JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 28 No. 5, pp. 67-74, May 2023
https://doi.org/10.9708/jksci.2023.28.05.067

Analysis and Improved Solution of Hussian et al.'s Authentication Protocol for Digital Rights Management

Mi-Og Park*

*Assistant Professor, Dept. of Computer Engineering, Sungkyul University, Anyang, Korea

[Abstract]

In this paper, we analyze the authentication protocol for DRM proposed by Hussain et al. in 2022, and present an improved solution. Hussain et al. argued that their authentication protocol guarantees man-in-the-middle attack, replay attacks, and mutual authentication. However, as a result of analyzing Hussain et al.'s authentication protocol in this paper, Hussain et al.'s authentication protocol still has an insider attack problem, a problem with Yu et al.'s authentication protocol that they pointed out. For this reason, when an inside attacker acquires information on a mobile device, a user impersonation attack was also possible. In addition, there were problems with the user's lack of ID format verification and the problem of the secret key mismatch of the digital contents between the server and the user. Therefore, this paper proposes an improved solution to solve these problems. As a result of analysis in this paper, the improved solution is safe from various attacks such as smart card attack, insider attack, and password guessing attack and can safely authenticate users of DRM.

▸ **Key words**: DRM, Authentication, Insider attack, Smart card, User impersonation attack

[요 약]

본 논문에서는 2022년에 Hussain et al.이 제안한 DRM을 위한 인증 프로토콜에 대해 분석하고, 개선된 해결방법을 제시한다. Hussain et al.은 자신들의 인증 프로토콜이 중간자 공격과 재생 공격, 그리고 상호 인증을 보장한다고 주장하였다. 그러나 본 논문에서 Hussain et al.의 인증 프로토콜을 분석한 결과, Hussain et al.의 인증 프로토콜은 그들이 지적하였던 Yu et al.의 인증 프로토콜의 문제점인 내부자 공격 문제가 여전히 존재한다. 이로 인하여 내부 공격자가 모바일 기기의 정보를 획득할 경우 사용자 가장 공격 등도 가능하였다. 또한 사용자의 ID 형식 확인 부재의 문제와 서버와 사용자간의 디지털 컨텐츠의 비밀키 불일치의 문제점이 존재하였다. 그러므로 본 논문에서는 이러한 문제를 해결하기 위하여 개선된 해결방법을 제안한다. 개선된 해결방법을 본 논문에서 분석한 결과, 스마트카드 공격, 내부자 공격, 패스워드 추측 공격 등 여러 공격에 안전하여 DRM의 사용자를 안전하게 인증할 수 있다.

▸ **주제어**: DRM, 인증, 내부자 공격, 스마트카드, 사용자 가장 공격

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@daum.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2023. 02. 07, Revised: 2023. 04. 11, Accepted: 2023. 04. 25.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 2022년에 Hussain et al.[1]은 DRM을 위한 개선된 인증 프로토콜을 제안하였다. 여기서 DRM이란 Digital Rights Management의 약자로서 다양한 기기를 이용한 사용자들이 다양한 컨텐츠를 즐기는 현대의 라이프 스타일에서는 없어서는 안 될 필수적인 요소로서, 디지털 컨텐츠를 제공하는 저작권자나 출판사에게는 디지털 컨텐츠를 보호하고, 디지털 컨텐츠를 이용하는 사용자들에게는 정당한 사용료를 지불하도록 하는 기술이라고 할 수 있다. 그러므로 DRM에서는 정당한 사용자외의 다른 사용자들이 디지털 컨텐츠를 불법적으로 사용할 수 없도록 하기 위해서, 정당한 사용자를 인증(authentication)하고 보호하는 것이 중요하며, 날로 발전해가는 현대의 라이프 스타일과 저작권에 대한 인식 개선을 고려하면 DRM에서의 인증은 더욱 중요한 기술이 될 것으로 기대한다.

이를 증명하듯이 많은 DRM 인증 논문들이 제안되어 오고 있으며, 2008년에 Chen et al.[2]가 제안한 모바일 기기에 기반한 안전하고 추적 가능한 E-DRM 시스템이 그 시작으로 보인다. DRM의 기본적인 모델은 [Fig. 1]과 같으며, 그에 대한 간단한 동작원리를 살펴보면 다음과 같다.

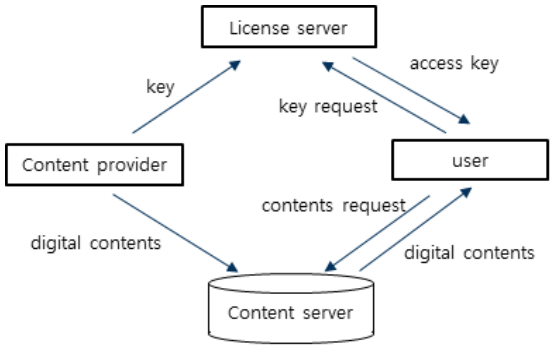

Fig. 1. Basic DRM Model

1.컨텐츠 제공자는 디지털 컨텐츠가 생성되면, 비밀키를 사용하여 디지털 컨텐츠를 암호화하고, 안전한 채널을 통하여 저작권 서버에게 키를 안전하게 전송하고, 컨텐츠 서버에게는 암호화된 디지털 컨텐츠를 전송한다.

