https://doi.org/10.14400/JDC.2017.15.10.253

다중서버를 위한 비-추적성을 제공하는 인증된 키 동의 기법

최해원, 김상진, 류명춘
경운대학교 항공산업보안학과

Untraceable Authenticated Key Agreement Scheme for Multi-server Environment

Hae-Won Choi, Sangjin Kim, Myungchun Ryoo
Department of Aerospace & Industrial Computing Security, Kyungwoon University

요 약 다중서버 환경에서 인가된 사용자만이 서버의 데이터와 서비스들을 이용할 수 있어야 함으로 인증된 키 동의는 보안 이슈들 중에서 가장 중요한 문제 중 하나이다. 이러한 보안 이슈를 지원하기 위해서 다양한 기법들이 최근 몇 년간 제안되었다. 특히, 최근에 Shin은 기존 기법의 보안 문제점을 도출하고 이를 해결할 수 있는 개선된 기법인 SIAKAS를 제안하였다. 본 논문에서는 SIAKAS가 여전히 응용서버 가장 공격에 취약하고 추적성을 제공하는 문제가 있음을 보이고, 이러한 문제들을 해결할 수 있는 비추적성을 제공하는 인증된 키 동의 기법인 UAKAS를 제안한다. UAKAS는 SIAKAS 및 관련된 기법들의 보안 및 프라이버시 문제를 해결하고 이들에 비해서 최소 12%의 연산 오버헤드를 줄일 수 있는 장점이 있다.

주제어 : 다중서버, 인증된 키 동의, 스마트카드, 가장공격, 비추적성

Abstract Authenticated key agreement in multi-server environments is one of very important security issues because only authorized user needs to access their data and services. To support this issue, numerous schemes have been proposed over recent years. Recently, Shin showed the security weaknesses in the previous scheme and proposed an improved scheme called SIAKAS to solve them. Unfortunately, this paper shows that SIAKAS is still weak against application server impersonation attack and could be traceable to attackers. To solve the problems in SIAKAS, we propose an untraceable authenticated key agreement scheme, denoted by UAKAS. UAKAS efficiently solves security and privacy issues in SIAKAS and the related schemes and could reduce the operation overhead at least 12% compared to them.

Key Words : Multi-server, Authenticated key agreement, Smart card, Impersonation attack, Untraceability

1. 서론

최근 몇 년간 무선 통신과 네트워크 기술의 빠른 진보를 통하여 많은 사람들이 네트워크 기반 저장 장치인 NAS (Network attached storage), 웹검색, 비디오 컨퍼런스, 멀티미디어 응용들을 포함한 다양한 서비스를 인

Received 2 September 2017, Revised 29 September 2017
Accepted 20 October 2017, Published 28 October 2017
Corresponding Author: Myungchun Ryoo
(Kyungwoon University)
Email: mcryoo@ikw.ac.kr

ISSN: 1738-1916

터넷을 통해 다양한 응용 서버로부터 모바일 장치를 이용하여 시간과 공간 제약 없이 활용하고 있다 [1,2,3,4]. 하지만 이들 모바일 컴퓨팅 환경은 적법한 사용자들을 다양한 공격으로 부터 안전하게 지킬 수 있는 인증 기법들을 필요로 한다 [5,6,7].

1981년 Lamport가 안전하지 않은 통신에서 패스워드 인증 기법을 제안하였지만 이 기법이 훔친 검증자 공격(Stolen verifier attack)에 취약함이 밝혀졌다 [8]. 또한, 최근 들어 인터넷 상에 다양한 응용 서버들을 기반으로 하는 서비스들이 제공되기 때문에 단일 서버 환경을 지원하는 보안 기법으로는 충분하지 않다. 즉, 다중서버 환경에서 인가된 사용자만이 응용 서버의 데이터와 서비스들을 이용할 수 있어야 하기 때문에 인증된 키 동의는 선결되어야 하는 보안 이슈 중 가장 중요한 문제이다. 이러한 보안 이슈를 지원하기 위해서 다양한 기법들이 최근 몇 년간 제안되었다 [9,10,11,12].

Juang이 2004년에 대칭키 암호시스템에 기반한 다중서버 환경의 인증기법을 제안한 이래 다양한 기법들이 제안되었다 [9]. Mishra등은 다중서버 환경에서 스마트 카드를 이용한 안전한 익명성을 제공하는 인증된 키 동의 기법 (Mishra et al.'s authenticated key agreement scheme, MAKAS)을 제안하였다 [10]. 하지만 최근에 Shin은 MAKAS가 사용자 가장공격과 재생공격 및 서비스거부공격에 취약함을 보이고 이를 해결하기 위한 개선된 기법(Shin's improved authenticated key agreement scheme, SIAKAS)을 제안하였다 [11]. SIAKAS는 MAKAS의 보안 취약점을 해결하기 위해서 단일 비밀 파라미터와 타임스탬프를 이용하였다.

