Secure Key Exchange Scheme for IPTV Broadcasting

Ravi Singh Pippal and Shashikala Tapaswi
ABV-Indian Institute of Information Technology and Management, Gwalior, India
E-mail: {ravi, stapaswi}@iiitm.ac.in

Jaidhar C. D.
Defence Institute of Advance Technology, Girinagar, Pune, India
E-mail: jaidharcd@diat.ac.in

Keywords: cryptography, IPTV, mutual authentication, nonce, smart card, STB

Received: October 7, 2011

In Internet Protocol Television (IPTV) broadcasting, service providers charge subscription fee by scrambling the program in Conditional Access System (CAS). This avoids unauthorized users to receive the programs. A smart card (CA card) is used to decrypt the Control Words (CWs) and transfer them back to Set-Top Box (STB) in order to descramble the scrambled program. This paper presents a secure mutual authentication and key exchange scheme between STB and smart card for IPTV broadcasting. Its security is based on one way hash function and the discrete logarithm problem. It allows subscribers to choose and change the password freely, provides dynamic session key agreement and mutual authentication between STB and smart card. Security analysis proves that the scheme is strong against subscriber and STB impersonation attacks, replay attack, stolen verifier attack, smart card loss attack, man-in-the-middle attack and attack on perfect forward secrecy which are considered as common threats in IPTV environment. Moreover, the scheme also prevents serious attacks such as smart card cloning and McCormac Hack attack particular to authentication using smart cards.

Povzetek: Članek opisuje način šifriranja vsebine za televizijo IP.

1 Introduction

There are several security issues that must be considered before transmitting confidential data over a public network. In order to prevent unauthorized access, first step of the communication is legitimacy verification. In other words, authentication is vital requirement which identifies the legitimate user in order to prevent unauthorized access. Verities of authentication schemes have been proposed in the literature [1, 2, 3, 4, 5, 6, 9]. Most widely used one is password based authentication scheme.

Using one way hash function, Peyravian and Zunic [1] proposed a secure method for protecting passwords while being transmitted over insecure channel. Further, secure password change phase has also been proposed. In addition, they claimed that their schemes do not require any symmetric key or public key cryptosystem. However, Tseng *et al.* [2] found that Peyravian-Zunic's scheme is insecure against dictionary attack and fails to provide mutual authentication. To overcome these flaws, they proposed improved schemes based on Diffie-Hellman key exchange scheme and claimed that their improved schemes not only provide secure password transmission and password change, but also generate a session key between user and the server. Yang *et al.* [3] pointed out that Tseng *et al.*'s protected password changing scheme is susceptible to modification attack. Further, they suggested an improved scheme without using symmetric or asymmetric cryptosystem to overcome the weakness of Tseng *et al.*'s scheme. They claimed that their scheme is secure against replay attack, guessing attack, server spoofing and modification attack. Nevertheless, Yoon *et al.* [4] and Ku and Tsai [5] found that Yang *et al.*'s scheme is still vulnerable to Denial-of-Service attack and stolen verifier attack. To overcome these security pitfalls, they proposed their modified schemes.

In all the schemes discussed so far, server maintains a database or verification table for the registered users to authenticate the legitimate users. However, there is a threat in such a process as an intruder can penetrate the server and steal or modify the contents of the verification table. To resist these possible attacks on the verification tables, smart card based password authentication scheme has been proposed. In this scheme, server authenticates the legitimate user without maintaining a verification table.

In this context, Hwang and Li [6] proposed a remote user authentication scheme based on ElGamal's cryptosystem. They claimed that their scheme does not maintain any password or verification table and it is secure against replay attack. However, Chan and Cheng [7] proved that Hwang-Li's scheme is vulnerable to impersonation attack. Chang and Hwang [8] found that Chan-Cheng's attack does not work well and they suggested different ways to cryptanalyze Hwang-Li's scheme. Based on symmetric key cryptography and one way hash function, Song [9] suggested an efficient smart card authentication scheme and claimed that the scheme is secure against impersonation attack, parallel session attack, replay attack and modification attack. Moreover, it provides mutual authentication and shared session key. Though, Pippal *et al.* [10] pointed out that Song's scheme is inadequate to resist Denial-of-Service attack and fails to provide perfect forward secrecy.