2.요청을 받은 컨텐츠 서버는 암호화된 디지털 컨텐츠를 데이터베이스에 저장하고, 인터넷에 컨텐츠에 대한 요약본을 디스플레이한다.

3.저작권 서버는 비밀키를 데이터베이스에 저장하고, 사용자가 디지털 컨텐츠에 접근하기 위한 비밀키를 요청하면, 사용자를 인증하고 정당한 사용자이면 비밀키를 전송한다.

4.디지털 컨텐츠를 원하는 사용자는 컨텐츠 서버와 저작권 서버에게 인증 요청을 하고, 저작권 서버와의 상호인증이 성공할 경우, 비밀키를 가지고 암호화된 디지털 컨텐츠에 접근할 수 있다.

이와 같은 DRM을 사용하는 인증 논문 중 2020년에 Yu et al.[3]는 DRM을 위한 3-factor 인증 프로토콜을 제안하였고, 2018년에 Lee et al.[4]가 제안한 DRM을 위한 생체정보 기반의 인증과 익명성(anonymity)을 제공하는 프로토콜을 개선한 것으로, Yu et al.는 Lee et al.의 인증 프로토콜이 공격자가 모바일 기기에 저장된 정보와 기존의 메시지를 사용할 경우, 사용자 가장 공격(user impersonation attack)이 가능함을 보였다. 그리고 이러한 사용자 가장 공격으로 인하여 Lee et al.의 인증 프로토콜은 디지털 컨텐츠의 비밀키 안전성(secret-key disclosure attack)을 보장하지 못하고, 결과적으로 사용자와 서버간의 상호인증을 보장하지 못한다고 분석하였다.

Lee et al.가 제안한 인증 프로토콜은 2018년에 Jung et al.[5]이 제안한 DRM을 위한 생체정보 기반의 인증과 익명성 제공 프로토콜의 문제점을 개선한 것으로, Jung et al.의 인증 프로토콜은 사용자의 생체정보 처리에 바이오해쉬 함수를 사용하였고, Lee et al.와 Yu et al., 그리고 Hussian et al. 등은 퍼지 추출(fuzzy extractor)[6, 7]을 사용하여 생체정보를 처리하였다. Lee et al.가 분석한 Jung et al.의 문제점 중의 하나는 사용자 익명성을 제공하기 위해서 DIDi를 사용하였으나, DIDi 값이 변경되지 않고 항상 같은 값이어서 사용자에게 안전한 익명성을 제공하지 못한다고 분석하였다. 또한 본 논문에서 Jung et al.의 인증 프로토콜을 분석한 결과, 그들의 프로토콜은 사용자 가장 공격, 재생 공격(replay attack), 내부자 공격(Insider Attack) 등의 공격에도 안전하지 않았다.

이러한 Lee et al의 인증 프로토콜의 문제점을 개선하면서 Yu et al.는 Burrows-Abadi-Needham(BAN) logic 분석 툴과 AVISPA 시뮬레이션 툴을 사용하여 자신들의 프로토콜의 안전성을 증명하였고, 그래서 Yu et al.은 자신들의 인증 프로토콜이 중간자 공격(man-in-the-middle attack)과 재생 공격에 안전하고, 자원이 제한된 환경에 적용가능하다고 주장하였다. 그러나 2021년에 Khan[8]은 Yu et al.의 인증 프로토콜이 내부자 공격과 사용자 가장 공격, 그리고 서비스 거부 공격(Denial of services Attack) 등에 안전하지 않음을 보였다. 내부자 공격은 사용자의 ID와 서버의 비밀키, 그리고 디지털 컨텐츠의 ID를 데이터베이스에 암호화하여 저장하지 않기 때문에, 이 정보들이 내부 공격자의 손에 들어갈 수 있고, 내

부 공격자는 이 정보들을 사용하여 정당한 사용자를 가장할 수 있고, 타임스탬프(time stamp)가 미포함된 것으로 인하여 서비스 거부 공격에 안전하지 않다고 지적하였다.

2022년에 Hussain et al.도 Khan et al.처럼 Yu et al.의 인증 프로토콜을 개선하면서, Yu et al.의 인증 프로토콜이 내부자 공격, 사용자 가장 공격, 그리고 서버 가장 공격의 문제점이 있음을 지적하였고, 가장 공격에 의한 안전성 문제는 결국 디지털 컨텐츠 사용을 위한 비밀키의 안전성을 보장하지 못한다고 분석하였다. Yu et al.의 이러한 문제점을 개선한 Hussain et al.은 BAN logic을 사용하여 자신들의 인증 프로토콜이 안전한 상호 인증을 보장한다고 주장하였고, 중간자 공격과 재생 공격에 대한 안전성은 AVISPA 툴을 사용하여 증명하였다.

그러나 Hussain et al.의 인증 프로토콜을 분석한 결과, Hussain et al.의 인증 프로토콜도 사용자의 ID와 그에 매핑되는 유일한 난수 PIDm을 데이터베이스에 그냥 저장하기 때문에 여전히 내부자 공격에 안전하지 않고, 이로 인하여 내부 공격자가 더 많은 정보들을 획득할 경우 사용자 가장 공격 등에도 안전하지 않았다. 그래서 본 논문에서는 Hussain et al.의 인증 프로토콜을 분석하고, 이에 대한 문제점을 해결하기 위한 간단한 개선방법을 제안한다.