본 논문에서는 SIAKAS가 응용서버 가장 공격에 취약하고 추적성의 문제가 있음을 보인다. 또한 이러한 SIAKAS 의 보안 및 프라이버시 문제들을 해결하기 위해 비추적성을 제공하는 인증된 키 동의 기법 (Untraceable authenticated key agreement scheme, UAKAS)을 제안한다. UAKAS 는 SIAKAS의 문제를 해결하기 위해 두 개의 비밀키를 응용서버 보안을 위해 활용하고, 비추적성을 위해 메시지에 포함된 모든 값에 난수를 적용한다. 이를 통해 UAKAS는 SIAKAS의 보안 및 프라이버시 문제를 효과적으로 해결할 수 있고, 관련된 다양한 기법보다 연산 복잡도에서도 우수함을 보인다.

본 논문의 구성은 다음과 같다. 2장에서 Shin등이 제안한 SIAKAS에 대한 리뷰를 제시하고 3장에서 이에 대한 보안 및 프라이버시 취약성을 보인다. 4장에서는 본 논문에서 제안한 비추적성을 지원하는 UAKAS를 제안한다. 5장에서 보안 및 성능 분석을 제시하고 6장에서 결론을 도출한다.

2. SIAKAS

본 장에서는 Shin이 제안한 개선된 키 동의 인증 기법인 SIAKAS에 대한 요약을 제시 한다 [11]. SIAKAS는 서버 등록단계, 사용자 등록단계, 로긴 단계, 인증 단계, 패스워드 변경단계로 구성된다. 본 논문에서 사용된 기호는 <Table 1>과 같다.

<Table 1> Notations

Symbol	Description
i	Remote user i
j	Application server j
RC	Registration server
ID_i, pw_i, BIO_i	Identity, password and bio information of i
SID_j	Identity of j
x	Master key of RC
PSK_j	Pre-shared keys of RC
SK_{ab}	Session key established between a and b
T_i	Timestamp at step i
N_i	Random number at step i
$h()$	One way hash function
$\|\|$	Concatenation operation
$\oplus$	XOR operation
Δt	The maximum of transmission delay time

2.1 서버 등록단계

이 단계는 응용서버들이 사용자들에게 서비스를 제공하기 위해 등록센터 (Registration center, RC)에 등록하는 단계이다. 응용서버가 등록을 요청하면 RC는 해당 응용서버 j의 식별자 SID_j와 PSK (Pre-shared key)를 이용하여 $h(h(PSK) \| SID_j)$를 계산하고 정당한 응용서버 j에게 안전하게 전달한다. 모든 응용서버는 RC의 파라미터 $h(PSK)$를 알지 못한다.

2.2 사용자 등록단계

사용자 i는 자신의 식별자 ID_i와 패스워드 pw_i 그리고 생체정보 BIO_i를 이용하여 응용서버들이 제공하는 서로 다른 서비스를 이용하기 위해 RC에 등록해야 한다.

(1) 사용자 i는 ID_i와 pw_i를 선택한 다음 생체정보 BIO_i를 센서에 입력하고 $W_1=h(pw_i \| ID_i)$과 $W_2=h(pw_i \oplus BIO_i)$를 계산하여 안전한 채널로 ID_i와 함께 RC에게 전송한다.

(2) RC가 $<W_1, W_2>$를 수신하면 $A_i=h(ID_i \| x)$, $B_i=h(A_i)$, $X_i=B_i \oplus W_2$, $Y_i=h(PSK) \oplus W_1$를 계산하고 스마트카드에 $<B_i, X_i, Y_i>$를 저장하여 안전한 채널로 사용자에게 전송한다.

사용자 i는 리더기에 스마트카드를 삽입하고 스마트카드 도난 및 정당한 사용자에 대한 검증을 대비하여 B_i를 $C_i=B_i \oplus h(pw_i \| BIO_i \| ID_i)$로 대체한다. 스마트카드가 도난이 되더라도 사용자의 패스워드와 생체정보 없이는 이용 불가능 하다. 최종적으로 스마트카드는 $<C_i, X_i, Y_i>$를 저장한다.

2.3 로긴 단계

사용자 i가 응용서버 j로부터 서비스를 제공받기 원할 때 로긴 단계가 실행되며 다음 과정을 수행한다.

(1) 스마트카드리더기에 스마트카드 SC_i를 삽입하고 ID_i와 pw_i를 입력하고 센서를 이용하여 사용자의 생체정보 BIO_i를 입력한다.

(2) 사용자 i는 난수 N_1을 생성하고 타임스탬프 T_1을 생성한다. 스마트카드는 C_i와 사용자가 입력한 pw_i, BIO_i, ID_i로부터 $B_i=C_i \oplus h(pw_i \| ID_i \| BIO_i)$를 계산한다.

