Journal of Information Security, **2013, 4, 225-233**
http://dx.doi.org/10.4236/jis.2013.44025 Published Online October 2013 (http://www.scirp.org/journal/jis)

On the Security of Anonymous Authentication Protocol for Mobile Pay-TV

Walid I. Khedr
Faculty of Computers and Informatics, Zagazig University, Zagazig, Egypt
Email: wkhedr@zu.edu.eg

Received May 27, 2013; revised June 26, 2013; accepted July 4, 2013

ABSTRACT

One of the promising multimedia services is the mobile pay-TV service. Due to its wireless nature, mobile pay-TV is vulnerable to attacks especially during hand-off. In 2011, an efficient anonymous authentication protocol for mobile pay-TV is proposed. The authors claim that their scheme provides an anonymous authentication to users by preventing intruders from obtaining users' IDs during the mutual authentication between mobile subscribers and head end systems. However, after analysis, it was found that the scheme does not provide anonymous authentication and users can be easily tracked while using their anonymous identity. The scheme is also subject to denial of service attack. In this paper the deficiencies of the original scheme are demonstrated, and then a proposed improved scheme that eliminates these deficiencies is presented.

Keywords: Authentication; Conditional Access Systems; Mobile Pay-TV Services; Privacy

1. Introduction

With the increased integration of pay-TV and wireless communication, multimedia pay service plays an important role in mobile broadcast TV services [1]. As these services are usually delay-sensitive due to high mobility feature and frequent handoffs, a fast and secure authentication scheme for such mobile broadcast TV services should be developed.

In order to reduce the delay introduced by the high mobility features and frequent handoffs and guarantee a secure and convenient access of services by authorized subscribers, a secure access management mechanism is required. This access management is provided by a conditional access system (CAS). A typical model of CAS consists of two parts, a head end system and numerous receivers, and the model is comprised of several important components [2], which include:

- Subscriber Authorization/Management System (SAS/SMS): subsystems responsible for subscriber authorization and management; its works including key management, user authentication, entitlement messages delivery, subscriber information management and rights management.
- Encrypter: a component for enciphering Control Word (CW), keys, or sensitive information.
- Multiplexer (MUX): a component for multiplexing A/V, data or IP into MPEG-2 transport stream.
- Scrambler: a component for signal scrambling.
- Transmitter: a subsystem for signal transmission.
- Receiver: a subscriber device with a CAS module used for access control.

Several CASs have been proposed to guarantee a secure and convenient access of services by authorized subscribers. Many studies have classified these schemes into symmetrical key-based schemes and public key-based schemes.

Public key-based conditional access system [3-5] may realize privacy preservation and avoid communicating with a third party during the handoff process. These methods suffer the heavy computation burden. In [6], a subscriber first has to register his subscriber information with a signature to a provider by applying public key cryptosystem. When a subscriber wants to subscribe to any programs, he uses his device to send a subscription message to the provider. The provider then sends a receipt with a signature for confirming this subscription to the subscriber. However, the scheme [6] only protects the customers' privacy, but not the provider's [2]. In [7], an "e-ticket" scheme for the authentication of pay-TV system is proposed. The scheme employed an encrypted authentication message with a blind and anonymous signature based on RSA public key cryptosystem to do the

mutual-authentication to protect the privacy for both customers and service provider. The schemes proposed in [8] and [9] are based on a public-key cryptosystem employing the technique of the multi-key RSA. While transmitting a requested TV program, the multimedia server and proxy server cooperatively encrypt the requested program without collusion attacks. In public-key cryptosystem each user possess a unique public/private key pair, so a multimedia server has to encrypt services with each user's specific public key which makes them inefficient and not suitable for mobile pay-TV systems.

Symmetrical key-based conditional access system [10-14] suffers from its troublesome key distribution and the involvement of a third party. In [14], an efficient anonymous authentication protocol for mobile pay-TV is proposed. The authors claim that their scheme provides an anonymous authentication to users by preventing intruders from obtaining users IDs during the mutual authentication between mobile subscribers and head end systems. However, after analysis, it was found that the scheme does not provide anonymous authentication and users can be easily tracked while using their anonymous identity. The scheme also is subject to DoS attack.

In this paper an improved scheme that enhances the Chen's scheme [14] is proposed. The deficiencies of the original scheme are demonstrated, and then a proposed improved scheme that eliminates these deficiencies is presented. The proposed scheme ensures the anonymity of the subscribers during handoffs operations, and ensures the anonymous mutual authentication between subscribers and head end systems with low computation and communication costs. Finally a mechanism that prevents denial of service attack is proposed.

The rest of this paper is organized as follows: Section 2 briefly reviews the Chen's scheme. Section 3 presents the security analysis of Chen's scheme. Section 4 presents the improved scheme. The security analysis and performance evaluation of the improved scheme are presented in Section 5. Finally, Section 6 concludes the paper.

2. Review of the Chen's Scheme

The scheme proposed in [14] introduced an efficient and anonymous mutual authentication protocol that eliminates the high computational cost and prevents security attacks introduced in a previous related protocol [15]. There are four phases in Chen's scheme, which includes initialization, issue, subscription and hand-off Phase.