본 논문의 구성은 2장에서 Hussain et al.의 인증 프로토콜을 리뷰하고, 3장에서 그들의 인증 프로토콜에 대한 안전성과 설계상의 문제점을 분석하여 그들의 주장과 달리 DRM을 위한 안전하고 효율적인 인증 프로토콜이 아니라는 것을 보인다. 4장에서는 Hussain et al. 인증 프로토콜의 문제점을 해결하기 위한 간단한 해결방법을 제시하고, 그에 대한 안전성과 계산 복잡도를 분석한다. 그리고 5장에서 결론에서 인증 프로토콜의 문제점과 논문에서 제안한 내용을 요약하였다.

II. Review of Hussain et al.'s Authentication Protocol

본 논문에서는 Hussain et al의 인증 프로토콜에 대한 안전성을 분석하기에 앞서, 본 장에서는 Hussain et al의 인증 프로토콜의 등록 단계, 로그인과 인증 단계, 그리고 패스워드 변경 단계를 살펴본다.

1. Registration phase

Hussain et al.가 제안한 등록 단계는 다음과 같다.

Step 1: 사용자 Um은 IDm과 PWm을 선택하고, 생체정보 BIO_m^*을 입력하여 Gen(BIOm)=<Rm, Pm>과 RPWm=h(PWm||Rm)을 계산한 후 안전한 채널을 통해 {IDm, RPWm}을 저작권 서버 LSj에 보낸다.

Step 2: 등록 요청을 받은 서버 LSj는 Xm=h(IDm||X_{LS})와 dm=Xm⊕h(IDm||RPWm)을 계산한 후 IDm과 PIDm을 데이터베이스에 저장하고, Xm과 PIDm은 안전한 채널을 통해 사용자에게 보낸다.

Step 3: 사용자 Um은 PIDm'=PIDm⊕h(PWm||Rm), Xm'=Xm⊕h(PWm||Rm), Zm= h(IDm|| PWm||Rm)를 계산하여 {Xm', PIDm', Zm}을 모바일 장치에 저장한다.

2. Login and Authentication phase

Hussain et al.의 로그인 단계와 인증 단계는 [Fig. 2]와 같다.

Step 1: 사용자 Um은 IDm과 PWm, 그리고 생체정보 BIOm을 입력하여 Rm=Rep(BIOm, Pm)를 계산하고 Zm?=h(IDm||PWm||Rm)이 동일한지 비교한다. 동일하면 난수 R1과 타임스탬프 Tm을 선택하여 Xm=Xm'⊕h(Rm||PWm), Z1=IDm⊕R1⊕h(Xm⊕Tm), Z2=IDc⊕R1⊕h(Xm⊕Tm), Zus=h(IDm||IDc||h(Xm||Tm)||R1||Tm)를 계산한 후, <Z1, Z2, Zus, PIDm, Tm>를 LSj에게 보낸다.

Step 2: LSj는 |Tm-Tc|<△T를 비교하여 조건이 맞으면 PIDm에 일치하는 IDm를 가져와서 Xm^*=h(IDm||X_{LS}), R1=Z1⊕IDm⊕h(Xm^*⊕Tm), IDc=Z2⊕R1⊕h(Xm^*⊕Tm), Mus^*=h(IDm||IDc||h(Xm^*||Tm)||R1||Tm)를 계산한 후, Mus^*?= Zus를 비교한다. 두 값이 동일하면, R2와 Tcs, 그리고 $PIDm^{new}$를 선택하여 TEMP1=h(IDm⊕R1), Z3=R2⊕h(Xm^*⊕Tcs)⊕TEMP1, Z4=$PIDm^{new}$⊕h(Xm^*||Tcs)⊕TEMP1, Z5=Kc⊕h(Xm^*||Tcs)⊕R2⊕TEMP1, Zsu=h(IDm||h(Xm^*⊕Tm)||Kc||R2||TEMP1||Tcs)를 계산한다. 그런 다음 PIDm을 $PIDm^{new}$로 대체하고 사용자 Um에게 <Z3, Z4, Z5, Zsu, Tcs>를 보낸다.

Step 3: 사용자 Um은 |Tcs-Tc|<△T의 조건을 비교하여 참이면, TEMP2=h(IDm⊕R1), R2=Z3⊕h(Xm||Tcs)⊕TEMP2, $PIDm^{new}$=Z4⊕h(Xm||Tcs)⊕TEMP2, Kc=Z5⊕h(Xm||Tcs)⊕R2⊕TEMP2, Msu^*계산한다. 그런 다음 Msu^* ?= Zsu의 조건이 참이면 KEY_{DC}^*=Kc⊕h(PWm||Rm)을 계산하여 저장한다.

3. Password change phase

Hussain et al의 패스워드 변경 과정은 다음과 같으며, 이와 같은 과정을 통해 정당한 사용자는 기존의 패스워드를 새롭게 변경할 수 있다.