(3) 스마트카드는 B_i와 $W_2 \oplus X_i$를 비교하여 사용자 i를 인증하고 인증이 실패하면 세션을 종료한다. 스마트카드 사용자 인증이 성공하면 $h(pw_i \| ID_i) \oplus Y_i$로부터 $h(PSK)$를 도출하고 $M_1=N_1 \oplus h(B_i)$, $M_2=ID_i \oplus h(N_1)$, $M_3=h(ID_i \| N_1 \| B_i \| SID_j \| T_1)$, $M_4=B_i \oplus h(h(PSK) \| SID_j)$를 계산하고 로긴 메시지 $<M_1, M_2, M_3, M_4>$를 생성한다.

(4) 스마트카드는 공개채널을 통해 응용서버 j에게 $<M_1, M_2, M_3, M_4, T_1>$을 전송한다.

2.4 인증 단계

$<M_1, M_2, M_3, M_4, T_1>$를 수신한 응용서버 j는 사용자 i를 다음과 같이 인증한다.

(1) 응용서버 j는 인증메시지의 신선성과 사용자 i의 적법성을 확인한다. 메시지를 수신한 시각 t_1을 구하고 $(T_1-t_1) \geq \triangle t$이면 사용자 i의 로긴 요청을 거절한다. T_1으로 메시지의 신선성을 확인하여 범위 안에 있으면 M_4로부터 A_i를 계산하기 위해 $h(h(PSK) \| SID_j)$를 계산한다. N_1을 구하기 위해 로긴 메시지의 M_1과 $h(A_i)$을 계산하고 N_1을 이용하여 사용자 i의 ID_i를 도출한다. $h(ID_i \| N_1 \| B_i \| SID_j \| T_1)$을 계산하여 수신한 M_3와 비교함으로서 사용자를 인증한다.

(2) 사용자 인증이 성공적이면 서버 j는 난수 N_2를 생성하고 $SK_{ji}=h(ID_i \| SID_j \| B_i \| N_1 \| N_2)$, $M_5=N_2 \oplus h(ID_i \| N_1)$, $M_6=h(SK_{ji} \| N_1 \| N_2 \| T_2)$, $M_7=SID_j \oplus h(h(PSK) \| SID_j)$을 계산하고 사용자 i에게 $<M_5, M_6, M_7, T_2>$를 전송한다.

(3) 메시지를 수신한 스마트카드는 타임스탬프 t_2을 통하여 $(T_2-t_2 \geq \triangle t$메시지의 신선성을 체크한다. 메시지의 신선성이 정상적으로 성공하면 M_5로부터 N_2를 계산하고 세션키 $SK_{ij}=h(ID_i \| SID_j \| B_i \| N_1 \| N_2)$를 연산하고 수신한 메시지 M_7과 M_6을 이용하여 합법적인 서버 j에 대한 인증을 수행한다. 응용서버들은 $h(PSK)$를 보유하지 않기 때문에 합법적인 응용서버 j만이 M_7을 생성할 수 있다.

(4) 합법적인 응용서버 j가 성공적으로 인증되면 $M_8=h(SK_{ij} \| N_2 \| N_1)$을 계산하여 이를 인증서버 j에게 전송한다.

(5) 응용서버 j는 $<M_8>$를 검증하고 합법적인 사용자 i로 인증한다.

2.5 패스워드 변경단계

패스워드의 변경은 RC의 도움 없이 사용자 i가 자유롭게 수행할 수 있다.

(1) 사용자 i는 SC_i를 삽입하고 ID_i와 pw_i를 입력하고 BIO_i를 입력한다. 스마트카드는 $B_i=C_i \oplus h(pw_i \| ID_i \| BIO_i)$, $W_2 \oplus X_i$를 계산하여 이 값이 B_i와 일치하는지 확인을 통해 스마트카드 소유자 인증을 실시한다. 인증이 성공적으로 끝나면 새로운 패스워드 pw_i^{new}를 입력한다.

(2) 스마트카드는 $W_2=h(pw_i \oplus BIO_i)$, $W_2^{new}=h(pw_i^{new} \|$

BIO_i), $X_i^{new}=X_i \oplus W_2 \oplus W_2^{new}$를 계산하고 X_i를 X_i^{new}로 변경한다.

3. SIAKAS에 대한 보안 취약성

본 장에서는 SIAKAS가 임의의 응용서버 가장 공격에 취약하고 세션 추적성이 가능함을 보인다. 공격을 제시하기 위해 본 논문에서는 적법한 사용자로 등록된 공격자 a와 응용서버의 식별자 SID를 쉽게 알 수 있다고 가정한다. 즉 공격자 a는 RC로부터 $\{N_a, M_a, h()\}$ 정보가 저장된 스마트카드를 발급 받을 수 있다. 또한 적법한 사용자는 로긴 단계 (4)의 M_4메시지 생성을 위해 응용서버의 식별자인 SID를 알 수 있다. 즉, 적법한 스마트카드를 발급받고 SID를 아는 적법한 사용자 a는 2장에서 살펴본 기법에서 임의의 응용서버 j에 대한 가장 공격을 수행할 수 있다. 또한, SIAKAS는 동일 사용자에 대한 세션 추적성을 제공하는 문제가 있다.

