Secure Communication in Digital TV Broadcasting

Hyo Kim

Division of Digital Media, Ajou University, Korea

Summary
To provide subscription-based Digital TV (DTV) data, services providers scramble the data stream (program content) with some secure measures such as ECM and EMM via using control words, and send the stream to conditional access system (CAS) in the set-top box (STB). Smart card is used to decrypt the control words and accordingly to enable the STB to descramble the scrambled signal. Therefore, secure communication between STB and smart card is a key issue to the service providers. The paper discusses and identifies some security issues in previous research works that have focused on secure communication between smart card and STB. Then, it proposes a secure mutual authentication and a key agreement protocol between smart card and STB. The proposed scheme is more efficient and secure than previously proposed schemes in that it eliminates time-consuming exponentiation operation. The proposed scheme also prevents smart card cloning and McCormac Hack problems.

Key words:
Security, Digital TV broadcasting, Set-top Box, Smart Card, Mutual Authentication, Key Agreement

1. Introduction

The rapid growth of modern network technologies has made digital video/audio broadcasting available throughout the world. Unlike the internet, most digital television broadcasting is unidirectional, which means that there is no authentication between the head-end and the subscriber on-line. Further, digital video streams are usually transmitted through insecure public channel. Therefore, service providers want to prevent unauthorized viewing of their video streams and utilize mutual authentication between STB and smart card to protect their benefit.

To control such an unauthorized use of video stream, and encourage users to pay for their program contents, service providers employ the conditional access systems (CAS). The CAS usually works inside the STB and can be accessed with the smart card. Users can be charged or allowed to access proper contents based on their subscription information.

Properly scrambled and encrypted data information is fed into CAS to prevent unauthorized accesses. An authorized subscriber can descramble the program with a smart card, which cooperatively works with the STB. CAS also can be used to charge the subscription fee by managing the decrypting device or keys [2,3,7].

When smart card and CAS communicate with each other in order to authenticate users, two security problems arise: smart card cloning and McCormac Hack. The former refers to an incidence that an illegal copy of a smart card is created with the proper ID numbers. This illegal copy can be used with the same kind of STB in the same way that the authentic card is used. That is, the copied card may allow unauthorized usage of program contents. McCormac Hack problem refers to an incidence that data transferred between smart card and STB are hacked and re-directed to another (other) STB. In this case, the STB with the redirected information works as if it were the original one [6].

Smart cards are secure and compact data carriers equipped with memory to store programs and multiple cryptographic keys to restrict data access and ensure that data are not modified, deleted, or appended. In addition, smart cards can be used to prove the digital identity of its cardholder by using cryptographic keys and algorithms stored in the card-protected memory. By the popular use of smart cards, International Standards Organizations (ISO) had set up international standards for smart card applications [8-10].

In 2004, Jiang et al. [4] presented a secure authentication scheme between STB and the smart card. Later, Hou et al. [1] proposed a modified authentication scheme which was allegedly more efficient. However, Hou et al.'s scheme was found to have some security flaws. In the paper, the security issues of Hou et al.'s scheme will be discussed and an improved scheme, which provides a better measure of security and efficiency, will be proposed. For this purpose, we will discuss the conventional CAS model and importance of mutual authentication between smart card and the STB in section 2. In section 3, we will review Hou et al.'s scheme and discuss its security issues. An improved mutual authentication and key agreement scheme will be presented in section 4. The security analysis is also given in section 4. Concluding remarks will be given in section 5.

Manuscript received September 5, 2008.
Manuscript revised September 20, 2008.