Step 1: 사용자 Um은 새로운 쌍 {ID_m^*, PW_m^*}과 BIO_m^*을 입력하여, $Gen(BIO_m^*)=<R_m^*, P_m^*>$과 $RPW_m^*=h(PW_m^*||R_m^*)$을 계산한 후 {ID_m^*, RPW_m^*}을 모바일 장치에 저장한다.

Step 2: 모바일 장치는 Z_m^* ?= $h(ID_m^*||PW_m^*||R_m^*)$를 비교하여, 두 값이 동일하면 사용자 Um이 정당하다고 확인한다.

Step 3: 사용자 Um은 새로운 패스워드 PW_m^{new}와 새로운 생체정보 BIO_m^{new}를 선택하여 $Gen(BIO_m^{new})=<R_m^{new}, P_m^{new}>$과 $RPW_m^{new}=h(PW_m^{new}||R_m^{new})$를 계산한다.

Step 4: 메시지를 받은 모바일 장치는 $X_m=h(ID_m||X_{LS})$과 $dm^{new}=X_m^*\oplus h(ID_m||RPW_m^{new})$를 계산하여 X_m과 PID_m^{new}를 보낸다.

Step 5: 사용자 Um은 $PID_m^{new*}=PID_m^{new}\oplus h(PW_m^{new}||R_m^{new})$과 $X_m^{new*}=X_m\oplus h(PW_m^{new}||R_m^{new})$, 그리고 $Z_m=h(ID_m||PW_m^{new}||R_m^{new})$를 계산하여, {$X_m^{new*}$, PID_m^{new*}, Z_m}를 업데이트한다.

III. Analysis of Hussain et al.'s Protocol

이번 장에서는 본 논문에서 분석한 Hussain et al. 인증 프로토콜의 안전성에 대해 분석한다. Hussain et al.은 자신들의 인증 프로토콜이 Yu et al의 인증 프로토콜의 문제점을 개선하여 내부자 공격과 다른 공격들에 안전하고 더 효율적이어서, DRM을 위한 안전한 상호 인증을 보장한다고 주장하였다. 그러나 본 논문에서 분석한 결과, Hussain et al.의 인증 프로토콜은 내부자 공격에 안전하지 않았고, 이로 인하여 발생하는 다른 공격들에도 안전하지 않았다.

User	License Server
Um inputes ID_m, PW_m	
Imprints biometirc BIO_m	
$R_m=Rep(BIO_m, P_m)$	
If Z_m ?= $h(ID_m\|\|PW_m\|\|R_m)$	
Select R_1 and T_m	
$X_m=X_m'\oplus h(PW_m\|\|R_m)$	
$Z_1=ID_m\oplus R_1\oplus h(X_m\oplus T_m)$	
$Z_2=IDc\oplus R_1\oplus h(X_m\oplus T_m)$	
$Z_{US}=h(ID_m\|\|IDc\|\|h(X_m\|\|T_m)\|\|R_1\|\|T_m)$	
$<Z_1, Z_2, Z_{US}, PID_m, T_m>$	
---------->	
	Check if $\|T_m-T_c\|<\triangle T$?
	Fetch ID_m corresponding PID_m
	Computes $X_m^*=h(ID_m\|\|X_{LS})$
	Computes $R_1=Z_1\oplus ID_m\oplus h(X_m^*\|\|T_m)$
	$IDc=Z_2\oplus R_1\oplus ID_m\oplus h(X_m^*\|\|T_m)$
	$M_{US}^*=h(ID_m\|\|IDc\|\|h(X_m^*\|\|T_m)\|\|R_1\|\|T_m)$
	Check if M_{US}^* ?= Z_{US}
	If ture, pick R_2, Tcs and PID_m^{new}
	Fetches Kc
	Calculates $TEMP1=h(ID_m\oplus R_1)$
	$Z_3=R_2\oplus h(X_m^*\oplus Tcs)\oplus TEMP1$
	$Z_4=PID_m^{new}\oplus h(X_m^*\oplus Tcs)\oplus TEMP1$
	$Z_{SU}=h(ID_m\|\|h(X_m^*\|\|Tcs)\|\|Kc\|\|R_2\|\|TEMP1\|\|Tcs)$
	Replaces PID_m with PID_m^{new}
	$<Z_3, Z_4, Z_5, Z_{SU}, Tcs>$
Check if $\|T_m-T_c\|<\triangle T$?	<----------
Calculates $TEMP2=h(ID_m\oplus R_1)$	
$R_2=Z_3\oplus h(X_m\oplus Tcs)\oplus TEMP2$	
$PIDm^{new}=Z_4\oplus h(X_m\oplus Tcs)\oplus TEMP2$	
$Kc=Z_5\oplus h(X_m\oplus Tcs)\oplus R_2\oplus TEMP2$	
$M_{SU}^*=h(ID_m\|\|h(X_m\|\|Tcs)\|\|Kc\|\|R_2\|\|TEMP2\|\|Tcs)$	
Check if M_{SU}^* ?= Z_{US}	
If true, $KEY_{DC}^*=Kc\oplus h(PW_m\|\|R_m)$	
Saves KEY_{DC}^*	

Fig. 2. Hussain et al.'s Login and Authentication Phase

1. Incorrectness of the Protocol

1.1 Absence of ID format Verification

등록 단계의 사용자가 등록을 위해서 저작권 서버에 사용자의 IDm과 PWm을 전송하면, 서버는 사용자의 IDm의 타당성을 확인하지 않고 사용자로부터 받은 IDm을 가지고 곧바로 다음 과정의 계산을 진행한다. Lee et al.와 Yu et al.의 인증 프로토콜은 모두 사용자의 ID에 대한 타당성을 먼저 확인한다. 그러나 Hussain et al.의 등록 단계는 그들이 제안한 그림이나 등록 단계의 설명부분을 살펴봐도 사용자 IDm의 타당성을 확인하는 과정이 없다.