SIAKAS의 문제점을 도출하기 위해서 먼저 SIAKAS에 대한 안전성 주장을 살펴보고 그 주장에 대한 문제점을 공격 시나리오를 통해 보인다.

3.1 SIAKAS에 대한 안전성 주장

SIAKAS에서는 등록 센터와 응용서버마다 단일 비밀 파라미터를 발급하고 사용자의 로긴 메시지에서는 생체정보와 목적지 식별자, 타임스탬프 정보를 추가하여 기존의 기법에 존재하는 보안적 단점을 보완하였다고 주장하였다 [11]. 특히 SIAKAS는 서버 가장 공격, 사용자 가장 공격, 서비스 거부 공격, 재생공격, 스마트카드 도난 공격, 오프라인 추측 공격을 포함한 다양한 공격에 안전하다고 주장하였다.

3.2 SIAKAS에 대한 응용서버 가장 공격

본 절에서는 SIAKAS에서 주장한 것과 반대로 SIAKAS가 응용서버 가장 공격에 취약함을 보인다. SIAKAS에 대한 응용서버 가장 공격이 가능함을 보이기 위해 a가 임의의 적법한 응용서버 j로 임의의 사용자 i에게 인증될 수 있음을 보인다. 공격을 위해 임의의 사용자 i와 적법한 응용서버 j로 위장한 a는 로긴(L)과 인증(A) 과정을 다음과 같이 수행한다.

(L1) 적법한 사용자 i는 스마트카드리더기에 스마트카드 SC_i를 삽입하고 ID_i와 pw_i 그리고 BIO_i를 입력한다.

(L2) 사용자 i는 난수 N_1을 생성하고 타임스탬프 T_1을 생성한다. 스마트카드는 C_i와 사용자가 입력한 ID_i와 pw_i 그리고 BIO_i로부터 $B_i=C_i \oplus h(pw_i \| ID_i \| BIO_i)$를 계산한다.

(L3) SC_i는 B_i와 $W_2 \oplus X_i$를 비교하여 사용자 i를 인증하고 인증이 실패하면 세션을 종료한다. 스마트카드 사용자 인증이 성공하면 $h(pw_i \| ID_i) \oplus Y_i$로부터 $h(PSK)$를 도출하고 $M_1=N_1 \oplus h(B_i)$, $M_2=ID_i \oplus h(N_1)$, $M_3=h(ID_i \| N_1 \| B_i \| SID_j \| T_1)$, $M_4=B_i \oplus h(h(PSK) \| SID_j)$를 계산하고 로긴 메시지 $<M_1, M_2, M_3, M_4>$를 생성한다.

(L4) SC_i는 공개채널을 통해 응용서버 j에게 $<M_1, M_2, M_3, M_4, T_1>$을 전송한다.

$<M_1, M_2, M_3, M_4, T_1>$가 전송될 때 응용서버 j로 위장한 a는 자신의 스마트카드 SC_a의 스마트카드 사용자 인증인 (L3)를 통해 $h(PSK)$를 도출하고 적법한 응용서버 j를 가장하기 위한 인증 과정을 다음과 같이 수행한다.

(A1) a는 인증메시지의 신선성과 사용자 i의 적법성을 확인한다. 메시지를 수신한 시각 t_1을 구하고 $(T_1-t_1) \geq \triangle t$이면 사용자 i의 로긴 요청을 거절한다. T_1으로 메시지의 신선성을 확인하여 범위 안에 있으면 M_4로부터 A_i를 계산하기 위해 응용서버 j의 아이디 SID_j를 이용하여 $h(h(PSK) \| SID_j)$를 계산한다. N_1을 구하기 위해 로긴 메시지의 M_1과 $h(A_i)$을 계산하고 N_1을 이용하여 M_2로부터 사용자 i의 ID_i를 도출한다. $h(ID_i \| N_1 \| B_i \| SID_j \| T_1)$을 계산하여 수신한 M_3와 비교함으로서 사용자를 인증한다.

(A2) 사용자 인증이 성공적이면 a는 난수 N_2를 생성하고 $SK_{ji}=h(ID_i \| SID_j \| h(A_i) \| N_1 \| N_2)$, $M_5=N_2 \oplus h(ID_i \| N_1)$, $M_6=h(SK_{ji} \| N_1 \| N_2 \| T_2)$, $M_7=SID_j \oplus h(h(PSK) \| SID_j)$을 계산하고 사용자 i에게 $<M_5, M_6, M_7, T_2>$를 전송한다.

