스마트카드를 이용한 향상된 동적 ID기반 원격 사용자 인증 기술

Improved Dynamic ID-based Remote User Authentication Scheme Using Smartcards

심 희 원* 박 준 형** 노 봉 남***
Hee-Won Shim Joonn-Hyung Park Bong-Nam Noh

요 약

원격 사용자 인증기술 중 패스워드에 기반을 둔 기술은 아직도 가장 보편적으로 사용되고 있는 인증 기술이다. 2004년 Das 등이 제안한 "동적 ID 기반의 원격 사용자 인증기술"은 스마트카드의 연산 기능을 이용하여 패스워드를 생성하고, 원격 시스템에서는 연산량이 적은 해쉬와 XOR만으로 인증을 수행할 수 있는 안전한 인증기법이다. 이 기법은 동적 ID 채용으로 ID도난을 방지하며, 인증시각을 이용하여 재사용 공격을 방지하는 특징이 있다. 그 밖에도 많은 공격에 대응할 수 있도록 고안되었다. 하지만, 이 기법은 후에 패스워드와 관계없이 원격 시스템에 인증이 가능한 치명적인 오류 뿐 아니라, 위장공격, 추측공격에 취약함이 밝혀졌다. 더욱이 인증 시각 정보를 이용하여 재사용 공격을 막은 기능도 최근의 실시간으로 이루어지는 재사용 공격에는 취약함을 보이고 있다. 본 논문에서는 Das 기법이 실시간 재사용공격에 취약한 점을 증명하고, 매번 변경되는 인증횟수를 이용하여 이를 개선하는 향상된 인증기법을 제안하였다. 향상된 인증기법은 기존 Das 기법이 가지는 장점을 그대로 계승하며, 추측공격, 위장공격, 실시간 재사용 공격에 대응하고, 상호인증 기능을 제공한다.

Abstract

Among the remote user authentication schemes, password-based authentication methods are the most widely used. In 2004, Das et al. proposed a "Dynamic ID Based Remote User Authentication Scheme" that is the password based scheme with smart-cards, and is the light-weight technique using only one-way hash algorithm and XOR calculation. This scheme adopts a dynamic ID that protects against ID-theft attack, and can resist replay attack with timestamp features. Later, many flaws of this scheme were founded that it allows any passwords to be authenticated, and can be vulnerable to impersonation attack, and guessing attack. By this reason many modifications were announced. These scheme including all modifications are similarly maintained security against replay the authentication message attack by the timestamp. But, if advisory can replay the login immediately, this attempt can be succeeded. In this paper, we analyze the security vulnerabilities of Das scheme, and propose improved scheme which can resist on real-time replay attack using the counter of authentication. Besides our scheme still secure against impersonation attack, guessing attack, and also provides mutual authentication feature.

☞ keyword : 스마트카드(Smartcard), 동적ID(Dynamic ID), 인증(Authentication), 상호인증(Mutual Authentication), 실시간재사용(realtime replay)

1. 서 론

오늘날과 같이 네트워크 기반의 많은 원격 서비스를 제공하는 시스템 자원에 접근하기 위해서는 원격 사용자 인증기술이 필수적이다. 1981년 Lamport[1]가 제안한 원격사용자 인증 기법을 시작으로 현재까지 수많은 인증기법들이 제안되어 왔으며, 이러한 인증기법들은 대부분 2가지 형태

* 정 회 원 : 전남대학교 일반대학원 정보보호협동(박사과정)
hwshim@hotmail.com
** 정 회 원 : 전남대학교 시스템보안연구센터 디지털포렌식팀
vulcan@hanmail.net
*** 정 회 원 : 전남대학교 전자컴퓨터정보통신공학부 교수
bongnam@jnu.ac.kr
[2008/10/29 투고 - 2008/10/30 심사(2009/01/08 2차) - 2009/02/16 심사완료]

로 구분될 수 있다. 첫째는 비교적 약한 패스워드를 사용하는 기법이며, 둘째는 강한 패스워드를 사용하는 기법이다. 약한 패스워드를 사용하는 인증기법은 공개키 기반의 암호학적 연산을 사용하여 안전성을 보장한다. 이러한 기법의 장점은 원격 시스템에 검증 테이블을 보관할 필요가 없이, 암호학적 연산에 의해 인증이 되므로 안전하며, 패스워드를 기억하기 쉽다는 점이다. 반대로 단점은 공개키 암호화 연산으로 인해 원격 시스템의 부하가 높아진다[2,3,4,5].