2. Conditional Access System (CAS)

This section introduces the CAS model and discusses some related works on mutual authentication and key agreement protocols between STB and smart card. For DTV broadcasting, CAS is an essential system to facilitate the subscription system. The overall structure of CAS is shown in figure 1 [5]. At the head-end, control word (CW) is used to initialize the generation of a pseudo random sequence number. This number is generated by a pseudo random sequence generator (PRG) in order to scramble and descramble video/audio and data signals. CW for each subscriber is encrypted with an authorization key (AK) for the corresponding channel. This encrypted CW forms entitlement control message (ECM). AK is also encrypted using master private key (MPK). And the encrypted AK forms entitlement management message (EMM). These ECM, EMM and the scrambled signals are re-multiplexed in a new transport stream (TS). And eventually the TS is broadcasted in the form of radio frequency signal. The subscriber management system (SMS) is used to administer or update the issue of the smart card for a subscriber, which contains MPK and other account information. At the receiver end, the STB receives the radio frequency signal and attempts to decrypt the encrypted information. The smart card is used for this decryption. Once the authentication process succeeds, STB descrambles the program according to the reverse steps of the head-end. More detailed description of this process is shown in Figure 2.

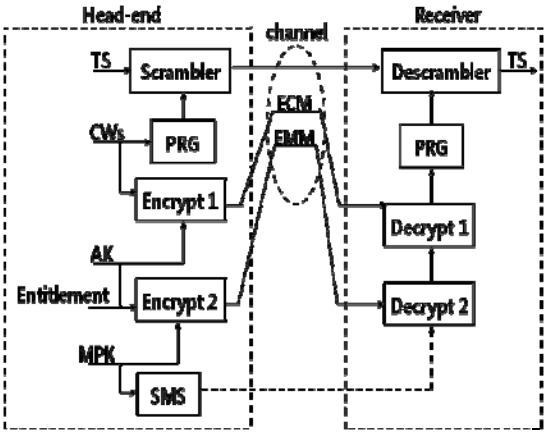

Figure 1. Control Access System (CAS)

As shown in Figure 2, when STB receives radio frequency signal from the channel, tuner and demodulator will process the signal to restore the TS stream. That is, ECM/EMM filters filter out the ECM and EMM sections. These two sections are sent to the smart card to be decrypted for CW with Decrypt2 and Decrypt1 as figure 1 shown. At this moment, mutual authentication and key agreement between STB and the smart card are needed. CW is encrypted with a session key (SK) in smart card and transferred back to STB. Then, descrambler can use CW to descramble the TS stream, and TS will be de-multiplexed and decoded. During this processes, if CW is not encrypted before it is transferred back to STB, the adversary may redirect the CW to a same type of descrambler to descramble the program directly by eavesdropping the communication of the smart card interface. That is if CW is not properly encrypted, a security issue may arise.

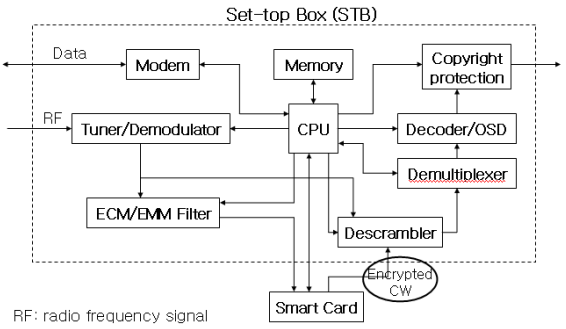

Figure 2. Cooperation of STB and smart card

What this indicates is that, without properly encrypted mutual authentication between STB and the smart card, an adversary can duplicate smart card or redirect the communication message between STB and a legitimated smart card to other STBs. This may entitle the unauthorized user to use the program content without a charge. Therefore, dynamic session key agreement and mutual authentication between STB and smart card are necessary for the system security.

3. Security Issues of Hou et al.'s Scheme

In 2004, Jiang et al.[4] proposed a key exchange with mutual authentication protocol between STB and smart card based on Schnorr's digital signature protocol and one-way hash function. In 2007, Hou et al. proposed a more efficient scheme for the communication between smart card and STB. However, their scheme was found to have a security issue. This section reviews Hou et al.'s scheme and discuss about its security problem.

Some notations are used in this section:

- ID_C : identity (ID number) of the smart card
- ID_S : identity (ID number) of STB.