메시지를 수신한 적법한 사용자 i는 인증 단계의

(3)-(4)를 성공적으로 수행함으로서 공격자 a를 적법한 응용서버 j로 인증할 것이다. 이렇게 공격자 a가 적법한 응용서버 j로 인증될 수 있는 이유는 사용자 등록 과정에서 응용서버 j에게 중요한 정보인 $h(PSK)$를 모든 사용자에게 노출하는데 있다.

3.3 SIAKAS에 대한 세션 추적성 공격

고도화된 정보화 사회에서 통신 세션에 대한 익명성 및 추적성은 보안 및 프라이버시와 직결된 중요한 문제이다 [12]. 다양한 보안 기법에서 난수 및 타임스탬프를 사용하는 이유는 메시지의 신선성을 제공함으로서 재전송 공격에 대응하고 세션 비추적성을 제공하는데 그 목적이 있다.

하지만 SIAKAS에서는 다른 임의의 세션에서 동일한 값이 노출됨으로서 어떤 사용자에 의한 통신인지는 알 수 없지만, 동일한 사용자에 의한 다른 세션들임을 확인할 수 있는 정보를 노출하는 문제가 존재한다. 이는 로긴 단계의 (3)번 M_4에 의해 제시된다.

공격자는 도청 공격을 통해 공개채널의 로긴 메시지 $<M_1, M_2, M_3, M_4, T_1>$를 수신하고 M_4의 동일성을 검사함으로서 다양한 목적의 트래픽 분석 공격을 수행할 수 있다.

4. UAKAS : 비추적성을 제공하는 인증된 키 동의 기법

본 장에서는 SIAKAS의 보안 문제점을 해결하기 위한 다중서버를 위한 비추적성을 제공하는 인증된 키 동의 기법 (Untraceable Authenticated Key Agreement Scheme, UAKAS)을 제안한다. UAKAS도 서버 등록단계, 사용자 등록단계, 로긴 단계, 인증 단계, 패스워드 변경단계로 구성된다.

4.1 서버 등록단계

이 단계는 응용서버들이 사용자들에게 서비스를 제공하기 위해 RC에 등록하는 단계이다. 응용서버 j가 등록을 요청하면 RC는 해당 응용서버 j의 식별자 SID_j와 PSK 그리고 비밀키 y를 이용하여 $h(h(PSK) \| SID_j)$와 $h(SID_j \| h(y))$를 계산하고 정당한 응용서버 j에게 안전한 채널을 이용하여 전달한다. 여기서 $h(PSK)$와 $h(y)$는 RC가 비밀로 유지한다.

4.2 사용자 등록단계

사용자 i는 응용서버 j의 서비스를 가입하기 위해서 자신의 식별자 ID_i와 패스워드 pw_i 그리고 생체정보 BIO_i를 이용하여 응용서버들이 제공하는 서로 다른 서비스를 이용하기 위해 RC에 다음과 같이 등록한다.

(1) 사용자 i는 가입하고자 하는 응용서버 j의 식별자인 SID_j와 자신의 ID_i와 pw_i를 선택한 다음 생체정보 BIO_i를 센서에 입력하고 $W_1=h(pw_i \| ID_i)$을 계산하여 안전한 채널로 사용자 등록 메시지 $<SID_j, ID_i, W_1>$를 RC에게 전송한다.

(2) RC가 $<SID_j, ID_i, W_1>$를 수신하면 $B_i=h(ID_i \| x)$, $X_i=h(B_i)$, $Y_i=h(h(h(PSK) \| SID_j) \| B_i) \oplus W_1$, $Z_i=h(SID_j \| h(y)) \oplus B_i$를 계산하고 스마트카드에 $<B_i, X_i, Y_i, Z_i>$를 저장하여 안전한 채널로 사용자 i에게 전송한다. 사용자 i는 정당한 사용자 검증을 대비하여 B_i를 $C_i=B_i \oplus h(pw_i \| BIO_i \| ID_i)$로 대체한다. 최종적으로 스마트카드는 $<C_i, X_i, Y_i, Z_i>$를 저장한다.

하나 이상의 응용서버 j의 서비스에 가입을 원하는 사용자를 위해서 RC는 하나이상의 Y_i와 Z_i 쌍을 발급할 수 있다.

4.3 로긴 단계

사용자 i가 응용서버 j로부터 서비스를 제공받기 원할 때 로긴 단계가 실행되며 다음 과정을 수행한다.

(1) 사용자 i는 스마트카드리더기에 SC_i를 삽입하고 ID_i와 pw_i를 입력하고 생체정보 BIO_i를 입력한다 (하나이상의 서비스가 등록된 경우 원하는 서비스를 제공하는 응용서버 j의 SID_j를 같이 입력한다).

(2) 사용자 i는 난수 N_1와 타임스탬프 T_1을 생성한다. SC_i는 C_i와 사용자가 입력한 ID_i, pw_i, BIO_i로부터 $B_i=C_i \oplus h(pw_i \| ID_i \| BIO_i)$를 계산한다.