반면에 강한 패스워드 인증기법은 대부분 일방향 해쉬 또는 XOR 연산을 통해 수행되기 때문에 구축비용이 상대적으로 저렴한 장점을 가진다. 더욱이 기존 원격시스템을 대체하는 경우에는 단순히 패스워드만을 대체하여 보다 쉽게 구현이 가능하다[5,6,7,8].

초기에 제안된 패스워드 인증기법은 검증 테이블을 기반하여 인증을 수행한다[1]. 이러한 경우, 공격자가 원격 시스템에 직접 침투하여 검증 테이블을 취득하게 되는 경우, 전체 시스템 사용자의 패스워드가 노출되는 파급효과를 가지게 된다. 더욱이 대부분의 사용자는 다른 원격 시스템에 접근하기 위해서도 동일한 패스워드를 사용하므로, 항상 패스워드 도난 공격에 노출될 것을 우려하여야 한다. 2004년 Das-Saxena-Gulati 3인은(이후, Das로 표기) 패스워드 검증 테이블 인증기법을 보완하여, 스마트카드를 이용한 원격 사용자 인증기법을 제안하였다[9]. 이 기법은 사용자가 자유롭게 패스워드를 선택하고, 변경할 수 있으며 검증 테이블을 이용하지도 않는다. 또한, 이 기법은 매번 변경되는 동적 ID를 채용하여 ID 도난공격에 대응하였으며, 패스워드 테이블 노출 공격, 재사용 공격, 위장공격, 추측 공격, 내부자 공격 등에 안전하게 고안되었다. 하지만 이 기법은 이후에 Wei-Chi Ku에 의해 패스워드와 관계없이 원격 시스템에 인증이 가능한 치명적인 오류가 있음이 증명되었다[10]. 이러한 결점은 그 이후에 여러 연구들에 의해 문제점이 보완되어 왔다[11,12,13].

하지만, Das의 기법 뿐 아니라 보완된 모든 인증기법의 가장 큰 문제점은 전송되는 시각 정보만을 이용하여 재사용 공격에 대응한 점이다. 즉, 패스워드가 사용되는 시점의 시각정보를 비밀정보와 연산하여, 원격 시스템에서 검증하는 시점의 시각과 현저하게 차이가 나면 인증을 중단하는 방식인데, 문제점은 공격자가 허용된 검증시각 내에 공격을 수행한다면 인증이 성공된다는 점이다.

본 논문에서는 Das 기법이 실시간 재사용공격에 취약한 점을 개선할 수 있도록 시각정보와 함께 매번 변경되는 인증횟수를 이용한 새로운 인증기법을 제안할 것이다. 또한 향상된 인증기법은 추측공격, 위장공격에 대응할 수 있으며, 대부분의 인증 시스템에서 필수적으로 요구되는 상호인증을 제공한다. 그리고 제안된 인증기법은 Das 기법의 장점을 그대로 계승하여 검증 테이블을 유지하지 않아 패스워드 도난 공격에 대응할 수 있다.

본 논문은 다음과 같이 구성된다. 1장은 본 장으로 서론이며, 2장은 Das의 인증기법에 대한 내용을 검토한다. 3장은 해당 기법의 보안 취약성을 확인하며, 4장에서는 새로운 인증기법을 제시한다. 5장에서는 제안된 기법의 보안성에 대한 분석 및 기존연구와의 비교를 하고, 6장에서 결론으로 끝을 맺는다.

2. Das 인증기법 검토

Das 인증기법은 등록, 인증, 패스워드 변경의 3가지 단계로 구성된다. 등록단계는 안전한 통신을 통해 최초 1회만 수행되며, 인증단계는 시스템에 접근할 때마다 수행된다. 표기법은 Das 인증기법의 것을 그대로 사용한다.

U	사용자
PW	U의 패스워드
S	원격 시스템
$h(.)$	일방향 해쉬 연산
$\oplus$	비트단위의 XOR 연산
$A \Rightarrow B: M$	안전한 통신을 통해 A가 B에게 M을 송신
$A \rightarrow B: M$	일반 통신을 통해 A가 B에게 M을 송신

2.1 등록단계

이 단계에서는 U_i가 PW_i를 선택하여 S에게 안전하게 전달하고, S는 다음과 같은 단계를 통해 등록한 스마트카드를 사용자에게 전달한다.

