Original Research Paper | Computer Science | Volume : 5 ¦ Issue : 9 ¦ Sep 2020 ¦ e-ISSN : 2456-5040

CRYPTANALYSIS OF AN AUTHENTICATION PROTOCOL FOR DIGITAL RIGHTS MANAGEMENT SYSTEM

Zhenghao Li

School of Computer Science and Technology, Tiangong University, China.

ABSTRACT

The latest progress of communication technology and low-power devices has led to in all kinds of resources environment to provide digital content services, such as smart home and the Internet of things. However, digital content is easily replicated and distributed through open channels. Therefore, authentication is becoming more and more important for digital rights management (DRM) systems to provide security services to authorized users.In 2019,SungJin Yu et al. proposed a lightweight three-factor authentication protocol for digital rights management system.This paper introduces the research background of the identity authentication scheme, and reviews the authentication protocol of Sungjin Yu et al. from the perspective of the registration phase and the login authentication phase.Then,through the cryptanalysis, We here prove that the DRM system protocol of SungJin Yu et al. is unsafe, and provide two attack schemes, namely, privileged insider impersonating a legitimate user and privileged insider impersonating a legitimate license server.

KEYWORDS: DRM systems; Protocol; Authentication; Cryptanalysis; Attack schemes.

1. INTRODUCTION:

Due to the development of embedded technology and low-power devices, users can access photos, videos, music, and documents on the Internet of Things (Kim, Lee, & Park, 2010; Liu, Chang, & Chang, 2015; Subramanya & Yi, 2006)at anytime and anywhere. However, this convenient method of access also allows illegal copying and distribution of digital content, as it has been provided through public channels.This issue makes digital rights management (DRM) technology essential for protecting rights related to digital content.In the process of providing digital content services to legitimate users, authentication is an essential security requirement in DRM systems.

More recently in 2017, Jung et al. (Jung, Kang, Lee, & Won, 2017) proposed a biometricbased user authentication and key agreement scheme for electronic patient records (EPR) information systems, which involve a similar architecture to DMR systems. However, in 2018, Lee et al. (Lee, Li, Chen, & Lai, 2018) showed that Jung et al.'s scheme (Jung, Kang, Lee, & Won, 2017) is vulnerable to secret-key disclosure attacks that compromise user anonymity. In addition, Lee et al. (Lee, Li, Chen, & Lai, 2018) proposed a biometric-based authentication scheme for a DRM system to resolve the security problems of Jung et al.'s scheme(Jung, Kang, Lee, & Won, 2017).However,in 2019,SungJin Yu et al. (SungJin Yu, Park, & Kim,2020) demonstrated that Lee et al.'s scheme (Lee, Li, Chen, & Lai, 2018) does not protect against device theft and user impersonation, and proposed a lightweight three-factor authentication protocol for DRM systems that seeks to overcome the shortcomings of Lee et al.'s scheme (Lee, Li, Chen, & Lai, 2018).In the present paper, we proved that the DRM protocol of SungJin Yu et al. (SungJin Yu, Park, & Kim,2020) is vulnerable to attacks through rigorous cryptanalysis, and provided two attack schemes.

2. REVIEW OF SUNGJIN ET AL.'S PROTOCOL:

This section reviews Sungjin Yu et al.'s authentication protocol. The notation used in this paper is explained in Table 1. The proposed protocol consists of three phases: registration, login and authentication, as detailed below.

Table 1: Notations

Notation	Description
U_i	Mobile user
S_j	License server
ID_i	Identity of mobile user
ID_{DC}	Identity of digital content
PW_i	User password
BIO_i	Biometrics of user
R_1	Random nonce of user
R_2	Random nonce of license server
X_S	Master key of license server
KEY_{DC}	Secret key of digital content
$h(\cdot)$	One-way hash function
$H(\cdot)$	Biohashing function
$\oplus$	Bitwise XOR operation
$\|$	Concatenation operation

2.1 Registration phase:

A new mobile user U_i who seeks access to digital-content services must register their identity with the license server S_j.

U_i selects identity ID_i and password PW_i and imprints biometrics BIO_i. Then, U_i computes $Gen(BIO_i) = \langle R_i, P_i \rangle$, and $RPW_i = h(PW_i \| R_i)$ and sends $\{ID_i, RPW_i\}$ to license server S_j via a secure channel.

Upon receiving the registration request message from U_i, license server S_j computes $X_i = h(ID_i \| X_S)$, $d_i = X_i \oplus h(ID_i \| RPW_i)$, $f_i = (RPW_i \| X_i)$. Then, S_j stores ID_i with X_i in a database and sends $\{d_i, f_i\}$ to the user via a secure channel.

After receiving the authentication message from S_j, U_i stores $\{d_i, f_i\}$ in a device.

2.2 Login and authentication phase:

A user U_i who wishes to use the digital content sends a login request message to license server S_j, so that they may mutually authenticate. The goal of this phase is to achieve mutual authentication and distribute the secret key to the content to a legitimate user. The detailed steps are as follows:

U_i inputs identity ID_i and password PW_i and imprints biometric BIO_i. Then, U_i computes $R_i = Rep(BIO_i, P_i)$, $RPW_i = h(PW_i \| R_i)$, $X_i = d_i \oplus h(ID_i \| RPW_i)$, $f_i^* = h(RPW_i \| X_i)$ and checks whether $f_i^* ?= f_i$. If they are equal, U_i generates a random nonce R_1 and computes $M_1 = X_i \oplus R_1$, $M_2 = ID_i \oplus R_1$, $M_3 = ID_{DC} \oplus R_1$, $M_{US} = h(ID_i \| ID_{DC} \| X_i \| R_1)$. Then, U_i sends the login request messages $\{M_1, M_2, M_3, M_{US}\}$ to license server S_j via an open channel.