The remainder of this paper is organized as follows: Section 2 briefly describes the work related to secure communication in IPTV broadcasting. The proposed key exchange scheme is presented in Section 3. Section 4 discusses security analysis of the proposed scheme and finally, section 5 concludes the paper.

2 Secure Communication in IPTV Broadcasting

Internet Protocol Television (IPTV) is a next generation television capable of transmitting, receiving and displaying a video stream. Gist of IPTV structure is shown in Figure 1. It provides access to on-demand gaming, home security, data services and digital music. IPTV is capable of providing a single stream to multiple users simultaneously and also to a single user such as Video on-Demand.

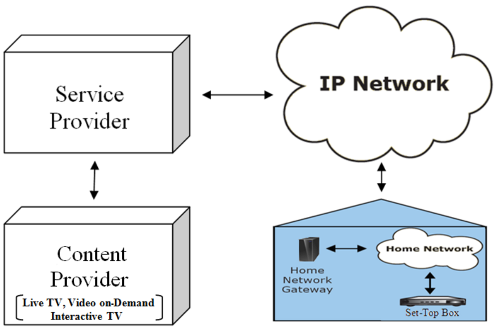

Figure 1: Overview of IPTV Structure

In IPTV broadcasting, service providers charge subscription fee by scrambling the program in CAS. A smart card is used to decrypt CWs and transfer them back to STB in order to descramble the scrambled program. STB receives encoded digital signals and decodes these signals to convert them back to analog signals so that the analog television can understand. Therefore, secure key exchange with mutual authentication between STB and smart card is needed to improve the security of the system. Without this, single smart card can be used in different STBs of the same type which results smart card cloning and McCormac Hack attacks [11].

Figure 2 shows a typical CAS, it operates as follows [12]. The server chooses a random variable CW which is used to initialize the Pseudo Random Generator (PRG) to generate a pseudo random sequence for scrambling the Transport Stream (TS). Simultaneously, for each subscriber, CW is encrypted by Authorization Key (AK) to form Entitlement Control Message (ECM). A Master Private Key (MPK) is used to encrypt AK and other entitlement message together in order to form Entitlement Management Message (EMM). These ECM, EMM and the scrambled TS stream are multiplexed into a new TS stream and broadcasted to subscribers over an insecure channel. Subscriber Management System (SMS) is used to deliver the smartcard, which contains MPK and other account information, to authorized subscriber.

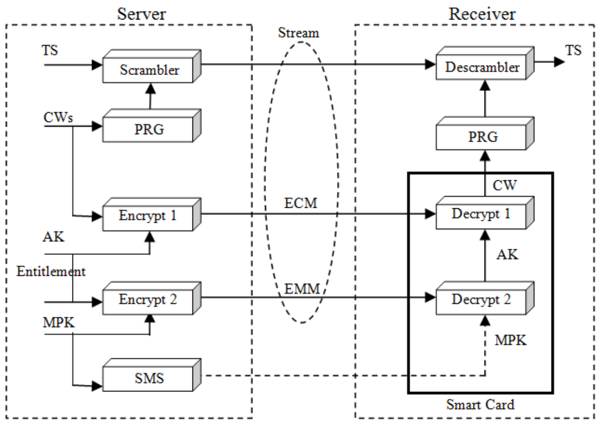

Figure 2: Conditional Access System

The receiver can descramble the program by following the same steps performed by the server in reverse order with the collaboration of smart card and STB [13]. In STB, an ECM/EMM filter is used to filter out the ECM and EMM sections and a descrambler is used to descramble the program. After receiving radio frequency (RF) signal, tuner and demodulator process the signal to bring back the TS stream. The ECM/EMM filters filter out the ECM and EMM sections and sent to the smart card to be decrypted for CW with Decrypt 1 and Decrypt 2. CW is encrypted by using Session Key (SK) and it is sent back to STB. This CW is used by descrambler to descramble the TS stream which is then de-multiplexed and decoded. The STB takes copyright protection before outputting program to subscriber.