R1.$N_i=h(PWi)\oplus h(x)$를 연산한다. (x는 S의 비밀키)

R2.등록된 사용자의 스마트카드에 $h(.), N_i, y$를 저장한다. (y는 S의 비밀키)

R3.$S \Rightarrow U_i$: $(PW_i$, 스마트카드$)$

2.2 인증단계

이 단계에서는 U_i가 S에 로긴하기 위해 메시지를 송신하는 단계와, S가 로긴 메시지를 송신하여 검증하는 단계로 구분한다.

로긴단계에서 사용자 U_i는 스마트카드를 리더기에 삽입하고, PW_i를 입력하면, 스마트카드는 다음을 연산한다.

L1.$CID_i=h(PW_i)\oplus h(N_i\oplus y\oplus T)$를 연산한다. ($T$는 U_i의 시스템의 현재 시각)

L2.$B_i=h(CID_i\oplus h(PW_i))$를 연산한다.

L3.$C_i=h(T\oplus N_i\oplus B_i\oplus y)$를 연산한다.

L4.$U_i \rightarrow S$: (CID_i, N_i, C_i, T)

검증단계에서 S는 U_i로부터 (CID_i, N_i, C_i, T)를 전달받은 시각 T^*를 구하고, 다음을 연산하여 사용자를 인증한다.

V1.만약 $(T^*-T\geq \Delta T)$이면 인증을 거부한다. (ΔT는 전송시간을 고려한 최소 인증시간)

V2.$h(PW_i)=CID_i\oplus h(N_i\oplus y\oplus T)$를 연산한다.

V3.$B_i=h(CID_i\oplus h(PW_i))$를 연산하고, $C_i=h(T\oplus N_i\oplus B_i\oplus y)$를 연산하여, 전송된 C_i와 같은지 비교한다. 만약 같지 않으면 인증을 거부한다.

2.3 패스워드 변경단계

U_i가 패스워드를 변경하고자 하는 경우, 다음과 같이 패스워드를 변경할 수 있다.

C1.U_i는 스마트카드를 리더기에 삽입하고, PW_i를 입력하여, 패스워드 변경을 요청한다.

C2.새로운 PW_i^*를 선택한다.

C3.사용자의 스마트카드에서는 다음을 연산한다.

$$Ni^* = N_i\oplus h(PW_i)\oplus h(PW_i^*) = h(PW_i^*)\oplus h(x)$$

C4.S에 안전하게 N_i^*를 전달하여, N_i와 교체한다.

3. Das 기법의 보안 취약성 분석

실시간 재사용공격: Das 기법 및 이를 수정한 기법들의 가장 큰 특징은 시각차(ΔT)를 이용하여 재사용 공격에 대응하도록 한 것이다. 그러나, 최근의 공격은 실시간으로 이루어지고 있으므로 인증이 이루어지는 시점과 공격이 이루어지는 시점에 시간차가 있다는 가정이 항상 옳지는 않다. 즉, 공격자는 사용자의 PC를 수시로 모니터링하며, 로긴 메시지를 송신하는 동시에 해당 메시지를 수집하고, 원격시스템에 접속한다. 스니핑 등을 통해 (CID_i, N_i, C_i, T)를 모두 재사용할 수 있으며, $(T^*-T\geq \Delta T)$이므로 검증이 성공된다. 이러한 공격은 중간자 공격과 결합되어 수행되며 실제 성공 가능하다[14].

위장공격: Das 기법의 가장 큰 결점은 검증단계의 마지막에서 사용되는 인증과정에 사용자의 패스워드가 사용되지 않는다는 점이다[10]. 따라서, 스마트카드를 취득한 공격자에 의해 패스워드와 관계없이 원격 시스템에 올바른 사용자로 위장하여 접근이 가능하다는 치명적인 결함을 가지고 있다. 또한, 공격자가 로긴메시지(CID_i, N_i, C_i, T)를 가로챈 경우, 일정시간이 흐른 이후에도 공격자는 $(CID_i, N_i\oplus T\oplus T^{**}, C_i, T^{**})$를 통해 정당한 사용자로 위장하여 원격 시스템에 접근할 수 있는 위장공격이 가능하다[12]. (T^{**}는 임의의 시간)

추측공격: 공격자가 자신의 스마트카드와 $h(PW_i)$를 통해 $h(x)(=h(PW_i)\oplus N_i)$를 구하고, 동일 시간의 다른 사용자의 로긴메시지$(CID_i^*, N_i^*, Ci^*, T)$를 가로챈 경우, $h(GuessPW_i)\oplus N_i^*$를 연산하여 $h(x)$와 같은지 비교하는 오프라인 공격이 가능하다. 패스워드는 보통 작은 크기의 의미 있는 값으

로 구성되므로 충분히 연산 가능한 공격이다[11].