이러한 사용자의 IDm 타당성 확인과정의 부재는, 정당한 사용자의 IDm을 획득한 공격자가 정당한 사용자를 가장하는 공격이 발생할 수 있는 것은 물론이고, 정당한 사용자의 IDm을 획득하지 않고도 공격자 마음대로 만든 임의의 IDm을 사용하여 서비스 거부 공격을 할 수도 있다. 게다가 더욱 큰 문제는 IDm의 타당성을 확인하지 않기 때문에 정당한 사용자가 선택한 IDm이 기존의 다른 정당한 사용자와의 ID와 중복될 수 있기 때문에, 디지털 컨텐츠의 요금 청구에 대한 문제가 발생한다.

Table 1. Notations

Notations	Description
Um	Mobile user
LSj	License server
IDm	Identification of Um
IDc	Identification of LSj
PWm	User password
BIOm	biometrics of User
X_{LS}, Kc	Secret keys of LSj, IDc
h()	One-way hash function
R_1, R_2	Random nonces
PIDm	Unique random nonce for each user
KEY_{DC}	Secret key of digital content
||	Concatenation operation
⊕	XOR operation

1.2 Incorrectness of Digital Contents Keys

본 논문에서 분석한 Hussain et al.의 다른 문제점은 [table 1]에서 보는 바와 같이 디지털 컨텐츠에서 사용하는 비밀키가 Kc와 KEY_{DC}로 2개이다. 그들이 개선하였던 Yu et al.의 프로토콜에서는 KEY_{DC} 한 개만 디지털 컨텐츠의 비밀키로 사용하였고, 이전의 프로토콜들에서도 동일하였다. Hussian et al.의 인증 단계를 분석하면, 서버 LSj에서 전송한 정보를 이용해 사용자가 컨텐츠의 비밀키 Kc를 계산해내서, 서버와 사용자는 동일한 Kc를 가지게 된다. 그 다음에 사용자는 자신의 패스워드 PWm과 Rm을 KEY_{DC}^*=Kc⊕h(PWm||Rm)와 같이 계산해서 KEY_{DC}^*를 저장한다. 만약 KEY_{DC}가 올바른 디지털 컨텐츠의 비밀키라고 가정할 경우, 이 값은 각 사용자의 패스워드 PWm과 Rm으로 구성되어있는데, 저작권 서버는 등록 단계나 인증 단계에서 이 두 값을 데이터베이스에 저장하지 않기 때문에 서버는 KEY_{DC}^* 값을 계산해 낼 수 없다. 그러므로 서버는 알 수 없는 키 값을 사용하여 디지털 컨텐츠에 접근하는 사용자는 접근 차단할 것이다.

만약, PWm과 Rm이 서버의 데이터베이스에 저장된다면 Hussian et al.의 인증 프로토콜은 내부 공격자가 사용자의 모든 정보를 손에 넣을 수 있기 때문에, 사용자 가장 공격에 더욱 취약하게 된다. 만약, Hussain et al.의 키 설계가 맞다고 가정할 경우, 같은 디지털 컨텐츠에 대해 각 사용자마다 다른 키 값을 가지게 되고, 이럴 경우에 서버는 각자 다른 키 값을 모두 저장하고 있어야 만이, 사용자의 컨텐츠 사용을 허락할 것이다. 그러므로 Hussain et al.의 인증 프로토콜은 안전한 프로토콜이라고 할 수 없다.

2. Safety Analysis

본 절에서는 Hussian et al. 인증 프로토콜의 안전성 측면에 대해 분석한다.

2.1 Privileged Insider Attack

Hussain et al.은 Yu et al.의 인증 프로토콜에 대한 문제점을 분석 및 개선하면서 Yu et al.의 인증 프로토콜이 민감한 정보를 저작권 서버의 데이터베이스에 저장하고 있기 때문에, 내부자 공격에 안전하지 않다고 분석하였다. 또한 내부 공격자는 획득한 데이터베이스의 IDi와 $Xi=h(IDi||X_{LS})$를 사용하여 사용자를 가장할 수 있기 때문에 사용자 가장 공격에도 안전하지 않다고 분석하였다. 그러나 본 논문에서 Hussain et al.의 인증 프로토콜을 분석한 결과, Hussain et al.의 등록 단계에서도 IDm과 PIDm을 데이터베이스에 그대로 저장하기 때문에 내부 공격자는 사용자의 IDm과 PIDm을 획득할 수 있다. PIDm은 로그인 요청 메시지의 일부이므로, 내부 공격자가 아니더라도 획득할 수 있는 값이다. 그러므로 Hussain et al.의 인증 프로토콜에서도 내부자 공격은 여전히 존재하는 문제점이다.