- (x_S , y_S): key pair of STB, (secret key, public key).
- $h(\cdot)$: one-way collision-resistant hash function whose output length is 128 bits.
- $DESenc_K(\cdot) / DESdec_K(\cdot)$: DES encryption/ decryption algorithms with key K
- $RSAenc_x(\cdot) / RSAdec_y(\cdot)$: RSA encryption using private key x / RSA decryption using public key y.
- $E_K(\cdot) / D_K(\cdot)$: Symmetric key encryption / decryption algorithm using key K.
- $\oplus$: bitwise exclusive-or operation

3.1 Review of Hou et al.'s Scheme

The scheme consists of five phases: (1) registration, (2) login, (3) mutual authentication, (4) key agreement, and (5) CW transmission. The STB has its secret key x_S and public key y_S.

Registration phase. When a new user (U) applies to subscribe the charge program with his/her smart card identity ID_C and password PW, U sends ID_C and PW to SMS. SMS computes C_1, CC_1 and PW' as follows.

$$C_1 = h(ID_C \oplus x_S)$$
$$CC_1 = DES_{PW}(C_1)$$
$$PW' = h(PW \oplus ID_C) \oplus h(ID_C \oplus x_S)$$

SMS stores $\{PW', ID_S, CC_1, E(\cdot), h(\cdot), MPK\}$ with other account information in the smart card and issues it to the user.

Login phase. If U wants to receive the program, he attaches his smart card to his STB and inputs ID_C and PW. The smart card will perform the following operations:

1. Compute C_1 by DES decryption algorithm and C_1' as follows.
$$C_1 = DES_{PW}(CC_1)$$
$$C_1' = PW' \oplus h(PW \oplus ID_C)$$
Check the equality of C_1 and C_1'. If the equality holds, the user login request is accepted. Otherwise, the smart card rejects the user login request.
2. If the user login request is accepted, the smart card generates a random number r with 512 bits length, computes C_2 and CID_C as follows, and sends (CID_C, C_2, r, T) to STB. Here, T is the timestamp which denotes the current day and time the smart card.
$$PW_{1i} = PW' \oplus h(PW \oplus ID_C)$$
$$C_2 = h(T \oplus PW_{1i})$$
$$CID_C = RSA_{yS}(ID_C)$$

Mutual authentication phase. Upon receiving the login request, STB and the smart card need do the following steps to realize mutual authentication.

1. Upon receiving (CID_C, C_2, r, T), if $(T'-T) < \Delta T$, STB accepts the smart card's request, where T' is the current time stamp of STB and ΔT denotes the expected valid time interval for transmission delay. If $(T'-T) \geq \Delta T$, STB rejects the login request. If the smart card is accepted, SMS computes C_2' and checks the equality of C_2 and C_2' as follows:
$$ID_C = RSA_{xS}(CID_C)$$
$$C_2' = h(T \oplus h(ID_C \oplus x_S))$$
2. If C_2 is equals to C_2', then STB chooses a random number e and computes C_3. STB then sends (C_3,T_1,e) to the smart card. Here, $C_3 = h(C_2' \oplus ID_S \oplus T_1 \oplus e)$. Here, T_1 is the current time stamp.
3. The smart card computes C_3' and checks the equality of C_3 and C_3', where $C_3' = h(C_2 \oplus ID_S \oplus T_1 \oplus e)$.
4. If the equality holds, the smart card accepts STB.

Key agreement phase. If the mutual authentication is done successfully, then both parties use the following equation to obtain a common session key $SK = H(r, e, ID_C, ID_S)$.

CW transmission phase. After decrypting out CW, the smart card uses the session key SK to encrypt it as $CW' = E_{SK}(CW)$ and sends CW' back to STB for descrambling the program. STB can decrypt the CW by $CW = D_{SK}(CW')$.

3.2 Security issues

Hou et al. claimed that their scheme has the following merits: security, dynamic session key, and mutual authentication. However, the transcript (C_3,T_1,e) sent from STB to the smart card in mutual authentication phase can be forged by the adversary. That is, if the adversary randomly chooses T_1', then he can compute e'. This is possible, since $e' = (T_1 \oplus e) \oplus T_1'$. Therefore, the adversary can compute (C_3, T_1', e') .

