제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

Sood 등이 제안한 동적 ID 기반 인증 스킴에 대한 보안 취약점 분석

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

Security Vulnerability Analysis for Dynamic Identity-Based Authentication Scheme Proposed by Sood et al.

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

요 약

2010년 Sood 등은 Wang 등의 인증 스킴이 여러 가지 보안 취약점을 가지고 있는 것을 지적하며 안전한 동적 ID 기반 인증 스킴을 제안하였다. 그러나 Sood 등이 제안한 동적 ID 기반 인증 스킴은 공격자가 통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 공개정보를 바꿈으로써 정당치 않은 세션 키가 생성되기 때문에 중간자 공격에 대한 취약성을 가지고 있다. 따라서 본 논문에서는 Sood 등이 제안한 동적 ID 기반 인증 스킴을 분석하고, Sood 등의 인증 스킴이 중간자 공격에 안전하지 못함을 증명한다.

1. 서론

패스워드는 스마트카드 기반 인증 프로토콜에서 가장 널리 사용되는 인증 기술이다. 1981년 Lamport는 안전하지 않은 통신 채널 상에서 원격 사용자를 인증하기 위한 패스워드 기반 인증 스킴을 제안하였다[1]. Lamport의 스킴은 패스워드 테이블 공개 및 통신 도청의 문제를 제거하였고 이 후 보안, 효율성, 비용을 향상시키기 위해 정적 ID 기반 원격 사용자 인증 스킴이 제안되었다. 그러나 정적 ID 기반 원격 사용자 인증 스킴은 인증 단계에서 사용자의 인증 메시지에 대한 부분적인 정보가 공격자에게 유출되는 문제점이 있다. 반면, 정적 ID 기반 인증 스킴에 대한 문제점을 해결하기 위해 ID 및 패스워드에 기반한 다중 인증을 제공하는 동적 ID 기반 인증 스킴이 제안되었다. 이에 따라 2004년 Das 등은 사용자의 익명성을 보장하여 사용자를 인증할 수 있는 동적 ID 기반 원격 사용자 인증 스킴을 제안하였다[2]. Das 등은 그들의 인증 스킴이 재전송 공격, 위장 공격, 오프라인 패스워드 추측 공격, 내부자 및 훔친 검증자 공격, 위조 공격에 안전하다고 주장하였다.

그러나 많은 연구들은 Das 등의 인증 스킴이 여러 가지 공격에 취약하다는 것을 증명하였다[3-8]. 2005년 Chien과 Chen은 Das 등의 인증 스킴에서 같은 사용자가 인증 메시지들 식별할 수 있기 때문에 효과적으로 사용자 익명성을 보장할 수 없다는 것을 지적하며, 조금 더 효과적으로 사용자의 익명성을 보장할 수 있는 인증 스킴을 제안하였다[3]. 2005년 Liao 등은 Das 등의 인증 스킴에 대한 보안성을 강화하여 상호 인증을 제공하는 인증 스킴을 제안하였다[4]. 그러나 2006년 Yoon과 Yoo는 Liao 등의 인증 스킴이 반사 공격과 내부자 공격에 취약하다는 것을 지적하며, Liao 등의 인증 스킴의 보안 결점을 제거한 개선된 동적 ID 기반 상호 인증 스킴을 제안하였다[5].

2006년 Liou 등은 스마트카드를 이용한 새로운 동적 ID 기반 원격 사용자 인증 스킴을 제안하였지만[6], 2008년 Shih는 Liou 등의 인증 스킴이 상호 인증을 달성할 수 없다는 것을 증명하였다[7]. 2009년 Wang 등은 Das 등의 인증 스킴이 합법적인 사용자의 스마트카드를 획득하고 임의의 패스워드를 선택하는 경우 훔친 스마트카드 공격에 취약하다는 것을 지적하며, Das 등의 인증 스킴을 개선한 동적 ID 기반 인증 스킴을 제안하였다[8]. 2010년 Sood 등은 Wang 등의 인증 스킴이 위장 공격, 훔친 스마트카드 공격, 오프라인 패스워드 추측 공격에 대한 취약성을 지적하며, 이러한 문제들을 해결하기 위해 안전한 동적 ID 기반 인증 스킴을 제안하였다[9]. 그러나 Sood 등이 제안한 동적 ID 기반 인증 스킴은 공격자가 통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 공개정보를 바꿈으로써 정당치 않은 세션 키가 생성되기 때문에 중간자 공격에 대한 취약성을 가지고 있다. 따라서 본 논문에서는 Sood 등의 인증 스킴이 중간자 공격에 안전하지 못함을 증명한다.

