An Efficient Satellite CAS Using Password-Based Protocol

YOUNGSOO KIM, JUNGCHAN NA, SEUNGWON SOHN
Network Security Department, Information Security Technology Division, ETRI
161 Kajong-Dong, Yusong-Gu, Taejon 305-600
KOREA

Abstract: - We shall introduce a new satellite Conditional Access System (CAS) in which a subscriber could use a pay-TV knowing only his or her identity and password, and not carrying a smart card. For this new system, two password-based protocols are presented which not only share a session key and authenticate each other but also get an authorization key. Since this system does not need an expensive Card Adaptive Device (CAD), it can reduce costs. Furthermore, this system provides for descrambler independence allowing it to be used through any TV set-top box that includes a descrambler.

Key-Words: - Conditional access system, Password-based protocol, Password guessing attack

1 Introduction

With the all-ready rapid development of technology in the fields of computers and communication, broadcasting technology has now been further developed. In accordance with the ever increasing demands of users and the diversity of broadcasting media, the number of broadcasting channels is increasing along with some specialized broadcasting channels coming into being. In order to broadcast these higher-quality and well-produced programs, subscriber subscription fee system will most likely dominate the specialized broadcasting station. So, to preserve the continued financial stability of the pay-TV system, the Conditional Access System (CAS) has been adopted so that only authorized subscribers are able to watch programs.

Most of the present CAS use a smart card that is separate from the TV set-top box and includes a decryption algorithm and a secret key [6]. But, it has some shortcomings. First, a subscriber has to buy and attach a comparatively expensive Card Adapter Device (CAD) to a TV set-top box in order to have use of the smart card. Additionally, the decryption algorithm and the secret key in the smart card must be periodically updated. Finally, since a descrambler in a TV set-top box is dependent on a smart card, a subscriber cannot watch programs without his or her own descrambler. Therefore, under the present CAS environment, the exchange of ownership of a descrambler would be very difficult and troublesome. Moreover, the owner would have to make available his or her own identity if the selling of the descrambler to another person is desired [7] – a very dangerous idea in the information society.

In this paper, we propose a new satellite CAS that allows it to be used by the subscriber knowing only the identity and password, and not carrying a smart card. For this new system, two password-based protocols, which would not only share a session key and authenticate each other, but also allow the download of an authorization key, are presented. As for the rest of the paper, in section 2, we review the current satellite CAS using smart cards. And, in section 3 we briefly examine the notion of password-based protocols and present a new satellite CAS using them. Finally, we conclude our findings in section 4.

2 The current satellite CAS

The present satellite CAS consists of a sender, a satellite network and a receiver. A sender is made up of a broadcasting station and a subscriber management system (SMS). To describe our protocols clearly, we summarize notations. A control word and an authorization key used for encrypting it are denoted as CW and AK. The shared secret *pwd* corresponds to the password of sender. PRNG(CW) means a pseudo-random number generated by a seed CW. SCR(x) stands for a value of scrambling x and $SCR^{-1}(y)$ for a value of descrambling y. $E_{AK}(CW)$ means a ciphertext of message CW under encryption

key AK and $D_{AK}(F)$ is a plaintext of ciphertext F under decryption key AK. AV denotes audio and video signal. K and h stand for a session key and a one-way hash function, respectively.

A broadcasting station makes AV and generates a pseudo-random number *I* using CW provided by the SMS. An encrypted CW under AK and a scrambled AV using *I* are sent to a subscriber's TV set-top box through a satellite network. In order to get the CW used for descrambling, a subscriber must have encryption key AK. This key generated by the SMS is encrypted using a subscriber's password stored in a smart card and sent to a subscriber on his first subscription or updating period. When a subscriber's TV set-top box gets F and J from a satellite network, it delivers them to its own descrambler. A smart card inserted in its descrambler yields a CW using the password and AK. Finally, a smart card delivers the CW to its descrambler, and that same descrambler retrieves AV using a pseudo-random number *I*. In these operations, a smart card and a descrambler authenticate each other using the Fiat-Shamir's zero-knowledge authentication [3].

3 A new satellite CAS

For user authentication in a distributed environment, a password scheme is still the most preferable, despite the potential for guessed attacks on passwords of low entropy. Since DH-EKE [1] was introduced for the purpose, several schemes have followed [2,4,5,7,9,10].

We propose a new satellite CAS that not only shares a session key and authenticates between a subscriber and the SMS but also downloads the AK by using a secure password-based protocol. Compared with current systems, it reduces the amount of computations by eliminating the AK-encryption module and simplifying the CW-decryption process. This system consists of a sender, a satellite network and a receiver. A sender is made up of a broadcasting station and SMS. Fig.1 shows operation modules for a new satellite CAS.