피싱: S는 U_i에 대한 인증이 가능하지만, U_i는 S에 대한 인증이 불가능하다. 피싱 등으로 의해 S를 가장하여 U_i의 로긴메시지 및 개인정보를 수집하는 것이 가능하다. 물론 수집된 로긴메시지는 일정 시간동안만 유효하다.

4. 향상된 인증기법

제안하는 향상된 인증기법의 기본적인 방식은 Das의 방식을 유지하여, 장점을 그대로 계승하도록 고안하였다.

향상된 인증기법은 Das 기법과 동일하게 등록, 인증, 패스워드 변경의 3단계로 동작한다. 표기법도 Das 표기법을 준용하되, 향상된 인증을 위해 다음과 같이 원격 시스템에서 인증시마다 수시로 변경되는 임시 검색 테이블을 추가하였다.

$TAB(N:K)$	사용자가 요청하는 N에 대응하는 임의의 수 K를 찾을 수 있는 S의 임시 검색 테이블

4.1 등록단계

이 단계에서는 U_i는 PW_i를 선택하고, $h(PW_i)$를 연산하여 S에게 안전하게 전달한다. S는 다음과 같은 단계를 통해 등록한 스마트카드를 사용자에게 전달한다.

R1.S는 U_i에 대응하는 임의의 수 K_i를 생성한다. (K_i는 충분히 커서 충돌 및 추측에 대응 가능)

R2.$N_i=h(h(PW_i)\oplus y\oplus K_i)$를 연산한다. ($y$는 S의 비밀키)

R3.$TAB(N_i:K_i)$ 데이터 열을 생성한다.

R4.등록된 사용자의 스마트카드에 $h(.)$, K_i, y를 저장한다. (y는 S의 비밀키)

R5.S$\Rightarrow U_i$: (PW_i, 스마트카드)

4.2 인증단계

이 단계에서는 U가 스마트카드를 이용하여 로긴메시지를 생성하고 전송하는 로긴단계와 S가 로긴메시지를 검증하여 사용자의 인증 여부를 결정하는 단계, 그리고 재차 U가 S를 인증하는 서버인증단계로 구분된다.

로긴단계에서 사용자 U_i는 스마트카드를 리더기에 삽입하고, PW_i를 입력하면, 스마트카드는 다음을 연산한다.

L1.$N_i=h(h(PW_i)\oplus y\oplus K_i)$를 연산한다.

L2.$CID_i=h(PW_i)\oplus h(N_i\oplus T\oplus y\oplus K_i)$를 연산한다. ($T$는 U_i의 시스템의 현재 시각)

L3.$C_i=h(CID_i\oplus N_i\oplus T\oplus y\oplus K_i)$를 연산한다.

L4.$U_i\rightarrow S$: (CID_i, N_i, C_i, T)

사용자인증단계에서 S는 U_i로부터 (CID_i, N_i, C_i, T)를 전달받고, 현재 시각 T^*를 구하여, 다음과 같은 방식으로 사용자를 인증한다.

V1.만약 ($T^*-T\geq\Delta T$)이면 인증을 거부한다. (ΔT는 전송시간을 고려한 최소 인증시간)

V2.$TAB(N_i:K_i)$에서 N_i에 해당하는 K_i를 찾는다. (찾지 못하면 종료)

V3.$h(PW_i)=CID_i\oplus h(N_i\oplus T\oplus y\oplus K_i)$를 연산한다.

V4.$N_i=h(h(PW_i)\oplus y\oplus K_i)$를 연산하고, 전송된 N_i와 동일한지 확인한다. (틀리면 종료)

V5.$C_i=h(CID_i\oplus N_i\oplus T\oplus y\oplus K_i)$를 연산하고, 전송된 Ci와 동일한지 확인한다. (틀리면 종료)

V6.$A_i=h(h(PW_i)\oplus T^*\oplus y\oplus(K_i+1))$를 연산한다. ($T$*는 S 시스템의 현재 시각)

V7.$S\rightarrow U_i$: (A_i, T^*)

V8.N_i*$=h(h(PW_i^*)\oplus y\oplus(K_i+2))$를 연산하고, $TAB(N_i:K_i)$를 $TAB(N_i^*:(K_i+2))$로 갱신한다[1].