본 논문의 구성은 다음과 같다. 2장에서는 Sood 등이

제안한 동적 ID 기반 인증 스킴을 분석하고, 3장에서는 Sood 등의 인증 스킴이 중간자 공격에 안전하지 못함을 증명한다. 마지막으로 4장에서는 결론을 맺는다.

2. Sood 등의 동적 ID 기반 인증 스킴 분석

본 장에서는 Sood 등이 제안한 동적 ID 기반 인증 스킴에 대하여 분석한다. <표 1>은 Sood 등이 제안한 동적 ID 기반 인증 스킴에서 사용하는 시스템 파라미터를 나타낸다. (그림 1)은 등록 단계이고, (그림 2)는 로그인 및 검증 단계이다.

<표 1> 시스템 파라미터

기호	의미
U_i	i번째 사용자
S	서버
A	공격자
ID_i	사용자 U_i의 식별자
P_i	사용자 U_i의 패스워드
x	서버의 비밀키
y_i	사용자 U_i의 랜덤 값
T	타임스탬프
$\oplus$	배타적 논리합 연산
$\|\|$	연접 연산
$h()$	일방향 해시 함수
$A \rightarrow B: X$	X가 A에서 B로 전송

2.1 등록 단계

① $U_i \rightarrow S: \{ID_i, P_i\}$

사용자 U_i가 서버 S에 등록을 하기 위해 안전한 통신 채널을 통하여 자신의 식별자 ID_i와 패스워드 P_i를 전송한다.

② 서버 S는 랜덤 값 y_i를 선택하여 다음의 보안 파라미터를 계산한다.

$N_i=h(ID_i||P_i)\oplus h(x)$

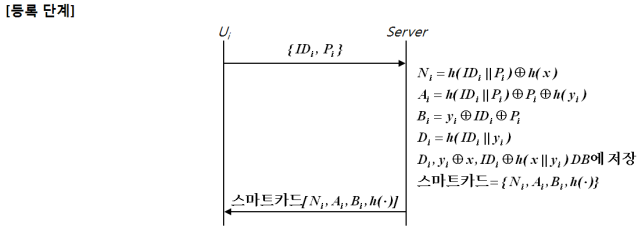
$A_i=h(ID_i||P_i)\oplus P_i \oplus h(y_i)$

$B_i=y_i \oplus ID_i \oplus P_i$

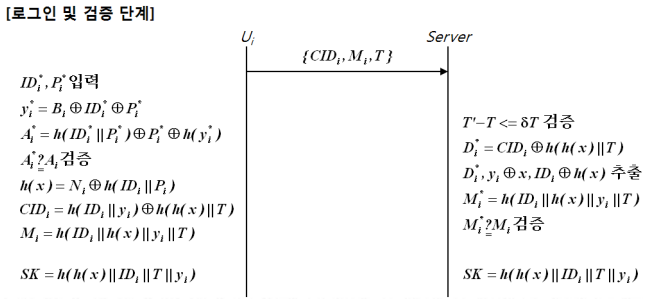
$D_i=h(ID_i||y_i)$

③ $S \rightarrow U_i: \{$스마트카드$[N_i, A_i, B_i, h(\cdot)]\}$

서버 S는 $y_i \oplus x$, $ID_i \oplus h(x)$를 계산하여 자신의 데이터베이스에 D_i와 같이 저장한다. 이 후 스마트카드 내에 보안



(그림 1) 등록 단계



(그림 2) 로그인 및 검증 단계

파라미터 N_i, A_i, B_i, $h(\cdot)$를 저장한 후 안전한 통신 채널을 통하여 사용자 U_i에게 스마트카드를 발행한다.