2.1. Initialization Phase

This phase is invoked whenever user U_i registers to the subscribers' database server (DBS) of HES via Subscriber Authorization System and Subscriber Management System (SAS/SMS) and the DBS saves U_i's identity ID. Both U_i and HES uses a set-top-box (STB) as a secure channel during this phase. The following steps are performed to complete this phase [14]:

1) U_i chooses his ID_i and pw_i and generates a random number b for calculating $PWB = h(pw_i, b)$. Then, U_i submits ID_i and PWB to the pay-TV system server S.

2) S checks the database whether his ID_i is already in the database or not. If ID_i is already in the database, S checks whether U_i performs a re-registration or not. If U_i performs a re-registration then S sets ID_i's registration number $N = N + 1$ and updates ID_i and N in the database otherwise S suggests U_i to choose another ID_i. If ID_i is not in the database then S sets $N = 0$ and stores values of ID_i and N in the database.

3) S calculates K, UD, Q and K, UD, Q and R, where:

$K = h(ID_i \oplus PWD)$,

$UD = h(ID_i \| N)$,

$Q = h(UD \| x) \oplus PWB$,

$R = h(PWB \| ID)_i \oplus h(y)$, where y is the secret key of the remote server stored in the hash function and x is the secret key of S.

4) S issues a smart card containing [K, R, Q] to U_i over a secure channel.

5) U_i stores the random number b on the smart card. Such that the smart card contains [K, R, Q, b].

2.2. Issue Phase

Assume that U_i's mobile subscriber device (MS_i) asks a service R_t and the HES performs this authentication process of issue phase for U_i to obtain a right code θ_i. The statements are described as follows:

1) U_i enters his ID_i and PW_i in order to login for obtaining the service, MS_i performs the following computations.

- Calculates PWB and $h(ID_i \oplus PWD)$ to verify whether $K = h(ID_i \oplus PWD)$. If it does not hold, MS_i terminates the request.
- Calculates $P = Q \oplus PWB = h(UD \| x)$ and

  $h(y) = h(PWB \| ID_i) \oplus R$
- Generates a random number n_i and calculates:

  $R_i = R_t \oplus h(y \| n_i)$, $CID_i = ID_i \oplus h(y \| T_i \| n_i)$

  $C_i = h(P \| CID_i \| T_i \| n_i)$.

  Here T_1 is the current timestamp
- Sends the message $m = [R_i, C_i, CID_i, T_1, n_i]$ to HES.

2) *HES* receives the message at the timestamp T_2 and performs the following computations:

- Checks the validity of $(T_2 - T)_1 \le \Delta T$. If it does not hold, HES terminates the request.

- Calculates $ID_i = CID_i \oplus h(y \| T_1 \| n_i)$ and verifies if ID_i is a valid user's identity. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of N in the database and calculates $P' = h(UD \| x)$, where $UD = h(ID_i \| N)$.
- Calculates $C_i' = h(P' \| CID_i \| T_1 \| n_i)$ and checks whether $C_i' = C_i$. If they are equal, *HES* accepts U_i's request of authentication.
- Calculates $R_t = R_i \oplus h(y \| n_i)$
- Then, HES chooses a token θ_i for U_i and stores it into DBS, and calculates:
  $D_i = h(P' \| CID_i \| T_2 \| n_i)$ $E_i = \theta_i \oplus h(P' \| T_2 \| n_i)$.
- Broadcasts the mutual authentication message $m_2 = [D_i, E_i, T_2]$.

3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3 - T_2) \le \Delta T$. If it does not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.

- Calculates $D_i' = h(P \| CID_i \| T_2 \| n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts HES's request of mutual authentication.
- U_i calculates the certified token $\theta_i = E_i \oplus h(P \| T_2 \| n_i)$ as the authentication session key to get service of the pay-TV system.

2.3. Subscription Phase

After obtaining a right code θ_i, U_i's MS_i asks a service R_t using θ_i and the *HES* performs this authentication process. The statements are described as follows:

1) U_i entries his ID_i and PW_i in order to login for obtaining the service, MS_i performs the following computations.

- Calculates PWB and $h(ID_i \oplus PWD)$ to verify whether $K = h(ID_i \oplus PWD)$. If it does not hold, MS_i terminates the request.
- Calculates $P = Q \oplus PWB = h(UD \| x)$ and $h(y) = h(PWB \| ID)_i \oplus R$.
- Generates a random number n_i and calculates:
  $R_i = \theta_t \oplus h(y \| n_i)$, $CID_i = ID_i \oplus h(y \| T_1 \| n_i)$
  $C_i = h(P \| CID_i \| T_i \| n_i)$.
  Here T_1 is the current timestamp
- Sends the message $m = [R_i, C_i, CID_i, T_1, n_i]$ to HES.

2) *HES* receives the message at the timestamp T_2 and performs the following computations:

- Checks the validity of $(T_2 - T_1) \le \Delta T$. If it does not hold, HES terminates the request.
- Calculates $ID_i = CID_i \oplus h(y \| T_1 \| n_i)$ and verifies if ID_i is a valid user's identity. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of N in the database and calculates $P' = h(UD \| x)$, where $UD = h(ID_i \| N)$.
- Calculates $C_i' = h(P' \| CID_i \| T_1 \| n_i)$ and checks whether $C_i' = C_i$. If they are equal, *HES* accepts U_i's request of authentication.
- Calculates $\theta_t = R_i \oplus h(y \| n_i)$.
- Then, HES chooses a token γ_i for U_i and calculates $D_i = h(P' \| CID_i \| T_2 \| n_i)$ and $E_i = \gamma_i \oplus h(P' \| T_2 \| n_i)$.
- Broadcasts the mutual authentication message $m_2 = [D_i, E_i, T_2]$.