To provide secure communication between STB and smart card, various elegant key exchange schemes have been proposed [14, 15, 16, 17]. Based on one way hash function and Schnorr's digital signature protocol, Jiang *et al.* [14] first proposed a key exchange scheme for DTV broadcasting. They claimed that their scheme allows users to freely choose the password, provides mutual authentication and session key agreement between STB and smart card. Moreover, it has lower computation cost. However, Yoon and Yoo [15] found that Jiang *et al.*'s scheme is susceptible to impersonation attack and fails to provide perfect forward secrecy. They also suggested a new key exchange scheme to overcome these security weaknesses and claimed that their scheme is free from replay attack, impersonation attack and provides perfect forward secrecy.

Based on symmetric and asymmetric key cryptosystems, Hou *et al.* [16] proposed a secure authentication scheme for DTV broadcasting and claimed that their scheme allows users to freely choose the password, provides security against replay attack, impersonation attack, offers mutual authentication and session key generation. However, Kim [17] found that the message transmitted during mutual authentication phase of Hou *et al.*'s scheme can be forged by the attacker. To overcome this security flaw, an improved scheme has also been suggested.

Secure IP multicast can be used to implement IPTV services, but still, it has problems that need to be addressed. These issues were addressed and a centralized form of secure group communication was proposed to transmit group cryptographic material [18]. However, Pinto and Ricardo [19] found that there are other issues also, like access control and network management, which were left. They proposed a secure and efficient IPTV solution which enforces individual access control to groups of real-time IPTV video channels, IP multicast admission control for both multicast senders and receivers, supports user generated videos and generates low signalling overheads. Moreover, it does not introduce perceivable delays, particularly in video channel zapping circumstances.

3 The Proposed Key Exchange Scheme

This section describes the proposed key exchange scheme for IPTV. The notations used throughout this paper are summarized as follows.

U_i	:	subscriber
ID_i	:	identity of U_i
PW_i	:	password chosen by U_i
SMS	:	Subscriber Management System
STB	:	Set-Top Box
ID_s	:	identity of STB
PW_i^*	:	password guessed by an attacker
x	:	secret key of STB
d	:	secret number of STB
p	:	large prime number
g	:	primitive element
$h(\cdot)$	:	secure one way hash function
$E_k(\cdot)$	:	symmetric encryption with key $'k'$
$D_k(\cdot)$	:	symmetric decryption with key $'k'$
$\oplus$	:	bitwise XOR operation
N_1	:	random nonce generated by U_i
N_2	:	random nonce generated by STB
S_{Key}	:	common shared session key
$\dashrightarrow$	:	secure channel
$\longrightarrow$	:	insecure channel

The proposed scheme consists of five phases: Registration phase, Login phase, Mutual Authentication phase, Key Agreement phase and CW Transmission phase. The detailed description of the proposed scheme is shown in Figure 3. This scheme works as follows.

3.1 Registration Phase

This phase is invoked when a new subscriber U_i wants to subscribe the subscribed program. In this phase, U_i selects ID_i and PW_i, computes $h(PW_i)$ and submits $\{ID_i, h(PW_i)\}$ to SMS. Upon receiving the registration request from U_i, SMS computes

$$x_i = g^{h(PW_i)} \times d \ mod\ p$$
$$y_i = h(ID_i, x)$$
$$z_i = y_i \oplus h(PW_i)$$

and issues a smart card over secure channel to U_i by storing $\{x_i, y_i, z_i, ID_s, p, g, h(\cdot), E_k(\cdot), MPK\}$ along with other account information into smart card memory.

3.2 Login Phase

This phase is invoked when U_i wants to receive the subscribed program. U_i inserts the smart card to STB and keys in ID_i and PW_i. The smart card generates a random nonce N_1, computes

$$a_i = g^{y_i} \ mod\ p$$
$$b_i = a_i^{y_i \times N_1} \ mod\ p$$
$$c_i = a_i^{h(PW_i) \times N_1} \ mod\ p$$
$$d_i = (h(PW_i) + y_i \times \lambda) \ mod\ (p-1)$$
$$e_i = g^{h(PW_i)} \ mod\ p$$
$$f_i = b_i \oplus c_i$$

where $\lambda = h(ID_i, ID_s, x_i, a_i, b_i, c_i, N_1)$. U_i sends the login request $\{ID_i, d_i, e_i, f_i, N_1\}$ to STB.