2.2 로그인 단계

① 사용자 U_i는 서버 S로부터 로그인하기 위해 카드 리더기에 스마트카드를 삽입하고, 자신의 식별자 ID_i^*와 패스워드 P_i^*를 입력하여 스마트카드에 전송한다. 스마트카드는 다음과 같이 y_i^*를 계산한 후 스마트카드 내에 있는 A_i와 계산한 A_i^*를 비교하여 무결성을 검증한다.

$y_i^*=B_i \oplus ID_i^* \oplus P_i^*$

$A_i^*=h(ID_i^*||P_i^*) \oplus P_i^* \oplus h(y_i^*)$

$A_i^*?=A_i$

② $U_i \rightarrow S: \{CID_i, M_i, T\}$

검증이 완료되면 스마트카드는 다음을 계산한 후 서버 S에 서비스를 제공받기 위해 서버 S에게 로그인 요청 메시지 $\{CID_i, M_i, T\}$를 전송한다.

$h(x)=N_i \oplus h(ID_i||P_i)$

$CID_i=h(ID_i||y_i) \oplus h(h(x)||T)$

$M_i=h(ID_i||h(x)||y_i||T)$

2.3 검증 및 세션 키 동의 단계

① 사용자 U_i로부터 로그인 요청 메시지를 수신받은 후 서버 S는 타임스탬프 T의 유효성을 검사한다. 타임스탬프 T의 유효성이 검증되면 서버 S는 $D_i^*=CID_i \oplus h(h(x)||T)$를 계산한 후 데이터베이스 내에서 D_i^*와 동일한 D_i를 검색하고, 데이터베이스 내에서 D_i와 같이 저장되어 있는 $y_i \oplus x$, $ID_i \oplus h(x)$를 찾는다. 서버 S는 $y_i \oplus x$, $ID_i \oplus h(x)$를 이용하여 다음과 같이 M_i^*를 계산한 후 전송받은 M_i와 계산한 M_i^*를 비교하여 무결성을 검증한다.

$M_i^*=h(ID_i||h(x)||y_i||T)$

$M_i^*?=M_i$

② M_i에 대한 무결성이 검증되면 서버 S는 사용자 U_i를 인증한다. 인증이 완료된 후 사용자 U_i와 서버 S는 $h(h(x)||ID_i||T||y_i)$를 계산하여 공통의 세션 키를 확립한다.

2.4 패스워드 변경 단계

① 사용자 U_i는 패스워드를 변경하기 위해 카드 리더기에 스마트카드를 삽입하고 자신의 식별자 ID_i^*와 패스워드 P_i^*를 입력하여 스마트카드에 전송한다. 스마트카드는 다음과 같이 y_i^*를 계산한 후 스마트카드 내에 있는 A_i와 계산한 A_i^*를 비교하여 무결성을 검증한다.

$y_i^*=B_i \oplus ID_i^* \oplus P_i^*$

$A_i^*=h(ID_i^*||P_i^*) \oplus P_i^* \oplus h(y_i^*)$

$A_i^*?=A_i$

② 검증이 완료되면 새로운 패스워드 P_i^{new}를 입력하여 스마트카드에 전송하고 스마트카드는 다음을 계산한 후 스마트카드 내에 있는 N_i, A_i, B_i를 N_i^{new}, A_i^{new}, B_i^{new}로 각각 업데이트한다.

$N_i^{new}=N_i \oplus h(ID_i||P_i) \oplus (ID_i||P_i^{new})$

$A_i^{new}=h(ID_i||P_i^{new}) \oplus P_i^{new} \oplus h(y_i)$

$B_i^{new}=y_i \oplus ID_i \oplus P_i^{new}$

3. 보안 취약점 분석

본 장에서는 Sood 등이 제안한 동적 ID 기반 인증 스킴이 중간자 공격에 안전하지 않음을 보인다. 공격자 A는 서버 S에 등록되어 있는 정당한 사용자로서 자신의 스마트카드 내에서 계산되는 y_A, $h(x)$를 추출할 수 있는 것으로 가정한다.