3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3 - T_2) \le \Delta T$. If it does not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.

- Calculates $D_i' = h(P \| CID_i \| T_2 \| n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts HES's request of mutual authentication.
- U_i calculates the certified token $\gamma_i = E_i \oplus h(P \| T_2 \| n_i)$ as the authentication session key to get service of the pay-TV system.

2.4. Hand-Off Phase

When MS_i moves to a new coverage area that older HES cannot support such that a hand-off occurs, MS_i needs to performer-authentication without re-login. The statements are described as follows:

1) MS_i performs the following computations:

- Generates a random number n_i and calculates:
  $Z_i = \theta_i \oplus h(y \| n_i)$, $CID_i = ID_i \oplus h(y \| T_1 \| n_i)$
  $C_i = h(P \| CID_i \| T_i \| n_i)$.
  Here T_1 is the current timestamp
- Sends the message $m = [Z_i, C_i, CID_i, T_1, n_i]$ to HES.

2) *HES* receives the message at the timestamp T_2 and performs the following computations:

- Checks the validity of $(T_2 - T_1) \le \Delta T$. If it does not hold, HES terminates the request.
- Calculates $ID_i = CID_i \oplus h(y \| T_1 \| n_i)$ and verifies if ID_i is a valid user's identity. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of N in the database and calculates $P' = h(UD \| x)$, where $UD = h(ID_i \| N)$.
- Calculates $C_i' = h(P' \| CID_i \| T_1 \| n_i)$ and checks whether $C_i' = C_i$. If they are equal, *HES* accepts U_i's request of authentication.
- Calculates $\theta_i = Z_i \oplus h(y \| n_i)$
- Then, HES chooses a token γ_i for U_i and calculates $D_i = h(P' \| CID_i \| T_2 \| n_i)$ and $F_i = \gamma_i \oplus h(P' \| T_2 \| n_i)$

- Broadcasts the mutual authentication message $m_2 = [D_i, F_i, T_2]$

3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3 - T_2) \le \Delta T$. If it does not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.

- Calculates $D_i' = h(P \| CID_i \| T_2 \| n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts HES's request of mutual authentication.
- U_i calculates the certified token $\gamma_i = F_i \oplus h(P \| T_2 \| n_i)$ to obtain new HES's service.

3. Security Analysis of Chen's Scheme

In [14] the authors claim several security properties such as anonymous service, mutual authentication, resisting replay attacks, resisting man-in-the-middle-attack, and forgery difficulty. However, in this section, it is shown that Chen's scheme vulnerable to man-in-the-middle-attack which leads to DoS attack. It is al so found that the scheme does not provide anonymous service. The aforementioned weaknesses are presented in detail as follows.

3.1. Corrections to Chen's Scheme

Before we present the weakness of Chen's scheme, there are some mistakes in the scheme that should be corrected. In step 3 of the initialization phase (Section 2.1), the system server S calculates *R* using the following equation:

$$R = h(PWB \| ID_i) \oplus h(y) \quad (1)$$

Here, *y* is a secret key of the remote server S which is stored in the hash function and known only to S.

In step 1 of the issue phase (Section 2.2), the mobile subscriber MS extracts $h(y)$ from *R* by computing $h(y) = h(PWB \| ID_i) \oplus R$ and use it to compute R_i and CID_i as follows:

$$R_i = R_t \oplus h(y \| n_i) \quad (2)$$

$$CID_i = ID_i \oplus h(y \| T_1 \| n_i) \quad (3)$$

As shown in Equations (2) and (3), the authors use $h(y \| n_i)$ and $h(y \| T_1 \| n_i)$ to compute R_i and CID_i respectively, which is not possible; since the MS_i does not know the secret key *y* to be able to compute $h(y \| n_i)$ and $h(y \| T_1 \| n_i)$. So, the MS could not compute R_i and CID_i as $h(y \| n_i)$ and $h(y \| T_1 \| n_i)$ are one way hash functions *i.e.* it is not possible to extract *y* from both $h(y \| n_i)$ and $h(y \| T_1 \| n_i)$. The same mistake is found in step 1 of the subscription phase (Section 2.3) and step 1 of the hand-off phase (Section 2.4) when computing (R_i, CID_i) and (Z_i, CID_i) respectively. To correct this mistake, the MS should replace *y* by $h(y)$ in Equations (2) and (3). This mistake can also be corrected by just replacing $h(y)$ by *y* in Equation (1) in the initialization phase *i.e.* $R = h(PWB \| ID_i) \oplus y$. We chose the second option.

3.2. Attack on Anonymous Service

The Chen's scheme is subject to MS tracking attack. This attack can be performed as follows:

1) An attacker A registers to the subscribers' database server (DBS) like any other user and chooses his ID_A and pw_A and generates a random number *b* for calculating $PWB = h(pw_A, b)$. Then, A submits ID_A and *PWB* to the pay-TV system server *S.*

2) S calculates:

$K = h(ID_A \oplus PWD)$

$UD = h(ID_A \| N)$

$Q = h(UD \| x) \oplus PWB$

$R = h(PWB \| ID_i) \oplus y$.