2.2 User Impersonation attack

Hussain et al.의 인증 프로토콜은 모바일 장치에 {Xm', PIDm', Zm}이 저장되어있는데, 공격자가 이러한 정보를 획득하였을 경우 다음 과정을 통해 중요한 정보들을 계산해낼 수 있다.

$$PIDm' = PIDm \oplus h(PWm||Rm) \quad (1)$$

PIDm'과 로그인 요청 메시지 PIDm, 그리고 (1)식을 사용하면 다음과 같이 h(PWm|| Rm)을 계산해낼 수 있다.

$h(PWm|| Rm)^* = PIDm' \oplus PIDm$

저장된 정보 Xm'과 앞의 과정에서 계산해 낸 h(PWm|| Rm)*을 식 (2)처럼 구성하면 Xm*을 계산해낼 수 있다.

$Xm' \oplus h(PWm||Rm)^* = Xm^*$ (2)

내부자 공격을 통해 획득한 IDm*과 로그인 요청 메시지 Z1, Z2, Zus, Tm을 사용하면 난수 R1을 계산해 낼 수 있다. 난수 R1을 계산하기 위해서 식 (3)을 $R1=Z1 \oplus IDm^* \oplus h(Xm^* \oplus Tm)$과 같이 계산한다.

$Z1= IDm \oplus R1 \oplus h(Xm \oplus Tm)$ (3)

식 (3)을 통해 난수 R1을 계산한 후에 식 (4)를 이용하여 IDc 값을 계산해 낼 수 있다.

$Z2 = IDc \oplus R1 \oplus h(Xm \oplus Tm)$ (4)

$IDc^*= Z2 \oplus R1^* \oplus h(Xm^* \oplus Tm)$

앞의 식 (3)과 (4)를 통해 계산해 낸 값을 사용해 Zus 값을 계산해 낼 수 있다.

앞에서 공격자가 계산해 낸 값들이 올바른 값일 경우, 공격자는 정당한 사용자를 가장할 수 있는 모든 정보를 가지게 되므로, 공격자 자신이 생성한 타임스탬프 Ta를 사용하여 정당한 사용자로 위장할 수 있다.

2.3 Key Attack of Digital Content

앞의 사용자 가장 공격에서 얻은 IDm*과 R1*을 사용한 공격자는 TMEP2*를 계산한 후, 공개 정보 Tcs와 Z3을 사용하여 R2를 계산해낼 수 있다. 이와 같이 공개 정보들과 획득한 정보들을 사용하면 Kc를 계산해낼 수 있고, 이로 인하여 공격자는 KEY_{DC}^*를 계산해 낼 수 있다.

$TMEP2^*=h(IDm^*||R1^*)$

$R2^*=Z3 \oplus (Xm^*||Tcs) \oplus TMEP2^*$

$PIDm^{new*} =Z4 \oplus h(Xm^*||Tcs) \oplus TEMP2^*$

$Kc^*=Z5 \oplus h(Xm^*||Tcs) \oplus R2 \oplus TEMP2^*$

Kc는 디지털 컨텐츠의 비밀키이고, 정당한 사용자와 서버만이 같은 값을 가지는데, 공격자가 Kc를 획득한다는 것은 프로토콜의 안전성에 문제가 있다는 것이다. 또한 본 논문의 3.1 절에서 분석한 KEY_{DC}의 문제점이 없다고 가정한다고 하더라도 공격자가 Kc를 계산해내면 공격자는 KEY_{DC}^*도 계산해낼 수 있다. 그러므로 Hussian et al.의 인증 프로토콜은 안전하다고 할 수 없다.

IV. Improved Solution

본 장에서는 Hussian et al. 프로토콜에 대한 문제점을 해결하기 위하여 다음과 같은 간단한 해결책을 제시한다. 먼저 등록 단계에서 사용자의 ID에 대한 타당성을 추가하여 사용자들을 구별할 수 있도록 한다. 또한 앞 장에서 분석한 Contents Keys에 대한 해결 방법은 Hussian et al.의 의도를 정확히 알 수 없지만, 본 논문에서는 한 개의 키를 사용한다고 가정하여 Kc는 사용하고 KEY_{DC}는 사용하지 않는 것으로 해결한다. 그러면 앞 장의 2.3에서 분석한 것처럼 사용자와 서버가 동일한 키 Kc를 공유하기 때문에, 사용자는 해당 컨텐츠에 접근하여 원하는 컨텐츠를 사용할 수 있다. 그러므로 Hussian et al. 프로토콜에서의 디지털 컨텐츠 키에 대한 문제를 해결할 수 있다.

안전성 측면에 대한 개선 방법은 다음 두 식에서 공통으로 사용하는 h(PWm||Rm) 값을 변경하고, 나머지 과정은 기존의 Hussian et al. 프로토콜과 동일하다.

