h(c_1) \oplus r_s \oplus h(A) \oplus h(c_1) \oplus r_s$$
$$= h(A)$$

$$c_{A5}' = c_{A5} \oplus h(P \| r_c)$$
$$= h(P \| r_c) \oplus h(A) \oplus h(P \| r_c)$$
$$= h(A)$$

이 후 각각 구한 $h(A)$에 대한 무결성을 검증한 후, 다음 세션을 위한 검증자를 $h(A)$로 업데이트 하게 된다. 따라서 훔친 검증자 공격을 통하여, 다음 세션에 직접적인 인증을 시도할 수는 없지만 검증자 값을 알 수 없는 값의 검증자인 $h(A)$로 교체하여 인증을 방해할 수 있다.

4. 결론

본 논문에서는 Cho가 제안한 원격 인증스킴의 안전성을 분석하였다. 분석한 결과 DoS 공격과 훔친 검증자 공격을 통해 서버로 하여금 다음 세션의 로그인을 하지 못하도록 하여, 사용자의 로그인 요청을 거부하게 된다. 따라서 Cho가 제안한 원격 인증스킴은 DoS 공격과 훔친 검증자 공격에 대해 취약하다.

Cho의 인증스킴과 같은 해시함수 기반의 인증스킴의 지속적인 연구 및 발전은 공개된 네트워크에서의 암호화 기술의 키 분배 문제를 해결하면서, 간단한 연산으로 안전한 사용자 인증을 수행할 수 있을 것이다. 앞으로 꾸준한 연구를 통해 보다 안전한 인증스킴을 개발할 수 있도록 많은 노력이 필요하다.

참고문헌

[1] D. P. Jablon, "Strong Password Only Authenticated Key Exchange," Computer Communication Review, Vol. 26, No. 5, pp. 5-26, 1996.

[2] J. Botting, "Security on the Internet:Authenticating the User," Telecommunications, Vol. 31, No. 12, pp. 77-80, 1997

[3] S. Halevi, H. Krawczyk, "Public-Key Cryptography and Password Protocols," Proceedings of 5th ACM Conference on Computer and Communications Security, pp. 122-131, 1998.

[4] M. S. Hwang, "Cryptanalysis of remote login authentication scheme," Computer Communications, Vol. 22, No. 8, pp. 742-744, 1999.

[5] L. H. Li, L. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," IEEE Transactions on Neural Networks, Vol. 12, No. 6, pp. 1498-1504, 2001.

[6] M. Peyravian, N. Zunic, "Methods for Protecting Password Transmission," Computer Security, Vol. 19, No 5, pp. 466-469, 2000.

[7] C. C. Lee, L. H. Lee, and M. S. Hwang, "A remote User Authentication Scheme Using Hash Functions," ACM Operating Systems Review, Vol. 36, No. 4, pp. 23-29, 2002.

[8] 조성제. "Lee-Hwang의 원격 인증스킴 개선방안," 한국정보기술학회논문지, 제 8권, 6호, 2010년