서버인증단계에서 U_i는 S로부터 (A_i, T^*)를 전달받고, 현재 시각 T^{**}를 구하여, 스마트카드에게 안

1) K_i를 2증가시키는 대신 1증가 시킨다면, 패스워드 변경시 서비스 거부 공격이 발생할 수 있다. 즉, 공격자는 U_i의 시스템 시각을 0으로 변경하고, C18단계에서 S를 가장하여, U_i에게 (A_i^*, T^*) 대신, (N_i^*, 0)를 전송한다면, 이후의 인증은 모두 실패하므로, (K_i+2)로 갱신하여 이를 방지한다.

전하게 전달한다. 스마트카드는 다음과 같은 방식으로 서버를 인증한다.

V9.만약 $(T^{**}-T^{*} \geq \Delta T)$이면 인증을 거부한다. $(\Delta T$는 전송시간을 고려한 최소 인증시간)

V10.$A_i=h(h(PW_i) \oplus T^{*} \oplus y \oplus (K_i+1))$를 연산하고, 전송 된 A_i와 동일한지 확인한다. (틀리면 종료)

V11.모든 과정이 성공한 경우에는 스마트카드에 K_i를 (K_i+2)로 갱신하여 저장한다. (만약 $K+2$가 저장 가능한 수의 범위를 벗어나는 경우에는 0부터 재시작함)

4.3 패스워드 변경단계

패스워드 변경단계는 기본적으로 인증단계의 연산방식을 이용하여 수행하되, 변경된 패스워드를 추가한다. 즉, 사용자 U_i는 스마트카드를 리더기에 삽입하고, 다음을 연산한다.

C1~3. L1~3.인증단계와 동일

C4.새로운 패스워드 PW_i^{*}를 선택한다.

C5.$CID_i^{*}=h(PW_i^{*}) \oplus h(N_i \oplus T \oplus y \oplus (K_i+2))$를 연산한다.

C6.$N_i^{*}=h(h(PW_i^{*}) \oplus y \oplus (K_i+2))$을 연산한다.

C7.$U_i \rightarrow S$: $(CID_i, N_i, C_i, T, CID_i^{*}, N_i^{*})$

U_i로부터 $(CID_i, N_i, C_i, T, CID_i^{*}, N_i^{*})$를 전달받고, S는 다음과 같이 연산한다.

C8~14. V1~7.인증단계와 동일

C15.$h(PW_i^{*})=CID_i \oplus h(N_i^{*} \oplus T \oplus y \oplus (K_i+2))$를 연산한다.

C16.$N_i^{*}=h(h(PW_i^{*}) \oplus y \oplus (K_i+2))$를 연산하고, 전송된 N_i^{*}과 동일한지 확인한다. (틀리면 종료)

C17.$A_i^{*}=h(h(PW_i^{*}) \oplus T^{*} \oplus y \oplus (K_i+1))$를 연산한다.

(T^{*}는 S 시스템의 현재 시각)

C18.$S \rightarrow U_i$: (A_i^{*}, T^{*})

C19.$TAB(N_i:K_i)$를 $TAB(N_i^{*}:(K_i+2))$로 갱신한다.

재차 U_i는 S로부터 (A_i^{*}, T^{*})를 전달받고, 서버를 인증한다.

V20.만약 $(T^{**}-T^{*} \geq \Delta T)$이면 인증을 거부한다. $(\Delta T$는 전송시간을 고려한 최소 인증시간)

V21.$A_i^{*}=h(h(PW_i^{*}) \oplus T^{*} \oplus y \oplus (K_i+1))$를 연산하고, 전송된 A_i^{*}와 동일한지 확인한다. (틀리면 종료)

V22.모든 과정이 성공한 경우에는 스마트카드에 K_i를 (K_i+2)로 갱신하여 저장한다.

5. 향상된 인증기법 평가

5.1 보안성 분석

본 논문에서 제안된 향상된 인증기법은 다음과 같은 공격에 대응할 수 있다.