(3) SC_i는 $h(B_i)$와 X_i를 비교하여 사용자 i를 인증하고 인증이 실패하면 세션을 종료한다. 스마트카드 사

용자 인증이 성공하면 $h(pw_i \| ID_i) \oplus Y_i$로부터 $h(h(h(PSK) \| SID_j) \| B_i)$를 $Z_i \oplus B_i$로부터 $h(SID_j \| h(y))$를 각각 도출하고 $M_1=h(SID_j \| h(y)) \oplus N_1$, $M_2=B_i \oplus h(N_1)$, $M_3=h(B_i \| N_1 \| SID_j \| h(h(h(PSK) \| SID_j) \| B_i) \| T_1)$를 계산하고 로긴 메시지 $<M_1, M_2, M_3, T_1>$를 생성한다.

(4) SC_i는 공개채널을 통해 응용서버 j에게 $<M_1, M_2, M_3, T_1>$을 전송한다.

4.4 인증 단계

$<M_1, M_2, M_3, T_1>$를 수신한 응용서버 j는 사용자 i를 다음과 같이 인증한다.

(1) 응용서버 j는 인증메시지의 신선성과 사용자 i의 적법성을 확인한다. 메시지를 수신한 시각 t_1을 구하고 $(T_1-t_1) \geq \triangle t$이면 사용자 i의 로긴 요청을 거절한다. T_1으로 메시지의 신선성을 확인하여 범위 안에 있으면 M_3로부터 B_i를 계산하기 위해 RC로부터 받은 $h(h(PSK) \| SID_j)$와 $h(SID_j \| h(y))$ 및 수신한 T_1을 이용하여 M_1으로부터 N_1을 구하기 위해 $h(SID_j \| h(y))$를 이용하고 M_2로부터 B_i를 구하기 위해 $M_2 \oplus h(N_1)$을 계산한다. 도출한 값들을 이용하여 $h(B_i \| N_1 \| SID_j \| h(h(h(PSK) \| SID_j) \| B_i) \| T_1)$을 계산하여 수신한 M_3와 비교함으로서 사용자 i를 인증한다.

(2) 사용자 i의 인증이 성공적이면 응용서버 j는 난수 N_2를 생성하고 $SK_{ji}=h(B_i \| SID_j \| h(h(h(PSK) \| SID_j) \| B_i) \| N_1 \| N_2)$, $M_4=N_2 \oplus h(B_i \| N_1)$, $M_5=h(SK_{ji} \| N_1 \| N_2 \| T_2)$를 계산하고 사용자 i에게 $<M_4, M_5, T_2>$를 전송한다.

(3) 메시지를 수신한 SC_i는 타임스탬프 t_2을 통하여 $(T_2-t_2 \geq \triangle t$메시지의 신선성을 체크한다. 메시지의 신선성이 성공하면 M_4로부터 N_2를 계산하고 세션키 $SK_{ij}=h(B_i \| SID_j \| h(h(h(PSK) \| SID_j) \| B_i) \| N_1 \| N_2)$를 계산하고 수신한 메시지 M_5를 이용하여 합법적인 서버 j에 대한 인증을 수행한다.

(4) 합법적인 응용서버 j가 성공적으로 인증되면 SC_i는 $M_6=h(SK_{ji} \| N_2 \| N_1)$을 계산하여 이를 인증서버 j에게 전송한다.

(5) 응용서버 j는 $<M_6>$을 검증하고 합법적인 사용자 i로 인증한다.

4.5 패스워드 변경단계

패스워드의 변경은 RC의 도움 없이 사용자 i가 자유롭게 수행할 수 있다.

(1) 사용자 i는 SC_i를 삽입하고 ID_i와 pw_i를 입력하고 BIO_i를 입력한다. SC_i는 $B_i=C_i \oplus h(pw_i \| ID_i \| BIO_i)$, $h(B_i)$를 계산하여 이 값이 X_i와 일치하는지 확인을 통해 스마트카드 소유자 인증을 실시한다. 인증이 성공적으로 끝나면 새로운 패스워드 pw_i^{new}를 입력한다.

(2) SC_i는 $W_1=h(pw_i \| ID_i)$, $W_1^{new}=h(pw_i^{new} \| ID_i)$, $C_i^{new}=B_i \oplus h(pw_i^{new} \| BIO_i \| ID_i)$, $Y_i^{new}=Y_i \oplus W_1 \oplus W_1^{new}$를 계산하고 C_i와 Y_i를 각각 C_i^{new}와 Y_i^{new}로 변경한다.

5. 분석

본 장에서는 UAKAS에 대한 보안 분석과 성능 분석을 제시한다. UAKAS는 SIAKAS가 가지는 보안 문제점을 효율적으로 해결하였고 비추적성을 추가로 제시한다. 또한 UAKAS는 SIAKAS에 비해 성능 면에서도 효율성을 제시한다. 특히, 분석한 내용을 중심으로 본 논문에서 제안한 UAKAS와 MAKAS 그리고 SIAKAS와의 비교를 제시한다.