3.3 Mutual Authentication Phase

Upon receiving the login request $\{ID_i, d_i, e_i, f_i, N_1\}$; STB first checks the validity of ID_i to accept/reject the login request. If true, STB computes

$$x_i = e_i \times d \ mod\ p$$
$$y_i = h(ID_i, x)$$
$$a_i = g^{y_i} \ mod\ p$$
$$b_i = a_i^{y_i \times N_1} \ mod\ p$$
$$c_i = b_i \oplus f_i$$

and checks whether

$$g^{d_i} = e_i \times a_i^{\lambda} \ mod\ p \tag{1}$$

is true or not.

$$\begin{aligned} g^{d_i} &= \left(g^{(h(PW_i)+y_i \times \lambda)}\right) mod\ p \\ &= \left(g^{h(PW_i)} \times g^{(y_i \times \lambda)}\right) mod\ p \\ &= \left(g^{h(PW_i)} \ mod\ p\right) \times \left((g^{y_i})^{\lambda} \ mod\ p\right) \\ &= e_i \times a_i^{\lambda} \ mod\ p \end{aligned}$$

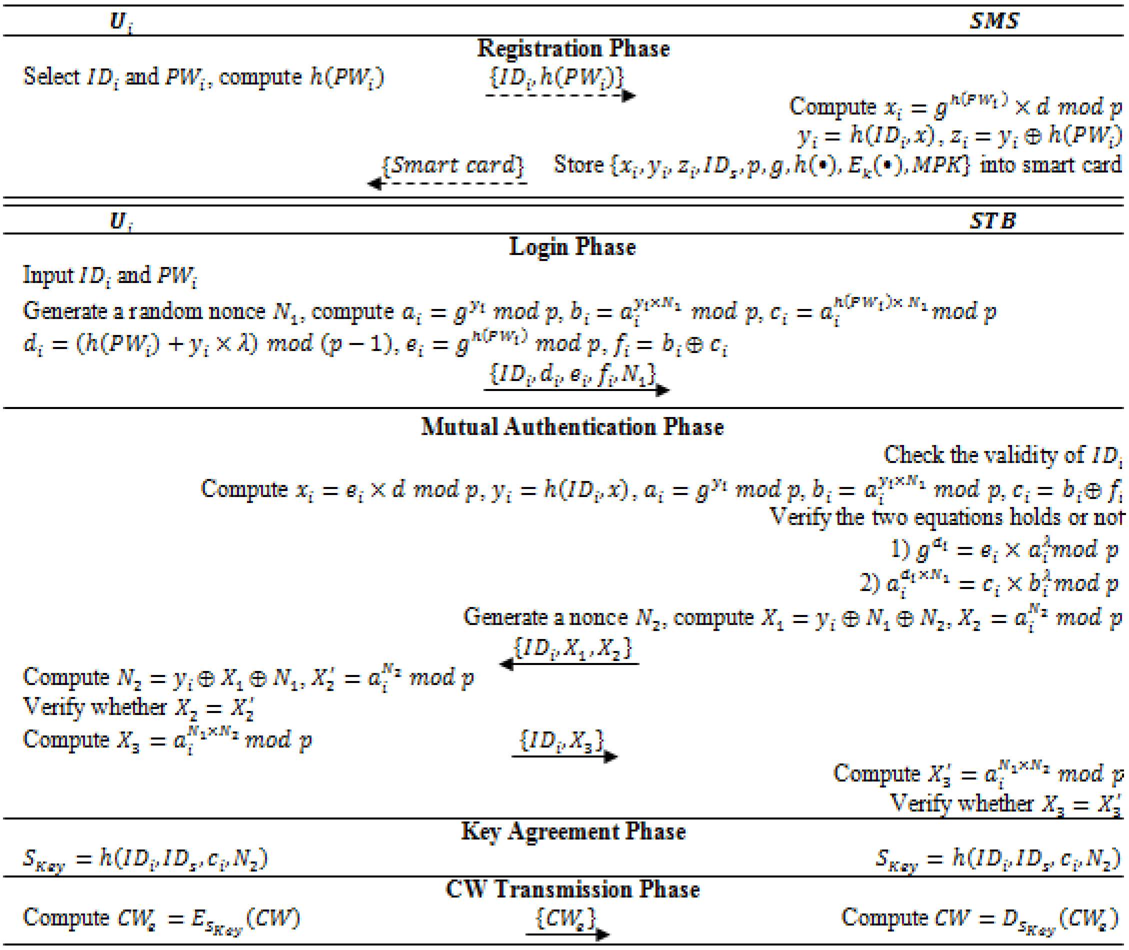

Figure 3: Proposed Key Exchange Scheme

If eq. 1 holds, STB checks whether

$$a_i^{d_i \times N_1} = c_i \times b_i^{\lambda} \ mod \ p \tag{2}$$

is true or not.

$$\begin{aligned} a_i^{d_i \times N_1} &= \left(a_i^{(h(PW_i)+y_i \times \lambda) \times N_1}\right) \ mod \ p \\ &= \left(a_i^{(h(PW_i) \times N_1)} \times a_i^{(y_i \times \lambda \times N_1)}\right) \ mod \ p \\ &= \left(a_i^{(h(PW_i) \times N_1)} \ mod \ p\right) \times \left((a_i^{y_i \times N_1})^{\lambda} \ mod \ p\right) \\ &= c_i \times b_i^{\lambda} \ mod \ p \end{aligned}$$

If both the equations, (eq. 1 and eq. 2), hold, STB generates a nonce N_2, computes $X_1 = y_i \oplus N_1 \oplus N_2$, $X_2 = a_i^{N_2} \ mod \ p$ and sends the message $\{ID_i, X_1, X_2\}$ to U_i's smart card. After getting the message $\{ID_i, X_1, X_2\}$ from STB, smart card computes $N_2 = y_i \oplus X_1 \oplus N_1$, $X_2' = a_i^{N_2} \ mod \ p$ and checks whether X_2 and X_2' are equal or not. If it holds, STB is authentic otherwise terminate the session. Subsequently, smart card computes $X_3 = a_i^{N_1 \times N_2} \ mod \ p$ and sends $\{ID_i, X_3\}$ to STB. Once the message $\{ID_i, X_3\}$ is received, STB computes $X_3' = a_i^{N_1 \times N_2} \ mod \ p$ and checks whether X_3 and X_3' are equal or not. If it holds, mutual authentication between U_i's smart card and STB is achieved.