실시간 재사용공격: 공격자가 U_i의 로긴메시지 (CID_i, N_i, C_i, T)를 가로채 ΔT안에 S에 실시간으로 접근하더라도, 인증횟수를 나타내는 K_i및 비밀정보 y를 알 수 없으므로 안전하다. 즉, 올바른 사용자가 먼저 인증을 성공한 경우라면, 이미 N_i가 $N_i^{*}(=h(h(PW_i^{*}) \oplus y \oplus (K_i+1)))$로 갱신된 이후라, N_i에 해당하는 검색 테이블의 레코드가 없으므로 접속이 불가능하다. 만약, 올바른 사용자의 접속을 지연시키거나, 접속을 임의로 막는 등의 실시간 중간자 공격을 수행한다면 올바른 사용자가 공격사실을 인지하고 즉각 대응할 수 있어, 보안상의 위협을 감소시킬 수 있다.

ID 도난 및 패스워드 테이블 도난 공격: 향상된 인증 기법은 동적으로 변경되는 CID를 ID로 활용하는 동적 ID의 개념을 계승하므로 익명성을 제공하는데 용이하며, ID 도난 공격에 대응할 수 있다. 또한, 사용자의 패스워드를 내부적으로 보관하지 않으므로 내부자 공격에 대응한다. 물론, 임시 검색 테이블에서 N_i에 해당하는 K_i를 찾을 수 있지만, N_i및 K_i가 인증 성공시마다 수시로 변경되는 값으로 인증 테이블로서 의미 있는 정보가 될 수 없으므로 패스워드 테이블 도난 공격에 대응할 수 있다. 그 밖에도 기존의 Das 기법의 장점을 그대로 계승하며, 패스워드가 노출된 상황에서도 스마트카드에 저장된 K_i, y를 위조할 수 없으므로 위조 공격에 대응한다.

위장공격: 공격자가 올바른 사용자의 로긴메시지(CID_i, N_i, C_i, T)를 가로챈 경우라도, 원격시스템

에서 $C_i(=h(N_i \oplus y \oplus T \oplus K_i \oplus CID_i))$를 검증하기 위해 필요한 2개의 비밀정보인 y와 K_i를 알 수 없기 때문에 인증이 실패하게 된다. 만약, 스마트카드를 공격자가 취득하여 y와 K_i를 이용해 연산할 수 있는 경우에도 $N_i(=h(h(PW_i) \oplus y \oplus K_i)))$를 검증하기 위해 필요한 사용자의 개인정보인 PW_i 역시 일방향 해쉬 함수를 통해 가역 연산이 불가능하므로 위장공격에 대응할 수 있다. 더욱이 K_i는 인증 성공시마다 증가되는 값으로, 이전에 사용된 로긴메시지로는 정당한 사용자로 위장할 수 없도록 원천적인 봉쇄를 한다.

추측공격: 공격자가 U_i의 로긴메시지(CID_i, N_i, C_i, T)를 가로채고, 스마트카드의 $h(.)$를 사용할 수 있는 경우라도 CID_i, N_i, C_i의 모든 로긴메시지가 추측하기 어려운 긴 길이의 비밀정보를 포함하여 해쉬되므로 오프라인 추측공격에 대응할 수 있다. 또한 오프라인 추측공격에 취약한 PW_i의 경우에도 직접 사용되지 않고, 모든 연산에서 $h(PW_i)$로 연산되므로 추측공격에 대응할 수 있다.

상호인증: 향상된 인증 기법은 원격 접속을 위한 사용자의 인증 뿐 아니라, 사용자가 원격 시스템을 인증할 수도 있도록 상호인증을 제공한다. 즉, 서버를 가장한 공격자는 비밀정보 y와 K_i를 알 수 없으므로, $A_i(=h(h(PW_i) \oplus T^* \oplus y \oplus (K_i+1)))$를 올바로 연산할 수 없고, 더욱이 A_i는 K_i에 의해 항상 변경되는 정보이므로 재사용할 수 없다.

5.2 기존 연구와의 비교

향상된 인증기법과 기존 연구와의 차이점에 대해 (표1)과 같이 보안성을 비교하였다. 비교된 보안성은 다음과 같다. (S1)실시간 재사용공격 대응;(S2)동적 ID사용에 의한 ID 도난 방지;(S3)패스워드 테이블 도난 방지;(S4)위조공격 방지;(S5)위장공격 방지;(S6)추측공격 방지;(S7)상호인증 기능 제공

이와 같이 향상된 인증기법은 기존 연구에 비해 실시간 재사용공격에 대응할 뿐 아니라, 기존 연구들이 가지는 보안성을 모두 가진다.