$PIDm' = PIDm \oplus h(PWm||Rm)$

$Xm' \oplus Xm=h(PWm||Rm)$

User		License server
Inputs ID_m, PW_m Imprints biometirc BIO_m Computes $Gen(BIO_m)=<R_m, P_m>$ $RPW_m=h(PW_m\|\|R_m)$	$<ID_m, RPW_m>$ ---------->	Check validity of ID Select PID_m Computes $X_m=h(ID_m\|\|X_{LS})$ $d_m=X_m \oplus h(ID_m\|\|RPW_m)$ Saves the ID_m and PID_m
	$<X_m, PID_m>$ <----------	
$PID_m'=PID_m \oplus h(ID_m \oplus PW_m \oplus R_m)$ $X_m'=X_m \oplus h(PW_m\|\|R_m)$ $Z_m=h(ID_m\|\|PW_m\|\|R_m)$ Stores $\{X_m', PID_m', Z_m\}$ in memory		

Fig. 3. Improved Registration Phase

Table 2. Security Function Comparison of the Related Protocols

	Jung et al.[5]	Lee et al.[4]	Yu et al.[3]	Analysis result of Hussian et al.[1]	Improved solution
Insider attack	X	O	X	X	O
User impersonation attack	X	X	X	X	O
Server impersonation attack	O	O	O	O	O
Stolen mobile device attack	O	X	X	X	O
Key disclosure of digital content	X	X	X	X	O
Replay attack	X	O	X	X	O
User anonymity	X	O	X	X	O
Password guessing attack	O	O	O	O	O
Mutual authentication	X	X	X	X	O

PIDm'과 Xm'은 두 값 모두 h(PWm||Rm)을 동일하게 사용하기 때문에, 앞의 "user impersonation attack"절에서, 모바일 장치를 분실할 경우(stolen mobile attack) 첫 번째 식을 이용하여 한번의 XOR 연산으로 h(PWm||Rm)를 얻어낼 수 있고, 이 값과 두 번째 식을 이용하면 Xm 값을 공격자가 쉽게 계산해낼 수 있었다. 그러므로 이 문제를 해결하기 위해서 두 식에서 h(PWm||Rm)이 중복되지 않도록 [Fig. 3]과 같이 등록 단계의 PID_m'를 $PID_m'=PID_m\oplus h(ID_m\oplus PW_m\oplus R_m)$로 변경한다. 공격자가 카드의 정보 PID_m'과 로그인 요청 메시지 PID_m를 사용해서 $PID_m'\oplus PID_m$연산을 하면 $h(ID_m\oplus PW_m\oplus R_m)$을 얻을 수 있다. 그 다음으로 카드의 저장 정보 Xm'을 이용해 계산하려면 Xm과 h(PWm||Rm)을 알아야하는데, 변경된 PID_m'로부터 Xm을 계산해내려면 ID_m과 PW_m, 그리고 R_m의 각각의 값을 알아야 하고, R_m은 높은 엔트로피의 생체정보 BIO_m을 알아야 만이 계산할 수 있다. 또한 이 값은 카드에 저장된 값이 아니기 때문에 이 값과 함께 연산한 ID_m과 PW_m을 각각 계산해내기 어렵다.

앞의 분석 절 (3)에서 공격자가 난수 R1을 계산 가능한 것은 Xm과 h(PWm||Rm)을 계산해낼 수 있었기 때문에 가능한 것이었는데, 본 절의 해결방법을 사용하면 공격자가 Xm을 계산해낼 수 없고, (3)식에서 R1을 계산해낼 수 없으므로 (4)에서 IDc를 계산해낼 수 없다.

$$Z1= IDm\oplus R1\oplus h(Xm\oplus Tm) \quad (3)$$

$$Z2= IDc\oplus R1\oplus h(Xm\oplus Tm) \quad (4)$$

그러므로 공격자는 그 다음 과정인 Zus도 계산해낼 수 없게 되어, PID_m'를 변경하는 간단한 방법으로 공격자는 스마트카드/모바일 장치 분실 공격을 통해 중요한 정보들을 얻어낼 수 없고, 결과적으로 정당한 사용자로 위장할 수 없다.

4.1 Password Change Phase

본 논문에서의 해결방법은 PID_m'를 변경하였기 때문에 새로운 패스워드로 변경하기 원하는 사용자를 위하여 패스워드 변경단계의 PID_m'도 기존의 $PID_m^{new}=PID_m^{new}\oplus h(PW_m^{new}||R_m^{new})$에서 $PID_m^{new}=PID_m^{new}\oplus h(ID_m\oplus PW_m^{new}\oplus R_m^{new})$로 변경해야한다.

4.2 Password Guessing Attack

패스워드 추측 공격은 패스워드 PW_m이 엔트로피가 높은 BIO_m과 함께 해시 연산하였기 때문에, PID_m', Xm', 그리고 Zm으로부터 PW_m을 계산해내기 어렵다. 그러므로 본 절의 개선방법은 패스워드 추측 공격에 대한 저항성을 가진다.

4.3 Insider Attack

앞의 내부자 공격 절에서 분석한 Hussian et al. 프로토콜은 사용자의 정보를 평문으로 저장하여 발생한 것으로, DB를 암호화하거나 다른 인증 프로토콜들처럼 DB는 안전하다고 가정하여 이 문제를 해결한다.

4.4 Replay attack

본 논문의 해결방법은 Hussain et al. 프로토콜과 동일하게 타임스탬프를 그대로 사용하기 때문에, 재생 공격에 대한 저항성을 가진다. 그러므로 본 논문에서 제안한 해결방법은 안전한 프로토콜이라고 할 수 있다.