3.4 Key Agreement Phase

If mutual authentication is achieved successfully, both U_i's smart card and STB compute common session key $S_{Key} = h(ID_i, ID_s, c_i, N_2)$. It consists of identities (ID_i and ID_s) as well as the random nonces (N_1 and N_2) chosen by U_i and STB.

3.5 CW Transmission Phase

After decrypting CW, smart card uses the session key S_{Key} to encrypt it as $CW_e = E_{S_{Key}}(CW)$ and sends CW_e back to STB to descramble the program. After receiving, STB decrypts it as $CW = D_{S_{Key}}(CW_e)$.

4 Security Analysis and Discussion

This section describes an in-depth security analysis of the proposed key exchange scheme for IPTV broadcasting. Since a smart card is a temper-resistant device, it is assumed that no one can extract any information stored in the smart card memory.

4.1 Subscriber Impersonation Attack

In the proposed scheme, the login request contains $\{ID_i, d_i, e_i, f_i, N_1\}$, where $d_i = (h(PW_i) + y_i \times \lambda)\ mod\ (p-1)$, $e_i = g^{h(PW_i)}\ mod\ p$ and $f_i = b_i \oplus c_i$. To impersonate the subscriber, attacker has to generate a forged login request by guessing the correct values of PW_i, y_i and d. Let us suppose that the attacker is successful in guessing the correct password PW_i^*. The correct values of y_i and d are still required to forge the login request. In addition, it is difficult to derive $h(PW_i)$ from e_i because of discrete logarithm problem. Moreover, if an attacker modifies any of the login request parameters, STB easily detects them as both the equations, (eq. 1 and eq. 2), are unsatisfied. Hence, this scheme provides security against subscriber impersonation attack.