(표 1) 보안성 분석

연구명 [참고문헌]	보안성						
	S1	S2	S3	S4	S5	S6	S7
향상된 기법	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**
Das[1]	no	yes	yes	no	no	no	no
Liao[11]	no	yes	yes	no	no	yes	yes
Misbahuddin[12]	no	no	yes	yes	yes	yes	yes
Gao[13]	no	no	yes	yes	yes	yes	yes

향상된 인증기법의 성능 분석은 (표2)와 같다. XOR는 단순연산으로 성능에 영향을 주지 않으므로, 해쉬연산이 수행된 횟수를 표기하였다.

(표 2) 성능 분석

연구명 [참고문헌]	성능(해쉬연산 횟수)					
	등록단계		인증단계		패스워드 변경	
	U_i	S	U_i	S	U_i	S
향상된 기법	**1**	**1**	**5**	**5**	**9**	**7**
Das[1]	0	2	4	3	2	0
Liao[11]	1	1	5	4	2	0
Misbahuddin[12]	1	1	5	6	-	-
Gao[13]	1	3	5	5	5	0

향상된 인증기법의 해쉬 연산 횟수는 등록단계와 인증단계에서 기존 연구와 동일한 수준을 유지한다. 단, 패스워드 변경단계에서는 기존 연구들에 비해 많은 연산량을 필요로 하지만, 패스워드 변경이 필요한 경우에만 사용되는 기능이므로 전체적인 성능에 큰 영향을 미치지 않는다.

5.3 구현 고려사항

향상된 인증기법을 구현하는 경우에는 다음의 사항을 고려하여 효용성 및 안정성을 높일 수 있다.

검색테이블의 관리: 향상된 인증기법은 임시 검색테이블을 활용하여 인증단계의 보안성을 개선한 반면, 원격서버의 검색테이블이 파손 및 노출되지 않도록 안전하게 관리되어야 한다. 또한, 성능의 향상을 위해 검색테이블을 메모리상에 위치시키는 방법 등으로 조회 및 갱신에 소요되는 시간을 최소화 할 수 있다.

충돌성 고려: PW_i가 동일한 사용자가 우연히

K_i 값도 동일한 상황이 발생하는 경우를 고려하여 원격서버가 구현되어야 한다. 즉, 원격서버의 검색테이블에서는 복수개의 N_i와 K_i 쌍이 존재할 수 있도록 충돌에 대비하여야 한다.

인증정보의 동기화: 성공한 인증횟수인 K_i는 원격서버에서 인증이 성공한 후에 증가되며, 스마트카드는 원격서버가 전송한 A_i를 검증한 이후에 K_i를 증가시킨다. 만약, 원격서버에서 인증이 성공한 후, 통신오류 등에 의해 A_i가 사용자에게 전달되지 않은 경우에는 원격서버와 사용자간의 K_i에 차이가 발생하게 되고, 이후의 인증은 지속적으로 실패하게 된다. 이러한 유사한 문제를 해결하는 사례로서 OTP(일회용 비밀번호)의 동기화 방식[15]을 사용한다면 K_i를 동기화할 수 있다. 즉, 원격서버는 마지막 인증이 성공한 K_i 이후부터 일정 개수의 N_i와 K_i 쌍을 유지하고, 인증시 이를 모두 비교하여 검증하도록 할 수 있다. 추가적으로 사용자와 원격시스템간의 시각은 항상 현재 시각으로 동기화되어야 한다.

최신 보안위협 대응: 향상된 인증기법은 사용자와 원격서버간에 일반적인 통신을 이용한 소지기반의 인증을 제공하는데 효과적이다. 다만, 최근의 피싱(Phishing), 중간자공격(MITMA), 서비스거부공격(DoS) 등에 대응하기 위해서는 추가적으로 메시지인증, 암호화, 전용장비 등의 적절한 보안수단이 제공되어야 추가적인 보안위협으로부터 안전하게 된다.