S issues a smart card containing [*K*, *R*, *Q*] to *A* over a secure channel.

3) The attacker *A* reads *R* from its smart card and compute $y = h(PWB \| ID_A) \oplus R$.

Note that based on the corrections presented in section 3.1, $h(y)$ is replaced by y in the step 2. Using the computed y the attacker A can perform MS tracing attack during issue phase, subscription or hand-off phases as follows:

1) The attacker *A* intercept message *m* during any of the three phases and extracts CID_i, T_1 and n_i from *m*. Using these three values and the computed y, the attacker can compute the MS' *ID* (ID_i) as follows:

$$ID_i = CID_i \oplus h(y \| T_1 \| n_i) \quad (4)$$

This allows the attacker to track MS_i; since ID_i is a fixed value for each user U_i.

2) The attacker *A* can also know the service R_t that the MS_i asked from HES by intercepting message *m* during the issue phase and extracting R_i and n_i from *m*. Using these two values and the computed y, the attacker can compute R_i as follows:

$$R_t = R_i \oplus h(y \| n_i) \quad (5)$$

3) The attacker *A* can also know the right code θ_i that used by MS_i to access service R_t by intercepting message *m* during the subscription or the hand-off phases and extracting (R_i, n_i) or (Z_i, n_i) respectively from *m*. Using either of these two values and the computed y, the attacker can compute θ_i as follows:

$$\theta_i = R_i \oplus h\left(y \| n_i\right) \quad (6)$$

$$\theta_i = Z_i \oplus h\left(y \| n_i\right) \quad (7)$$

3.3. Denial of Service Attack

The scheme is subject to denial of service attack. This attack can be performed through two methods. The first method can be performed during the subscription and hand-off phases by applying man-in-the-middle attack as follows:

1) The attacker A intercept message m_2 during any of the two phases and extract:

$E_i = \gamma_i \oplus h\left(P' \| T_2 \| n_i\right)$ or

$F_i = \gamma_i \oplus h\left(P' \| T_2 \| n_i\right)$ respectively.

2) The attacker generates a random session key γ_A and computes:

- $E_i' = \gamma_A \oplus E_i = \gamma_A \oplus \gamma_i \oplus h\left(P' \| T_2 \| n_i\right)$
  $= \gamma_i' \oplus h\left(P' \| T_2 \| n_i\right)$ or
- $F_i' = \gamma_A \oplus F_i = \gamma_A \oplus \gamma_i \oplus h\left(P' \| T_2 \| n_i\right)$
  $= \gamma_i' \oplus h\left(P' \| T_2 \| n_i\right)$

3) After receiving message m_2, U_i calculates the session key:

- $\gamma_i' = E_i \oplus h\left(P \| T_2 \| n_i\right)$ or
- $\gamma_i' = F_i \oplus h\left(P \| T_2 \| n_i\right)$

This results in U_i and *HES* using different session keys (γ', γ respectively) which prevent U_i from getting the service of the pay-TV system.

The second method can be performed during the hand-off phase as follows:

1) The attacker uses a rogue HES to transmit messages using a high signal strength in order to force MS_i to discard the signal sent by the legitimate HES and roam with the rogue HES.

2) When MS_i roam with the rogue HES, it needs to perform re-authentication without re-login by sending $m: Z_i, C_i, CID_i, T_1, n_i$, where:

$Z_i = \theta_i \oplus h\left(y \| n_i\right)$

$CID_i = ID_i \oplus h\left(y \| T_1 \| n_i\right)$

$C_i = h\left(P \| CID_i \| T_1 \| n_i\right)$.

3) The rogue HES receives the message and immediately reply with message $m_2: D_i, F_i', T_1$, where $D_i = C_i = h\left(P \| CID_i \| T_1 \| n_i\right)$ and F_i' is a random value generated by the rogue HES.

4) After receiving message m_2 at the time T_3, U_i checks the validity of $\left(T_3 - T_1\right) \le \Delta T$ which should hold; since $\left(T_3 - T_1\right)$ should equal to the round trip time (RTT) between U_i and the rogue HES. Note that ΔT should be less than or equal to 200 milliseconds as stated in [16]. It is clear that the RTT between U_i and the rogue HES is less than 200 milliseconds; since they are within the transmission range of each other.

5) U_i calculates $D_i' = h\left(P \| CID_i \| T_1 \| n_i\right)$ and checks whether $D_i' = D_i$ and accepts the rogue HES's request of mutual authentication.

6) U_i calculates the false authentication session key $\gamma_i' = F_i' \oplus h\left(P \| T_1 \| n_i\right)$, which prevents U_i from getting the service of the pay-TV system.

4. The Improved Scheme

To withstand the above attacks, we propose an improved scheme based on the original Chen's scheme [14] with lightweight modifications. The improved scheme introduces few modifications to the four phases as follows.

4.1. Initialization Phase

As assumed in [14], both S and its HESs share a secret key x. Both U_i and HES use a set-top-box (STB) as a secure channel during this phase. The following steps are performed to complete this phase:

1) U_i chooses his ID_i and pw_i and generates a random number b for calculating $PWB = h\left(pw_i, b\right)$. Then, U_i submits ID_i and PWB to the pay-TV system server S.