4. Improved Scheme

4.1 Proposed Scheme

In the proposed scheme, unlike Hou et al.'s scheme, STB has only secret key x_S . Let $H(\cdot)$ be one-way collision-resistant hash function whose output length is 128 bits. Further, since RSA algorithm is not used in

the proposed scheme, there are no exponentiation operations. We show six phases as follows.

Registration phase. When a new user (*U*) applies to subscribe the charge program with his/her smart card identity ID_C and password *PW*, *U* computes $IP = H(ID_C, PW)$ and sends ID_C and *IP* to SMS. Note that, instead of *PW*, *IP* is sent to SMS. SMS computes *C* such that $C = IP \oplus H(ID_C, x_S)$ and stores $IP, C, ID_S, h(\cdot), H(\cdot)$, and *MPK* with other account information in the smart card and issues it to the user.

Login phase. If *U* wants to receive the subscriber programs, he attaches his/her smart card to his/her STB and inputs ID_C and *PW*. The smart card will perform the following operations:

1. Check the equality of *IP* and $H(ID_C, PW)$. If the equality does not hold, the smart card rejects the user login request.
2. If the user login request is accepted, the smart card generates a random number *r* with 512 bits length, computes C_2 and CID_C as follows, and sends (CID_C, C_2, *r*, *T*) to STB. Here, *T* is the current time stamp of the smart card.

$$C_2 = h(T \oplus C \oplus IP)$$

$$CID_C = ID_C \oplus h(ID_S)$$

Mutual authentication phase. Upon receiving the login request, STB and the smart card need do the following steps to realize mutual authentication.

1. Upon receiving (CID_C, C_2, *r*, *T*), STB checks if $(T'-T) < \Delta T$. Here, T' is the current time stamp of STB and ΔT is the reasonable delay between smart card and STB. If $(T'-T) \geq \Delta T$, STB stops the communication. Otherwise, STB obtains ID_C, computes C_2', and then checks that received C_2 equals to C_2'.

$$ID_C = CID_C \oplus h(ID_S)$$

$$C_2' = h(T \oplus H(ID_C, x_S))$$

2. If C_2 equals to C_2', then STB chooses a random number *e* and computes *e*', C_3 as follows. Here, T_1 is the current time stamp of the STB.

$$e' = h(ID_S) \oplus e \oplus T_1$$

$$C_3 = h(C_2' \oplus ID_S \oplus T_1 \oplus e')$$

3. STB sends (C_3, T_1, *e*) to the smart card.
4. The smart card computes C_3' and checks the equality of C_3 and C_3'.

$$e' = h(ID_S) \oplus e \oplus T_1$$

$$C_3 = h(C_2' \oplus ID_S \oplus T_1 \oplus e')$$

5. If the equality of C_3 and C_3' does not hold, the smart card rejects the communication. Otherwise, the smart card accepts STB.

Key agreement phase. If the mutual authentication is done successfully, then both parties use the following equation to obtain a common session key $SK = H(r, e, ID_C, ID_S)$.

CW transmission phase. After decrypting out *CW*, the smart card uses the session key SK to encrypt it as $CW' = E_{SK}(CW)$ and sends CW' back to STB for descrambling the program. STB can decrypt the *CW* by $CW = D_{SK}(CW')$.

Password change phase. The user can freely change his smart card's password from *PW* to PW'. To change the password, the user inputs ID_C and *PW* to the smart card. The smart card then checks the equality of $IP = H(ID_C, PW)$. If the equality holds, the user enters new password PW' to the smart card. The smart card computes $IP' = H(ID_C, PW')$ and $R' = IP' \oplus R \oplus IP$. It then replaces *R* with *R*' and *IP* with IP'.