4.2 STB Impersonation Attack

To impersonate STB, the attacker has to generate valid response message $\{ID_i, X_1, X_2\}$ corresponding to the login request $\{ID_i, d_i, e_i, f_i, N_1\}$. However, without the knowledge of y_i and N_2, no one can compute the correct value of X_1 and X_2. Moreover, attacker is unable to get N_2 from the eavesdropped response message as the value of y_i is unknown. Therefore, the scheme is secure against STB impersonation attack.

4.3 Replay Attack

An attacker may try to act as an authentic subscriber by resending previously intercepted messages. This scheme uses random nonces, N_1 and N_2, which are different from session to session. As a result, attackers cannot enter the system by resending the previously transmitted messages to impersonate legal subscribers. Suppose that the intercepted login request $\{ID_i, d_i, e_i, f_i, N_1\}$ is replayed to pass the authentication phase. Attacker is unable to retrieve N_2 correctly from the response message $\{ID_i, X_1, X_2\}$ to compute the correct message $\{ID_i, X_3\}$ for mutual authentication. Consequently, STB rejects the request by comparing X_3 with X_3'.

4.4 Stolen Verifier Attack

In order to verify the legitimacy of subscribers, use of verification table at STB is not efficient. Moreover, if STB stores U_i's secret information, it will be always under the risk. In the proposed scheme, STB keeps long term secret key $'x'$ and secret number $'d'$ to avoid maintaining verification table used to verify subscriber login request. Hence, the scheme avoids stolen verifier attack.

4.5 Man-in-the-Middle Attack

If an attacker intercepts the communicating messages exchanged between the subscriber and STB, it does not generate any useful information as they are dissimilar from session to session due to property of randomness of N_1 and N_2. Moreover, to alter N_1, one needs to recalculate b_i, c_i, d_i and f_i. Similarly, y_i is needed to alter N_2. Hence, the scheme is able to resist man-in-the-middle attack.

4.6 Smart Card Cloning and McCormac Hack Attack

In the proposed scheme, if an attacker uses the cloned smart card to another STB, it will not pass the mutual authentication phase as there is no STB's ID_s in the cloned smart card memory.

If an attacker redirects one smart card's communication message to another STB, the STB cannot decrypt the message as it has no information about the session key S_{Key}.

4.7 Smart Card Loss Attack

If accidently, subscriber's smart card is lost or stolen; the scheme must be strong enough so that no one can impersonate the smart card owner. In this scheme, attacker is unable to receive the program without knowing the correct ID_i and PW_i of the subscriber even if he or she got subscriber's smart card.

4.8 Attack on Perfect Forward Secrecy

In the proposed scheme, the session key is computed as $S_{Key} = h(ID_i, ID_s, c_i, N_2)$. The attacker is unable to find out the present session key or any of the previously used session keys from the eavesdropped messages as the values of ID_s, c_i and N_2 are unknown to the attacker and it is infeasible to guess all these values simultaneously.

4.9 Subscriber can change the Smart Card Password Securely

This phase is invoked whenever U_i wants to change the current password PW_i with a new password PW_{inew}. U_i inserts the smart card to STB and keys in ID_i and PW_i'. The smart card computes $z_i' = y_i \oplus h(PW_i')$ and checks whether computed z_i' equals stored z_i or not. If true, U_i is prompted to enter a new password PW_{inew}. The smart card computes $z_{inew} = y_i \oplus h(PW_{inew})$, $x_{inew} = (x_i / g^{h(PW_i)}) \times g^{h(PW_{inew})}\ mod\ p$ and stores x_{inew}, z_{inew} instead of x_i, z_i respectively, in the smart card memory. Thus, U_i can change the smart card password.

It can be clearly seen that the given scheme keeps all the previous advantages and achieves the necessary security requirements.

5 Conclusion

In IPTV services, content is crucial that needs strong protection from unauthorized entities. In order to provide secure communication, dynamic session key generation and mutual authentication between smart card and STB is imperative. Considering all the common threats in IPTV environment, this paper proposes secure key exchange scheme for IPTV broadcasting. Security analysis section shows that the proposed scheme is robust against impersonation attacks, replay attack, stolen verifier attack, smart card loss attack and man-in-the-middle attack.