Upon receiving the login request messages from U_i, S_j computes $R_1 = M_1 \oplus X_i$, $ID_i = M_2 \oplus R_1$, $ID_{DC} = M_3 \oplus R_1$, $M_{US}^* = h(ID_i \| ID_{DC} \| X_i \| R_1)$ and checks whether $M_{US}^* ?= M_{US}$. If it is valid, S_j retrieves KEY_{DC}, generates a random nonce R_2 and computes $M_4 = R_2 \oplus X_i$, $M_5 = KEY_{DC} \oplus X_i$, $M_{SU} = h(ID_i \| X_i \| KEY_{DC} \| R_2)$. Finally, S_j sends $\{M_4, M_5, M_{SU}\}$ to U_i via an open channel.

After receiving the authentication messages from S_j, U_i computes $R_2 = M_4 \oplus X_i$, $KEY_{DC} = M_5 \oplus X_i$, $M_{SU}^* = h(ID_i \| X_i \| KEY_{DC} \| R_2)$. Then, U_i checks whether $M_{SU}^* ?= M_{SU}$ and stores KEY_{DC} in a device.

3. CRYPTANALYSIS OF SUNGJIN ET AL.'S PROTOCOL:

This section uses an informal analysis to assess the security of Sungjin et al.'s protocol. Sungjin Yu et al. claim that their protocol is safe and effective, and can be protected from various types of attacks. However, in the following situations, we have proposed two attack schemes so that their protocol cannot meet the security requirements.

3.1 Privileged insider impersonates a legitimate user:

The privileged attacker U_A obtains $\langle ID_i, X_i \rangle$ from $License\ Server(S_j)$'s database. Next, the attacker U_A can impersonates U_i, the process is as follows:

The attacker U_A randomly selects a random number R_a, and computes $M_1 = X_i \oplus R_a$, $M_2 = ID_i \oplus R_a$. The attacker selects ID_{DC}, and computes $M_3 = ID_{DC} \oplus R_a$, $M_{UaS} = h(ID_i \| ID_{DC} \| X_i \| R_a)$. Then, the attacker sends the message $\{M_1, M_2, M_3, M_{AUS}\}$ to $License\ Server(S_j)$.

After $License\ Server(S_j)$ receives the message $\{M_1, M_2, M_3, M_{AUS}\}$, it can be verified. After S_j retrieves the corresponding KEY_{DC}, calculates $M_4 = R_2 \oplus X_i$, $M_5 = KEY_{DC} \oplus X_i$, $M_{SUa} = h(ID_i \| X_i \| KEY_{DC} \| R_2)$. Then $License\ Server(S_j)$ sends message $\{M_4, M_5, M_{SUa}\}$ to U_A. U_A calculates $KEY_{DC} = M_5 \oplus X_i$, and the attacker U_A obtains the key KEY_{DC} of the digital content. At this point, the attack is complete.

3.2 Privileged insider impersonate a legitimate license server:

The privileged attacker S_A obtains $\langle ID_i, X_i \rangle$ from $License\ Server(S_j)$'s database. When user U_i sends a message $\{M_1, M_2, M_3, M_{US}\}$ to the license server, S_A intercepts the message and impersonates a legitimate server. S_A computes $R_1 = M_1 \oplus X_i$, $ID_i = M_2 \oplus R_1$, $ID_{DC} = M_3 \oplus R_1$. Then, S_A randomly selects KEY_{FAKE} as the key of the digital content to achieve the purpose of destroying the shared key. S_A randomly select a random number R_a and calculate $M_4 = R_a \oplus X_i$, $M_5 = KEY_{FAKE} \oplus X_i$, $M_{SaU} = h(ID_i \| X_i \| KEY_{FAKE} \| R_a)$. Then, S_A sends a message $\{M_4, M_5, M_{SaU}\}$ to U_i. After U_i receiving the message $\{M_4, M_5, M_{SaU}\}$, U_i can pass the verification and obtain the key KEY_{FAKE} of the forged digital content, but cannot successfully obtain the digital content. The attack is complete.

4. CONCLUSIONS:

This paper introduces the research background of the identity authentication scheme. Then we reviewed Sungjin Yu et al.'s scheme and proposed two attack schemes to prove that Sungjin Yu et al.'s scheme is insecure. This paper provides references for other similar programs. The future work is to repair the security flaws on the basis of this paper, so that the digital rights management system can achieve higher security.

REFERENCES:

I. Jung, J., Kang, D., Lee, D., & Won, D. (2017). An Improved and Secure Anonymous Biometric-Based User Authentication with Key Agreement Scheme for the Integrated EPR Information System. Plos One, 12(1), e0169414.

II. Kim, H., Lee, Y., & Park, Y. (2010). A robust and flexible digital rights management system for home networks. Journal of Systems and Software, 83(12), 2431-2440.

III. Lee, C. C., Li, C. T., Chen, Z. W., & Lai, Y. M. (2018). A Biometric-Based Authentication and Anonymity Scheme for Digital Rights Management System. Information technology and control, 47(2).

IV. Liu, Y., Chang, C. C., & Chang, S. C. (2015). A group key distribution system based on the generalized aryabhata remainder theorem for enterprise digital rights management. Journal of Information Hiding & Multimedia Signal Processing, 6(1), 140-153.

V. Subramanya, S. R., & Yi, B. K. (2006). Digital rights management. Potentials IEEE, 25(2), p.31-34.

VI. Yu, S., et al. (2020). A lightweight three-factor authentication protocol for digital rights management system. Peer-to-peer Networking and Applications,1-17.