4.2 Analysis of the proposed scheme

The proposed scheme has several advantages as follows:

(1) Resistance against replay attack : In the proposed scheme, session key (*SK*) is generated as the output of a one-way hash function whose input is the concatenation of r, e, ID_C, ID_S. The four values r, e, ID_C and ID_S are only known to the smart card and the STB. Since the random number *r* is seed information for each session key, replay attack and impersonation attack are not possible. Moreover, since the session key is different at each communication, it is difficult to attack the encryption algorithm to get *CW* with known plaintext attack.

(2) Security against smart card cloning problem : The proposed scheme is also resistant to smart card cloning problem. When an adversary uses his cloned smart card to another STB, there is no corresponding STB's ID (ID_S) in the cloned smart card and the hash function in STB is different from the hash function of the cloned smart card. Therefore, it is impossible to use such cloned smart card into another STB.

(3) Security against McCormac Hack attack : When an adversary redirects one smart card's communication message to another STB, the STB has no information of session key without

mutual authentication and key exchange. Therefore, the STB cannot decrypt the message redirected from the smart card.

(4) Computational efficiency : Since the limited computation capability of the smart card, the computational work for the smart card should be considered carefully. It is reasonable to get rid of time-consuming operations such as exponentiation computations. Since this scheme only uses exclusive "or" operations, it is more efficient than Jiang et al.'s and Hou et al.'s scheme. Further, while the password is directly sent to SMS in Jiang et al. and Hou et al.'s schemes, the hash value of identity number of the smart card and the password are sent to SMS in the proposed scheme. This provides a better system security.

5. Conclusions

We discussed possible security issues in Hou et al.'s scheme, and proposed a more efficient and secure communication between smart card and STB in digital TV broadcasting. The proposed scheme satisfies security, mutual authentication, dynamic session key agreement, low computation and free password change for the user. The proposed scheme also prevents two serious problems in DTV broadcasting: smart card cloning and McCormac Hack problem.

References

[1] T.-W. Hou, J.-T. Lai and C.-L. Yeh, "Based on Cryptosystem Secure Communication between Set-top Box and Smart card in DTV Broadcasting," TENCON 2007, IEEE Region 10 Conference, 2007, pp.1-5.

[2] 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 Trans. On MULTIMEDIA, Vol. 6, No. 5, October 2004, pp.760-769.

[3] T. Jiang et al, "Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcast," IEEE Trans. On Consumer Electronics, Vol. 50, Feb. 2004, pp.225-230.

[4] T. Jiang et al., "Secure Communication between Set-top Box and Smart Card in DTV Broadcasting," IEEE Trans. On Consumer Electronics, Vol. 50, No. 3, August, 2004, pp.882-886.

[5] F. Kamperman and B.V. Rijnsoever, "Conditional access system interoperability through software downloading", IEEE Trans. On Consumer Electronics, Vol. 47, No.1, 2001, pp.47-53.

[6] W. Kanjanarin and T. Amomraksa, "Scrambling and Key Distribution Scheme for Digital Television," IEEE International Conference on Networks, Oct. 2001, pp.140-145.

[7] R. Tu, "On Key Distribution Management for Conditional Access System on Pay-TV System," IEEE Trans. On Consumer Electronics, Vol. 45, Feb. 1999, pp.151-158.

[8] ISO/IEC DIS 7816-2, "Information Technology – Identification cards - Integrated circuit(s) cards with contact – part 2: Dimensions and location of the contacts (Revision of ISO 7816-2:1988)"

[9] ISO/IEC DIS 7816-3:1989, "Identification cards – Identification cards - Integrated circuit(s) cards with contact – part 3: Electronic signals and transmission protocol"

[10] ISO/IEC DIS 7816-4:1995, "Information Technology – Identification cards - Integrated circuit(s) cards with contact – part 4: Interindustry commands for interchange"

Hyo Kimreceived the M.S. degree in Communication from the University of Utah in 1998 and the Ph.D degree in Communication from the Rutgers University in 2003. He is a faculty member at Ajou University in Korea. His research interests include digital television broadcasting and the internet application research.