[Table 2]는 본 논문의 해결방법과 관련된 다른 인증 프로토콜들의 안전성을 분석한 것으로, X는 해당 공격에 안전하지 않거나 해당 기능을 제공하지 않는다는 것을 나타

Table 3. Computation Complexity

	Jung et al.[5]	Lee et al.[4]	Yu et al.[3]	Hussian et al.[1]	Improved solution
User Um	8Th+1Tf	4Th+1Tf	5Th+1Tf	8Th+1Tf	8Th+1Tf
Server LSj	5Th	5Th	2Th	6Th	6Th
Total cost	13Th+1Tf	9Th+1Tf	7Th+1Tf	14Th+1Tf	14Th+1Tf

내고, O는 그 반대의 의미이다. [Table 3]은 관련 인증 프로토콜들의 계산 복잡도를 비교한 것으로, Th는 해시함수 연산을 나타내고, Tf는 바이오해쉬함수나 퍼지 추출 연산을 나타낸다. 앞의 [table 2]를 분석하면, 본 논문의 간단한 해결방법은 기존의 계산 복잡도를 증가시키지 않으면서도 여러 공격에 안전한 것을 알 수 있다. 그러므로 본 논문에서의 개선방법은 사용자를 인증하는 안전한 DRM 프로토콜이라고 할 수 있다.

V. Conclusions

본 논문에서는 Hussian et al.의 DRM 인증 프로토콜에 대한 안전성을 분석하였고 그 결과, Yu et al.의 인증 프로토콜과 동일하게 그들의 인증 프로토콜도 내부자 공격, 사용자 가장 공격 등 여러 공격에 안전하지 않았다. 또한 Hussian et al.의 인증 프로토콜은 등록 단계에서 사용자의 ID 중복 문제와 디지털 컨텐츠의 비밀키에 대한 문제도 존재하였다. 그래서 본 논문에서는 이들의 문제점을 해결하기 위한 간단한 개선방법을 제안하였다. 그 중 가장 중요한 기존의 PIDm'의 계산을 간단히 변경하여 안전성을 분석한 결과, 모바일 장치 분실 공격에 안전하고, 그 결과 사용자 가장 공격, 패스워드 추측 공격, 재생 공격 등 여러 공격에 안전하였다. 그러므로 본 논문에서의 개선방법은 DRM을 위한 안전한 사용자 인증 프로토콜이라고 할 수 있다.

REFERENCES

[1] S. Hussian, Y. B. Zikria, G. A. Mallah, C. M. Chen, M. D. Alshehri, F. Ishmanov, and S. Ashraf, "An Improved Authentication Scheme for Digital Rights Management System," Wireless Communications and Mobile Computing, Vol. 2022, pp. 1-11, Jan. 2022. DOI: 10.1155/2022/1041880

[2] C. L. Chen, "A secure and traceable E-DRM system based on mobile device," Expert Systems with Applications, Vol. 35, Issue 3, pp. 878-886, Oct. 2008. DOI: 10.1016/j.eswa.2007.07.029

[3] S. J. Yu, K. S. Park, Y. H. Park, H. P. Kim, and Y. H. Park, "A lightweight three-factor authentication protocol for digital rights management system," Peer-to-Peer Networking and Applications, Vol. 13, pp. 1340-1356, Feb. 2020. DOI : 10.1007/s12083-019-00836-x

[4] C. C. Lee, C. T. Li, Z. W. Chen, and Y. M Lai., "A Biometric-Based Authentication and Anonymity Scheme for Digital Rights Management System," Information Technology and Control, Vol 47, No. 2, pp. 262-274, Apr. 2018. DOI 10.5755/j01.itc.47.2.18506

[5] J. W. Jung, D. W. Kang, D. H. Lee, and D. H. Won, "An Improved and Secure Anonymous Biometric-Based User Authentication with Key Agreement Scheme for the Integrated EPR Information System," PLoS ONE, Vol. 12, No. 1, Jan. 2017. DOI: 10.1371/journal.pone.0169414

[6] Y. Dodis, L. Reyzin and A. Smith, "Fuzzy extractor: how to generate strong keys from biometrics and other noisy data," Advances in Cryptology, EUROCRYPT'04, LNCS Vol. 3027, pp. 523-540, May 2004. DOI: 10.1007/978-3-540-24676-3_31

[7] J. Kim, K. Lee, and D. H. Lee, "An Efficient LWE-Based Reusable Fuzzy Extractor," The Korea Institute of Information Security & Cryptology, Vol. 32, NO. 5, pp. 779-790, Oct. 2022. DOI: 10.13089/JKIISC.2022.32.5.779

[8] M. A. Khan, A. Ghani, M. S. Obaidat, P. Vijayakumar, K. Mansoor, and S. A. Chaudhry, "A robust anonymous authentication scheme using biometrics for digital rights management system," In 2021 International Conference on Communications, Computing, Cyber security, and Informatics (CCCI), pp. 1-5. IEEE, 2021. DOI: 10.1109/CCCI52664.2021.958321

Authors

Mi-Og Park received the M.S. and Ph.D. degrees in Computer Science and Engineering from Soongsil University, Korea, in 1993 and 2004, respectively. Dr. Park joined the faculty of the Department of Computer Engineering at Sungkyul University, Korea, in 2005. She is interested in mobile security, security protocol and IoT security.