5.1 보안 분석

UAKAS는 다양한 보안 및 프라이버시 공격에 안전하다. 본 보안 분석에서는 SIAKAS의 보안 문제가 되었던 익명성, 가장 공격, 추적성 관점에 초점을 맞춘다.

(익명성) UAKAS의 주고받는 메시지를 통해 임의의 공격자가 사용자의 신원을 확인할 수 있는 방법이 없다. UAKAS를 통해서 $<M_1, M_2, M_3, T_1>$, $<M_4, M_5, T_2>$, $<M_6>$가 공개채널을 통해 전송된다. 여기서 사용자 식별자와 연계된 값은 M_2이다. 하지만 이 값으로부터 사용자 식별자인 ID_i나 B_i를 도출하기 위해서는 적법한 응용서버 j의 비밀 값과 연계된 $h(y)$나 $h(SID_j \| h(y))$를 알아야

한다. 하지만 UAKAS에서 공격자가 이 값을 알 수 있는 방법이 없다. 즉, UAKAS는 사용자의 익명성을 제공한다. 또한, UAKAS에서는 사용자 식별자인 ID_i 대신에 B_i를 이용함으로서 적법한 응용서버라고 하더라도 사용자의 적법성은 확인할 수 있지만, 사용자의 식별자를 확인할 수 있는 방법은 없다.

(가장 공격) UAKAS는 다양한 가장 공격에 안전하다. 특히, SIAKAS에서 문제가 되었던 응용서버 가장 공격의 안전성에 대해 살펴본다. 응용서버 가장 공격을 위해서 공격자는 사용자의 로긴 메시지에 대한 적법한 응답 메시지 $<M_4, M_5, T_2>$를 생성할 수 있어야 한다. 하지만 UAKAS의 정당한 사용자로 등록된 공격자라고 하더라도 자신의 스마트카드에 저장된 정보를 이용하여 정당한 M_5를 생성할 수 없다. 이는 공격자가 로긴 메시지로부터 $h(h(h(PSK) \| SID_j) \| B_j)$를 계산할 수 없으므로 적법한 SK_{ji}와 이를 통한 M_5를 생성하지 못하는데 그 이유가 있다. 즉, UAKAS는 다양한 가장 공격에 안전하다.

(비추적성) UAKAS는 세션 메시지 간 비연결성을 제공함으로서 비추적성을 제공한다. 즉, UAKAS에서 주고받는 메시지인 $<M_1, M_2, M_3, T_1>$, $<M_4, M_5, T_2>$, $<M_6>$를 통해서 다른 임의의 세션에서 동일한 사용자에 의한 통신이 얼마나 자주 진행되는지 확인할 수 없다. 이는 UAKAS에서 이용하는 모든 메시지에 포함된 값들에 난수 및 타임스탬프가 적절히 이용됨으로서 메시지의 신선성을 제공함으로서 달성되었다.

<Table 2> Security Comparisons

Security \ Scheme	MAKAS	SIAKAS	UAKAS
Password guessing	Yes	Yes	Yes
Impersonation	No	No	Yes
Replay	No	Yes	Yes
User anonymity	No	Yes	Yes
Untraceability	No	No	Yes

다양한 보안 및 프라이버시 분석을 통해 <Table 2>와 같이 UAKAS를 다양한 기법과 비교하였다. 이를 통해 UAKAS가 관련된 기법보다 보안 및 프라이버시 관점을 보다 잘 제공할 수 있음을 확인할 수 있다.

5.2 성능 분석

UAKAS의 성능 분석을 제시하기 위해서 주된 연산인 해쉬 연산(h)과 XOR 연산(x) 측면에서의 분석을 제시한다. <Table 3>은 UAKAS가 관련된 기법들보다 약 12% 해쉬 연산의 오버헤드를 줄임으로서 성능에서도 장점이 있음을 보여준다.

<Table 3> Performance Comparisons

Phase \ Scheme		MAKAS	SIAKAS	UAKAS
Registration		7h+5x	7h+4x	5h+5x
Login	User	6h+5x	5h+6x	5h+5x
Auth.	Server	7h+4x	7h+5x	6h+3x
	User	4h+1x	4h+2x	3h+1x
Password Change		5h+3x	6h+7x	5h+4x

6. 결론

본 논문에서는 최근에 Shin이 제안한 개선된 키 동의 인증 기법인 SIAKAS에 대해 살펴보고 SIAKAS에 존재하는 응용서버 가장 공격과 추적성에 대한 취약성이 존재함을 보였다. 또한, 이러한 SIAKAS의 문제점을 해결하기 위해서 비추적성을 제공하는 인증된 키 동의 기법인 UAKAS를 제안하였다. 분석에서 제시한 바와 같이 UAKAS는 기본의 MAKAS와 SIAKAS의 보안 및 프라이버시 문제를 효율적으로 해결하였다. 특히, UAKAS가 안전하면서도 기존 기법들의 연산 오버헤드를 12%이상 감소시키는 것을 확인할 수 있었다. 본 논문에서 제안한 UAKAS는 다양한 멀티서버 기반의 서비스를 제공하기 위한 기본 보안 기법으로 활용될 수 있을 것이다.