2) S checks the database whether his ID_i is already in the database or not. If ID_i is already in the database, S checks whether U_i performs a re-registration or not. If U_i performs a re- registration then S sets ID_i's registration number $N = N + 1$ and updates ID_i and N in the database otherwise S suggests U_i to choose another ID_i. If ID_i is not in the database then S sets $N = 0$ and stores values of ID_i and N in the database.

3) S calculates the following values:

- $K = h\left(ID_i \oplus PWD\right)$
- A user authentication key for each user $y_i = h\left(x \| ID_i\right)$, where x is the secret key of S.
- A new permutation of the MS_i's ID ($CID_i^1 = h\left(y_i, ID_i\right)$) to be used by MS_i's as a new ID during the next communication with the HES.
- $UD = h\left(CID_i^1 \| N\right)$, $P_i^1 = h\left(UD \| x\right)$ and $Q = E_{y_i}\left(P_i^1\right)$
- $k_i^1 = h\left(x \| CID_i^1\right)$, $z_i^1 = E_{k_i^1}\left(CID_i^1, y_i\right)$ and $R = h\left(PWB \| ID_i\right) \oplus y_i$

4) S sends $\left[K, R, Q, z_i^1\right]$ to U_i over the secure channel.

5) U_i computes $y_i = h\left(PWB \| ID_i\right) \oplus R$ and stores $\left[K, R, Q, z_i^1, b, y_i\right]$.

The user U_i uses CID_i^1 to identify itself to the next HES during the issue phase, the subscription phase or the

hand-off phase. This new ID should be known to the next HES to be able to authenticate U_i. So, the current HES encrypt the new ID (CID_i^1) along with user authentication key y_i and send it to U_i which sends it to the next HES in the next phase. Note that only HESs can decrypt z_i^1; since the decryption key k_i^1 is generated using the secret key x which is only known to the server S and its HESs.

4.2. Issue Phase

Assume that U_i's mobile subscriber device (MS_i) asks a service R_t and the HES performs this authentication process of issue phase for U_i to obtain a right code θ_i. The statements are described as follows:

1) U_i enters his ID_i and PW_i in order to login for obtaining the service, MS_i performs the following computations.

- Calculates PWB and $h(ID_i \oplus PWD)$ to verify whether $K = h(ID_i \oplus PWD)$. If it does not hold, MS_i terminates the request.
- Calculates $P_i^1 = D_{y_i}(Q)$
- Generates a random number n_i and calculates:

  $R_i = R_t \oplus h(y_i \| n_i)$

  $CID_i^1 = h(y_i, ID_i)$

  $C_i = h(P_i^1 \| CID_i^1 \| T_i \| n_i)$.

  Here T_1 is the current timestamp
- Sends the message m to HES:

  $(m: R_i, C_i, CID_i^1, T_1, z_i^1, n_i) | HMAC(y_i, m)$

Here $HMAC(y_i, m)$ is the HMAC of the message m using the key y_i

2) *HES* receives the message at the timestamp T_2 and performs the following computations:

- Checks the validity of $(T_2 - T_1) \le \Delta T$. If it does not hold, HES terminates the request.
- To validate the $HMAC$ and the new ID (CID_i^1), *HES* calculates $k_i^1 = h(x \| CID_i^1)$ and $D_{k_i^1}(z_i^1) = (CID_i'^1, y_i)$ to get the user authentication key y_i.
- Uses y_i to validate $HMAC(y_i, m)$ then checks whether the computed $CID_i'^1$ equal to CID_i^1. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of N in the database and calculates $P_i'^1 = h(UD \| x) = h(h(CID_i^1 \| N) \| x)$.
- Calculates $C_i' = h(P_i'^1 \| CID_i^1 \| T_1 \| n_i)$ and checks whether $C_i' = C_i$. If they are equal, *HES* accepts U_i's request of authentication.
- Calculates $R_t = R_i \oplus h(y_i \| n_i)$
- Then, *HES* chooses a token θ_i for U_i and stores it into DBS, and calculates:

  $D_i = h(P_i'^1 \| CID_i^1 \| T_2 \| n_i)$ $E_i = \theta_i \oplus h(P_i'^1 \| T_2 \| n_i)$
- Computes a new permutation of the MS_i's ID ($CID_i^2 = h(y_i, CID_i^1)$) to be used by MS_i's as a new ID during the next communication with the HES.
- Compute $UD = h(CID_i^2 \| N)$, $P_i^2 = h(UD \| x)$ and $Q = E_{y_i}(P_i^2)$.
- $k_i^2 = h(x \| CID_i^2)$, $z_i^2 = E_{k_i^2}(CID_i^2, y_i)$.
- Broadcasts the mutual authentication message $(m_2: D_i, E_i, T_2, Q, z_i^2) | HMAC(y_i, m_2)$.

3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3 - T_2) \le \Delta T$ and uses y_i to validate the *HMAC*. If they do not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.

- Calculates $D_i' = h(P_i^1 \| CID_i^1 \| T_2 \| n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts HES's request of mutual authentication.
- U_i calculates the certified token $\theta_i = E_i \oplus h(P_i^1 \| T_2 \| n_i)$ as the authentication session key to get service of the pay-TV system.
- U_i stores $Q = E_{y_i}(P_i^2)$, θ_i, CID_i^1 and z_i^2.