In addition, it is secure against two serious attacks in IPTV broadcasting such as smart card cloning and McCormac Hack attack. Proposed scheme allows the subscribers to choose and change their smart card password freely. It ensures perfect forward secrecy as well as dynamic session key generation with mutual authentication.

Acknowledgement

The authors would like to thank ABV-Indian Institute of Information Technology and Management, Gwalior, India for providing academic support.

References

[1] Peyravian, M. and Zunic, N. (2000). Methods for protecting password transmission. *Computers and Security*, 19(5), pp. 466–469.

[2] Tseng, Y.M., Jan, J.K. and Chien, H.Y. (2001). On the security of methods for protecting password transmission. *Informatica*, 12(3), pp. 469–476.

[3] Yang, C.C., Chang, T.Y. and Hwang, M.S. (2003). Security of improvement on methods for protecting password transmission. *Informatica*, 14(4), pp. 551–558.

[4] Yoon, E.J., Ryu, E.K. and Yoo, K.Y. (2005). Attacks and solutions of Yang *et al.*'s protected password changing scheme. *Informatica*, 16(2), pp. 285–294.

[5] Ku, W.C. and Tsai, H.C. (2005). Weaknesses and improvements of Yang-Chang-Hwang's password authentication scheme. *Informatica*, 16(2), pp. 203–212.

[6] Hwang, M.S. and Li, L.H. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1), pp. 28–30.

[7] Chan, C.K. and Cheng, L.M. (2000). Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(4), pp. 992–993.

[8] Chang, C.C. and Hwang, K.F. (2003). Some forgery attacks on a remote user authentication scheme using smart cards. *Informatica*, 14(3), pp. 289–294.

[9] Song, R. (2010). Advanced smart card based password authentication protocol. *Computer Standards and Interfaces*, 32(5-6), pp. 321–325.

[10] Pippal, R.S., Jaidhar, C.D. and Tapaswi, S. (2010). Comments on symmetric key encryption based smart card authentication scheme. *In Proceedings of* 2^{nd} *International Conference on Computer Technology and Development*, Cairo, Egypt, pp. 482–484.

[11] Kanjanarin, W. and Amornraksa, T. (2001). Scrambling and key distribution scheme for digital television. *In Proceedings of IEEE International Conference on Networks*, Bangkok, Thailand, pp. 140–145.

[12] Jiang, T., Zheng, S. and Liu, B. (2004). Key distribution based on hierarchical access control for conditional access system in DTV broadcast. *IEEE Transactions on Consumer Electronics*, 50(1), pp. 225–230.

[13] Kamperman, F. and Rijnsoever, B.V. (2001). Conditional access system interoperability through software downloading. *IEEE Transactions on Consumer Electronics*, 47(1), pp. 47–53.

[14] Jiang, T., Hou, Y. and Zheng, S. (2004). Secure communication between set-top box and smart card in DTV broadcasting. *IEEE Transactions on Consumer Electronics*, 50(3), pp. 882–886.

[15] Yoon, E.J. and Yoo, K.Y. (2009). Robust key exchange protocol between set-top box and smart card in DTV broadcasting. *Informatica*, 20(1), pp. 139–150.

[16] Hou, T.W., Lai, J.T. and Yeh, C.L. (2007). Based on cryptosystem secure communication between set-top box and smart card in DTV broadcasting. *In Proceedings of TENCON 2007*, IEEE Region 10 Conference, Taipei, Taiwan, pp. 1–5.

[17] Kim, H. (2008). Secure communication in digital TV broadcasting. *International Journal of Computer Science and Network Security*, 8(9), pp. 1–5.

[18] Pinto, A. and Ricardo, M. (2010). Secure multicast in IPTV services. *Computer Networks*, 54(10), pp. 1531–1542.

[19] Pinto, A. and Ricardo, M. (2011). On performance of group key distribution techniques when applied to IPTV services. *Computer Communications*, 34(14), pp. 1708–1721.