REFERENCES

[1] B.-S. Shim, D.-G. Yoo, “Trends and Activation Plans for Next-generation Wireless Broadband Industry,” Journal of Digital Convergence, Vol. 13, No. 12, pp. 13-21, 2015.

[2] Y.-T. Song, “The Effect of Web-based Communication to Internet Users of Information Characteristics :

Focus on Internalization and Conformity," Journal of Digital Convergence, Vol. 14, No. 7, pp. 117-126, 2016.
[3] S. Yoo, K. Choi, "Consumer protection in e-commerce: the Safety Transaction Service in Korea," Journal of Digital Convergence, Vol. 11, No. 11, pp. 29-36, 2013.
[4] S.-B. Kim, "Improvement of IPTV Policy under the Smart Environment," Journal of Digital Convergence, Vol. 11, No. 10, pp. 141-152, 2013.
[5] J.-M. Kim, H.-J. Kouh, "Security Analysis of Information Flow using SAT," Journal of Digital Convergence, Vol. 14, No. 6, pp. 253-261, 2016.
[6] D. Y. Kim, "Trend and Improvement for Privacy Protection of Future Internet," Journal of Digital Convergence, Vol. 14, No. 6, pp. 405-413, 2016.
[7] H.-W. Choi, M.-C. Ryoo, C.-S. Lee, H. Kim, "Secure Data Gathering Protocol over Wireless Sensor Network," The Journal of Digital Policy & Management, Vol. 11, No. 12, pp. 367-380, 2013.
[8] L. Lamport, "Password authentication with insecure communication," ACM Communication, Vol. 24, No. 11, pp. 770-772, 1981.
[9] W. S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Trans. on Consumer Electronics, Vol. 50, No. 1, pp. 251-255, 2004.
[10] D. Mishra, A. K. Das, S. A. Mukhopadhyay, "A secure user anonymity-preserving biometric based multi-server authenticated key agreement scheme using smart cards," Expert Systems with Applications, Vol. 41, No. 18, pp. 8129-8143, 2014.
[11] K.-C. Shin, "Analysis and security improvements to Mishra et al.'s authentication," Journal of Security Engineering, Vol. 13, No. 4, pp. 261-278, 2016.
[12] H. Kim, "Remote User Authentication Scheme with Key Agreement Providing Forward Secrecy," Journal of Security Engineering, Vol. 12, No. 1, pp. 1-12, 2015.
[13] W.S.Choi, D.H.Won, "Security Enhanced User Authentication Scheme with Key Agreement based on Fuzzy Extraction Technology ," Journal of Internet Computing and Services, Vol. 17, No. 3, pp. 1-10, 2017.
[14] Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung, Junghyun Nam and Dongho Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography." Sensors, Vol. 14, No. 6, 2014.
[15] Jongho Moon, Younsung Choi, jaewook Jung, Dongho Won, "An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards." PloS one,Vol 10, No. 12 , 2015.

최 해 원(Choi, Hae Won)

- 1996년 2월 : 경일대학교 컴퓨터공학과(공학사)
- 2000년 2월 : 경북대학교 컴퓨터공학과(공학석사)
- 2009년 2월 : 경북대학교 컴퓨터공학과(공학박사)
- 2006년 3월 ~ : 경운대학교 항공산업보안학과 교수
- 관심분야 : 알고리즘, 유비쿼터스 컴퓨팅, 보안
- E-Mail : chw@ikw.ac.kr

김 상 진(Kim, Sang Jin)

- 1994년 2월 : 계명대학교 컴퓨터공학과 (공학사)
- 1996년 2월 : 경북대학교 컴퓨터공학과 (공학석사)
- 2000년 8월 : 경북대학교 컴퓨터공학과 (공학박사)
- 1999년 9월 ~ 현재 : 경운대학교 항공산업보안학과 교수
- 관심분야 : 알고리즘, 게임이론, 보안
- E-Mail : sjkim@ikw.ac.kr

류 명 춘(Ryoo, Myung Chun)

- 1989년 2월 : 영남대학교 컴퓨터학과(공학사)
- 1991년 2월 : 영남대학교 컴퓨터공학과(공학석사)
- 2009년 2월 : 영남대학교 컴퓨터공학과(공학박사)
- 1997년 3월 ~ 현재 : 경운대학교 항공산업보안학과 교수
- 관심분야 : 지능정보시스템, Bioinformatics, 보안
- E-Mail : mcryoo@ikw.ac.kr