4.3. Subscription Phase

After obtaining a right code θ_i, U_i's MS_i asks a service R_t using θ_i and the *HES* performs this authentication process. The statements are described as follows:

1) U_i entries his ID_i and PW_i in order to login for obtaining the service, MS_i performs the following computations.

- Calculates PWB and $h(ID_i \oplus PWD)$ to verify whether $K = h(ID_i \oplus PWD)$. If it does not hold, MS_i terminates the request.
- Calculates $D_{y_i}(Q) = P_i^2$.
- Generates a random number n_i and calculates $R_i = \theta_i \oplus h(y_i \| n_i)$, $CID_i^2 = h(y_i, CID_i^1)$ and $C_i = h(P_i^2 \| CID_i^2 \| T_1 \| n_i)$. Here T_1 is the current timestamp.
- Sends the message m to HES: $(m: R_t, C_i, CID_i^2, T_1, z_i^2, n_i) | HMAC(y_i, m)$.

2) *HES* receives the message at the timestamp T_2 and performs the following computations:

- Checks the validity of $(T_2 - T)_1 \le \Delta T$. If it does not hold, HES terminates the request.
- To validate the $HMAC$ and the new ID (CID_i^2), *HES* calculates $k_i^2 = h(x \| CID_i^2)$ and $D_{k_i^2}(z_i^2) = (CID_i'^2, y_i)$ to get the user authentication

key y_i.

- Uses y_i to validate $HMAC(y_i, m)$ then checks whether the computed $CID_i'^2$ equal to CID_i^2. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of *N* in the database and calculates $P_i'^2 = h(UD \| x) = h(h(CID_i^2 \| N) \| x)$.
- Calculates $C_i' = h(P_i'^2 \| CID_i^2 \| T_1 \| n_i)$ and checks whether $C_i' = C_i$. If they are equal, *HES* accepts U_i's request of authentication.
- Calculates $\theta_i = R_i \oplus h(y_i \| n_i)$.
- Then, HES chooses a token γ_i for U_i and calculates $D_i = h(P_i'^2 \| CID_i^2 \| T_2 \| n_i)$ and $E_i = \gamma_i \oplus h(P_i'^2 \| T_2 \| n_i)$.
- Computes a new permutation of the MS_i's ID ($CID_i^3 = h(y_i, CID_i^2)$) to be used by MS_i's as a new ID during the next communication with the HES.
- Computes $UD = h(CID_i^3 \| N)$, $P_i^3 = h(UD \| x)$ and $Q = E_{y_i}(P_i^3)$.
- $k_i^3 = h(x \| CID_i^3)$, $z_i^3 = E_{k_i^3}(CID_i^3, y_i)$.
- Broadcasts the mutual authentication message $(m_2 : D_i, E_i, T_2, Q, z_i^3) | HMAC(y_i, m2)$.

3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3 - T_2) \le \Delta T$ and uses y_i to validate the *HMAC*. If they do not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.

- Calculates $D_i' = h(P_i^2 \| CID_i^2 \| T_2 \| n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts HES's request of mutual authentication.
- U_i calculates the certified token $\gamma_i = E_i \oplus h(P_i^2 \| T_2 \| n_i)$ as the authentication session key to get service of the pay-TV system.
- U_i stores $Q = E_{y_i}(P_i^3)$, γ_i, CID_i^2 and z_i^3.

4.4. Hand-off Phase

When MS_i moves to a new coverage area that older HES cannot support such that a hand-off occurs, MS_i needs to performer-authentication without re-login. The statements are described as follows:

1) MS_i performs the following computations:

- Calculates $D_{y_i}(Q) = P_i^3$.
- Generates a random number n_i and calculates $Z_i = \theta_i \oplus h(y_i \| n_i)$, $CID_i^3 = h(y_i, CID_i^2)$ and $C_i = h(P_i^3 \| CID_i^3 \| T_1 \| n_i)$. Here T_1 is the current timestamp.
- Sends the message *m* to HES: $(m : Z_i, C_i, CID_i^3, T_1, z_i^3, n_i) | HMAC(y_i, m)$.

2) *HES* receives the message at the timestamp T_2 and performs the following computations:

- Checks the validity of $(T_2 - T)_1 \le \Delta T$. If it does not hold, HES terminates the request.
- To validate the *HMAC* and the new ID (CID_i^3), *HES* calculates $k_i^3 = h(x \| CID_i^3)$ and $D_{k_i^3}(z_i^3) = (CID_i'^3, y_i)$ to get the user authentication key y_i.
- Uses y_i to validate $HMAC(y_i, m)$ then checks whether the computed $CID_i'^3$ equal to CID_i^3. If it does not hold, *HES* terminates the login request, otherwise *HES* checks the value of *N* in the database and calculates $P_i'^3 = h(UD \| x) = h(h(CID_i^3 \| N) \| x)$.
- Calculates $C_i' = h(P_i'^3 \| CID_i^3 \| T_1 \| n_i)$ and checks whether $C_i' = C_i$. If they are equal, *HES* accepts U_i's request of authentication.
- Calculates $\theta_i = Z_i \oplus h(y_i \| n_i)$
- Then, HES chooses a token γ_i for U_i and calculates $D_i = h(P_i'^3 \| CID_i^3 \| T_2 \| n_i)$ and $F_i = \gamma_i \oplus h(P_i'^3 \| T_2 \| n_i)$
- Computes a new permutation of the MS_i's ID ($CID_i^4 = h(y_i, CID_i^3)$) to be used by MS_i's as a new ID during the next communication with the HES.
- Computes $UD = h(CID_i^4 \| N)$, $P_i^4 = h(UD \| x)$ and $Q = E_{y_i}(P_i^4)$
- $k_i^4 = h(x \| CID_i^4)$, $z_i^4 = E_{k_i^4}(CID_i^4, y_i)$.
- Broadcasts the mutual authentication message $(m_2 : D_i, F_i, T_2, Q, z_i^4) | HMAC(y_i, m2)$.