6. 결 론

본 논문에서는 기존에 제안된 패스워드 인증기법들이 실시간 재사용공격에 공통적으로 취약한 부분을 개선하여, 인증횟수를 이용한 향상된 인증기법을 제안하였다. 제안된 인증기법은 기존의 Das 기법이 가지는 장점을 그대로 계승하여, ID 및 패스워드 테이블 도난 공격에 대응할 수 있으며, 위장공격, 추측공격 등에도 대응 가능하다. 더욱이 상호인증을 제공하여 원격시스템을 가장한 공격도 봉쇄하였다. 그리고 기존 연구들과의 보안성 및 성능 비교를 통해 효용성을 입증하였다.

참 고 문 헌

[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, vol.24, no.11, pp.770-772, 1981.

[2] T. ElGamal, "A public key cryptosystem and signature scheme based on the discrete logarithms", IEEE Trans. on Info. Theory, vol. 31, no.469~472, 1985.

[3] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards", Computers & Security, vol. 18, no.8, pp. 727-733, 1999.

[4] C. C. Yang, R. C. Wang, and T. Y. Chang, "An improvement of the Yang-Shieh password authentication schemes", Applied Mathematics and Computation, vol. 162, pp. 1391-1396, 2005.

[5] Chwei-Shyong Tsai, Cheng-Chi Lee, and Min-Shiang Hwang. "Password Authentication Schemes: Current Status and Key Issues", International Journal of Network Security, Vol.3, No.2, pp.101~115, Sept. 2006.

[6] H. M. Sun, "An Efficient remote user authentication scheme using smartcards", IEEE Trans. on Consumer Electron., vol. 46, no. 4, pp.958-961, Nov. 2000.

[7] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards", ACM Operating Systems Review, vol.36, no.3, pp.46-52, July 2002.

[8] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards", IEEE Trans. on Consumer Electron., vol.49, no.2, pp.414-416, May 2003.

[9] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE

Trans. Consumer Electron., vol. 50, No. 2, pp. 629-631, May 2004.

[10] W. C. KU and S. T. C, "Impersonation attack on a dynamic ID based remote user authentication using smartcards", IEICE Transaction on Communication, vol.e88-b, no.5, May 2005.

[11] I-EN Liao,C.C.Lee,and M.S.Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme", in IEEE CS Press, International Conference on Next Generation WebServicesPractices(NWeSP'05),pp.437-440,Seoul,Korea,August 2005.

[12] Md. Misbahuddin, Md. Aijaz Ahmed, A. Ananda Rao, C. Shoba Bindu, and M.A. Muqsit Khan. "A Novel Dynamic ID-Based Remote User Authentication Scheme". Annual India Conference, pp:1-5,Sept. 2006.

[13] Zhengxian Gao and Yaquing Tu, "An Improvement of Dynamic ID-Based Remote User Authentication Ssheme with Smart Cards", World Congress on Intelligent Control and Automation Proc. 7th, pp25-27,Jun. 2008.

[14] Joel Dubin, "One-time password tokens: Best practices for two-factor authentication", http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1216485,00.html, Sep. 2006.

[15] IETF RFC4226, "HOTP: An HMAC-Based One-Time Password Algorithm", Dec. 2005.

◐ 저 자 소 개 ◑

심 희 원

1998년 단국대학교 전자계산학과(이학사)
2000년 홍익대학교 일반대학원 전자계산학과(이학석사)
2008~현재 전남대학교 일반대학원 정보보호협동(박사과정 재학)
관심분야: PKI, OTP, 네트워크 보안, 암호이론, etc.
E-mail : hwshim@hotmail.com

박 준 형

1999년 2월 아주대학교 수학과(이학사), 정보및컴퓨터공학과(공학사)
2002년 2월 전남대학교 멀티미디어협동(이학석사)
2004년 8월 전남대학교 정보보호협동(이학박사)
2004년 9월 ~ 현재 전남대학교 시스템보안연구센터 디지털포렌식팀
관심분야 : 디지털 포렌식스, 개인정보보호, 봇넷 대응, IT 컴플라이언스
E-mail : vulcan@hanmail.net

노 봉 남

1978년 전남대학교 수학교육학과(이학사)
1982년 KASIT 대학원 전산학과(이학석사)
1994년 전북대학교 일반대학원 전산학과(이학박사)
1983 ~현재 전남대학교 전자컴퓨터정보통신공학부 교수
2000 ~ 현재 시스템보안연구센터 소장
관심분야 : 네트워크 보안, 운영체제 보안, etc.
E-mail : bongnam@jnu.ac.kr