사용자 U_B가 서버 S로부터 로그인을 하는 동안 공격자 A는 사용자 U_B가 서버 S로부터 전송하는 로그인 요청 메시지 $\{CID_B, M_B, T\}$를 차단하고 복사한다. 공격자 A는 추출한 y_A, $h(x)$와 ID_A, T를 이용하여 다음과 같이 CID_A와 M_A를 계산한 후 로그인 요청 메시지 $\{CID_B, M_B, T\}$를 $\{CID_A, M_A, T\}$로 교환하여 전송한다.

$CID_A=h(ID_A||y_A) \oplus h(h(x)||T)$

$M_A=h(ID_A||h(x)||y_A||T)$

로그인 요청 메시지 $\{CID_A, M_A, T\}$를 수신받은 후 서버 S는 타임스탬프 T의 유효성을 검사한다. 타임스탬프 T의 유효성이 검증되기 때문에 서버 S는 $D_A^*=CID_A \oplus h(h(x)||T)$를 계산한 후 데이터베이스 내에서 D_A^*와 동일한 D_A를 검색하고, 데이터베이스 내에서 D_A와 같이 저장되어 있는 $y_A \oplus x$, $ID_A \oplus h(x)$를 찾는다. 서버 S는 다음과 같이 M_A^*를 계산한 후 전송받은 M_A와 계산한 M_A^*를 비교하여 무결성을 검증한다.

$M_A^*=h(ID_A||h(x)||y_A||T)$

$M_A^*?=M_A$

M_A에 대한 무결성이 검증되기 때문에 서버 S는 사용자 U_B를 인증한다. 인증이 완료된 후 사용자 U_B와 서버 S는 다음과 같이 세션 키를 확립한다.

$SK_{U_B}=h(h(x)||ID_B||T||y_B)$

$SK_S=h(h(x)||ID_A||T||y_A)$

공격자 A가 위와 같이 공격을 수행할 경우 사용자 U_B와 서버 S가 계산한 세션 키는 서로 다르기 때문에 메시지가 변경된 것을 알지 못하고 정당치 않은 세션 키를 올바른 세션 키로 신뢰하게 된다. 따라서 Sood 등이 제안한 동적 ID 기반 인증 스킴은 중간자 공격에 취약하다.

4. 결론

본 논문에서는 Sood 등이 제안한 동적 ID 기반 인증 스킴에 대한 안전성을 분석하였다. 분석한 결과 Sood 등이 제안한 동적 ID 기반 인증 스킴은 공격자가 통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 공개정보를 바꿈으로써 정당치 않은 세션 키가 생성되기 때문에 중간자 공격에 취약하다.

참고문헌

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

[2] M. L. Das, A. Saxena, and V. P. Gulati, “A Dynamic ID-based Remote User Authentication Scheme,” IEEE Transactions on Consumer Electronics, Vol. 50, no. 2, pp. 629-631, May 2004.

[3] H. Y. Chien and C. H. Chen, “A Remote Authentication Scheme Preserving User Anonymity,” Proc. Advanced Information Networking and Applications, Vol. 2, pp. 245-248, Mar. 2005.

[4] I. E. Liao, C. C. Lee, and M. S. Hwang, “Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme,” Proc. Next Generation Web Services Practices, pp. 437-440, Jul. 2005.

[5] E. J. Yoon and K. Y. Yoo “Improving the Dynamic ID-Based Remote Mutual Authentication Scheme,” Proc. OTM Workshops 2006, pp. 499-507, Jul. 2006.

[6] Y. P. Liou, J. Lin, and S. S. Wang, “An New Dynamic ID-Based Remote User Authentication Scheme Using Smart Cards,” Proc. 16th Information Security Conference, pp. 198-205, Jul. 2006.

[7] H. C. Shih, “Cryptanalysis on Two Password Authentication Schemes,” Laboratory of Cryptography and Information Security, Jul. 2008.

[8] Y. Y. Wang, J. Y. Liu, F. X. Xiao, and J. Dan, “A more efficient and secure dynamic ID-based remote user authentication scheme,” Computer Communications, Vol. 32, no. 4, pp. 583-585, Mar. 2009.

[9] S. K. Sood, A. K. Sarje, and K. Singh, “An Improvement of Wang et al.'s Authentication Scheme Using Smart Cards,” 2010 National Conference on Communications, Jan. 2010.