3) After receiving message m_2 at the time T_3, U_i checks the validity of $(T_3 - T_2) \le \Delta T$ and uses y_i to validate the *HMAC*. If they do not hold, U_i terminates the request. Otherwise, U_i executes the following operations to authenticate *HES*.

- Calculates $D_i' = h(P_i^3 \| CID_i^3 \| T_2 \| n_i)$ and checks whether $D_i' = D_i$. If they are equal, U_i accepts HES's request of mutual authentication.
- U_i calculates the certified token $\gamma_i = F_i \oplus h(P_i^3 \| T_2 \| n_i)$ as the authentication session key to get service of the pay-TV system.
- U_i stores $Q = E_{y_i}(P_i^4)$, γ_i, CID_i^3 and z_i^4.

5. Security and Performance Analysis

In this section, the security of the proposed improved scheme with respect to the resistance to user tracking and denial of service attack is analyzed. This section also evaluates the performance of the proposed scheme.

5.1. Resistance to User Tracking

The proposed improved scheme prevents user tracking by ensuring the anonymity feature of users. As discussed in Section 3.2, an attacker can track a legitimate user by registering himself to the subscribers' database server (DBS) like any other user, then receives $R = h(PWB \| ID_i) \oplus y$ which is used by the attacker to compute $y = h(PWB \| ID_A) \oplus R$. Using the computed y the attacker A can perform MS tracing attack as described in Section 3.2. The attacker is able to perform this attack; because the server S uses the same secret y to compute the R values for all users. So, if the attacker extracts y from his R value, he can use the same y to extract the IDs of other uses.

In the proposed scheme, the server S generate a unique user authentication key $y_i = h(x \| ID_i)$ for each user using the hash of the user ID and the server's own secret key x. This prevent an attacker A form using his user authentication key (y_A) to extract the IDs of other uses. The proposed scheme also preserves users' privacy by using pseudo identity, CID_i^j to identify users. This pseudo identity generated using a one-way function combined with the user authentication key, y_i, and the user's previous CID_i^{j-1}: $CID_i^j = h(y_i, CID_i^{j-1})$ and is updated in each phase. So, it is impossible to anticipate the messages of the user each phase which guarantees indistinguishability. Also the integrity of messages exchanged between users and HES is guaranteed due to the use of timestamps and the HMAC of each message which is included with the message. The HMAC value is computed using the user authentication key (y_i) which is only known to U_i and HES.

5.2. Resistance to Denial of Service Attack

As discussed in Section 3.3, Chen's scheme is subject to denial of service attack. The attacker can perform this attack because the integrity of message m_2 of the subscription and hand-off phases is not guaranteed. So, an attacker can easily modify E_i or F_i during the subscription or hand-off phases without being detected by U_i which prevents him from getting the service of the pay-TV system.

In the proposed scheme, the integrity of messages exchanged between users and HES is guaranteed due to the use of timestamps and the HMAC of each message which is included with the message. The HMAC value is computed using the user authentication key, (y_i) which is only known to U_i and HES. This prevents the DoS attack that can be launched against the Chen's scheme as described in Section 3.3. This also prevents the attacker from making an impersonation attack and replay attacks using the open values and some modified values.

5.3. Performance Analysis

This section evaluates the performance of the proposed scheme. To analyze the efficiency of the proposed scheme, the proposed scheme is compared with the Chen's scheme [14]. The efficiency of the proposed scheme is analyzed with the same metrics used in Chen's scheme analysis. We define the notation t_H as the hash computation time and t_E as the symmetric encryption/decryption time. The four phases of both the Chen's scheme and the proposed scheme are simulated and implemented using OpenSSL library [17] on an Intel Dual- Core CPU at 2.30 GHz. **Table 1** shows a comparison between the Chen's scheme and the proposed scheme with respect to the hash computation time and the symmetric encryption/ decryption time. Note that we neglect the XOR operation since it is an extremely light-weight one. As shown in **Table 1**, the proposed scheme takes the following extra operation for each phase:

- It takes extra 3 hash operations and more two symmetric encryption/decryption about extra 62 μs for the initialization phase.
- It takes extra 6 hash operations and more four symmetric encryption/decryption about extra 81 μs for the issue phase.
- It takes extra 6 hash operations and more four symmetric encryption/decryption about extra 81 μs for the subscription phase.
- It takes extra 8 hash operations and more four symmetric encryption/decryption about extra 89 μs for the hand-off phase.

This indicates that the proposed scheme introduces a minor increase in computation overhead, which is the cost to enhance the security of the original scheme.

6. Conclusion

Recently, an efficient anonymous authentication protocol for mobile pay-TV is proposed [14]. However, the scheme is vulnerable to user tracking attack and denial of service attack. An improved scheme is proposed to prevent these two attacks by lightweight modifications and, thus, can be applied in environments requiring a high level of security. The improved scheme introduces a minor increase in computation overhead and maintains the

Table 1. Performance comparison.

Phase	Chen's Scheme	Proposed Scheme
Initialization	$6t_H = 30\mu s$	$9t_H + 2t_E = 92\mu s$
Issue	$16t_H = 67\mu s$	$22t_H + 4t_E = 148\mu s$
Subscription	$16t_H = 67\mu s$	$22t_H + 4t_E = 148\mu s$
Hand-off	$12t_H = 52\mu s$	$20t_H + 4t_E = 141\mu s$

same number of messages of the original scheme.

REFERENCES

[1] H. S. L. Pequeno, G. A. M. Gomes, R. M. C. Andrade, J. N. de Souza and M. F. de Castro, "FrameIDTV: A Framework for Developing Interactive Applications on Digital Television Environments," *Journal of Network and Computer Applications*, Vol. 33, No. 4, 2010, pp. 503-511.

[2] H.-M. Sun and M.-C. Leu, "An Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems," *IEEE Transactions on Multimedia*, Vol. 11, No. 5, 2009, pp. 947-959. http://dx.doi.org/10.1109/TMM.2009.2021790

[3] X. Li, J. Niu, M. Khurram Khan and J. Liao, "An Enhanced Smart Card Based Remote User Password Authentication Scheme," *Journal of Network and Computer Applications*, Vol. 36, No. 5, 2013, pp. 1365-1371.

[4] X. Li, Y. Xiong, J. Ma and W. Wang, "An Efficient and Security Dynamic Identity Based Authentication Protocol for Multi-Server Architecture Using Smart Cards," *Journal of Network and Computer Applications*, Vol. 35, No. 2, 2012, pp. 763-769.

[5] Z. Tan, "A Lightweight Conditional Privacy-Preserving Authentication and Access Control Scheme for Pervasive Computing Environments," *Journal of Network and Computer Applications*, Vol. 35, No. 6, 2012, pp. 1839-1846.

[6] N.-Y. Lee, C.-C. Chang, C.-L. Lin and T. Hwang, "Privacy and Non-Repudiation on Pay-TV Systems," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, 2000, pp. 20-27. http://dx.doi.org/10.1109/30.826376

[7] R. Song and L. Korba, "Pay-TV System with Strong Privacy and Non-Repudiation Protection," *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, 2003, pp. 408-413. http://dx.doi.org/10.1109/TCE.2003.1209533

[8] S. F. Yeung, J. C. Lui and D. K. Yau, "A Multikey Secure Multimedia Proxy Using Asymmetric Reversible Parametric Sequences: Theory, Design and Implementation," *IEEE Transactions on Multimedia*, Vol. 7, No. 2, 2005, pp. 330-338. http://dx.doi.org/10.1109/TMM.2005.843361

[9] H. Roh and S. Jung, "An Authentication Scheme for Consumer Electronic Devices Accessing Mobile IPTV Service From Home Networks," 2011 *IEEE International Conference on Consumer Electronics* (*ICCE*), Las Vegas, 9-12 January 2011, pp. 717-718.

[10] Y.-L. Huang, S. Shieh, F.-S. Ho and J.-C. Wang, "Efficient Key Distribution Schemes for Secure Media Delivery in Pay-TV Systems," *IEEE Transactions on Multimedia*, Vol. 6, No. 5, 2004, pp. 760-769. http://dx.doi.org/10.1109/TMM.2004.834861

[11] H.-M. Sun, C.-M. Chen and C.-Z. Shieh, "Flexible-Pay-per-Channel: A New Model for Content Access Control in Pay-TV Broadcasting Systems," *IEEE Transactions on Multimedia*, Vol. 10, No. 5, 2008, pp. 1109-1120. http://dx.doi.org/10.1109/TMM.2008.2001381

[12] R. Di Pietro and R. Molva, "An Optimal Probabilistic Solution for Information Confinement, Privacy, and Security in RFID Systems," *Journal of Network and Computer Applications*, Vol. 34, No. 3, 2011, pp. 853-863.

[13] W. I. Khedr, "SRFID: A Hash-Based Security Scheme for Low Cost RFID Systems," *Egyptian Informatics Journal*, Vol. 14, No. 1, 2013, pp. 89-98.

[14] T.-H. Chen, Y.-C. Chen, W.-K. Shih and H.-W. Wei, "An Efficient Anonymous Authentication Protocol for Mobile Pay-TV," *Journal of Network and Computer Applications*, Vol. 34, No. 4, 2011, pp. 1131-1137.

[15] J.-H. Yang and C.-C. Chang, "An ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem," *Computers & Security*, Vol. 28, No. 3-4, 2009, pp. 138-143. http://dx.doi.org/10.1016/j.cose.2008.11.008

[16] WMF-T33-107-R020v02, "Architecture, detailed Protocols and Procedures," 2012.

[17] OpenSSL, "OpenSSL 1.0.1e," 2013.