This system would not require a TV set-top box to include an expensive CAD, so it can reduce the cost. Furthermore, since it provides the independence, a subscriber could watch programs through any TV set-top box with a descrambler. Operation process is as follows:

- If someone requests to subscribe, the SMS issues an identity and password. Meanwhile, SMS generates a CW and AK and sends them to the broadcasting station.
- The broadcasting station generates a pseudo-random number *I* using the CW. Also, it makes AV and generates J, the value of scrambling AV with *I*:

$$I = \mathrm{PRNG}(CW),\ J=SCR_I(AV) \quad \text{.....(1)}$$

- The broadcasting station encrypts CW with AK and yields F:

$$F=E_{AK}(CW) \quad \text{.....(2)}$$

- The broadcasting station broadcasts J and F through a satellite network (F is contained in Entitlement Control Message (ECM)), and a subscriber's TV set-top box receives them.
- When subscribers want to watch programs, they input their own identity and password into the TV set-top box by a remote controller.
- By using a password-based protocol, a TV set-top box shares session key K with the SMS and downloads the AK using it. (AK being updated periodically)
- The subscriber's TV set-top box decrypts F, which is obtained from the satellite network, with AK and formulates CW:

$$CW=D_{AK}(F) \quad \text{.....(3)}$$

- The subscriber descrambler generates a pseudo-random number *I* using the CW and receives an original AV by descrambling J with *I*:

$$I=\mathrm{PRNG}(CW),\ AV = SCR^{-1}_I(J) \quad \text{.....(4)}$$

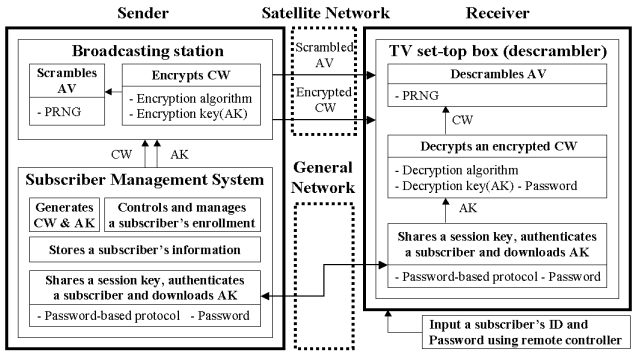

Fig. 1 A new proposed satellite CAS

In next two sections, two password-based protocols are presented. The first protocol is a 6-message protocol, which uses random numbers (ex. R_{BS}, *salt*) which are generated by a broadcasting station to progress security. The second protocol is a 2-message protocol, which reduces the running time and computational complexity for more practicality.

3.1 The first proposed password based protocol

The first protocol is a 6-message protocol that is based on SPEKE [4]. It uses two random numbers, *salt* and R_{BS}. This protocol prevents a denial-of-service attack using R_{BS}, which is generated by a broadcasting station and interchanged with the receiver. It was also designed to include *salt* to W, a hash value of the *pwd*, in order to protect a dictionary attack. This protocol needs some additional computations and messages to generate and send random numbers.

-*Operation processes*: If someone requests to subscribe, the SMS of the broadcasting station issues an identity and password and stores them. If a subscriber wants to watch programs, the identity and *pwd* are inputted into a subscriber's TV set-top box by remote controller. The subscriber's TV set-top box sends the identity to the broadcasting station. The SMS verifies the identity, generates (*salt*, R_{BS}) and sends them to the subscriber. The subscriber's TV set-top box computes W=h(*pwd*, *salt*), selects a random number A(1 A p-2, p is a large prime) and sends W^A mod p to a broadcasting station with R_{BS}. Then, the broadcasting station selects a random number B(1 B p-2) and sends W^B mod p to a subscriber. The subscriber's TV set-top box computes a session key $K=W^{AB}$ mod p and sends h(K), a hash value of K to the broadcasting station. Finally, the broadcasting station computes $Y=E_W(AK)$ and sends the encrypted value with K to the receiver. Fig.2 shows above described operations.

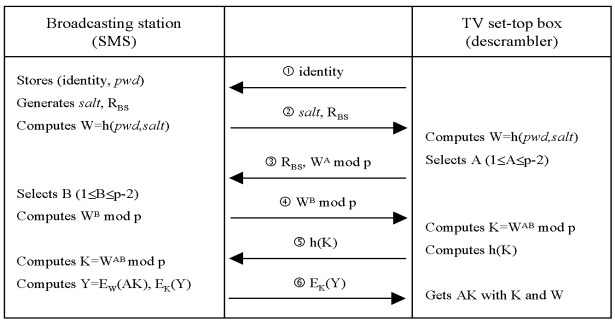

Fig.2 First password-based protocol applicable to a new satellite CAS

-*Security*: This protocol uses random numbers, *salt* and R_{BS}, to prevent dictionary attacks or denial-of-service attacks. If we do not use *salt* and compute simply W=h(pwd), anyone who steals the broadcasting station's database can conduct a dictionary attack. Therefore, we have included *salt* to W in order to prevent this kind of attack. On the other hand, R_{BS} is a random number the broadcasting station sends and the subscriber returns providing proof that the subscriber is actually receiving at the location where he or she is claiming to be. This is helpful against an attacker who sends numerous requests with forged serial number of a specific descrambler to avoid capture. Besides, this protocol replaces the fourth message of the EKE[1] or SPEKE[4] in which the client authenticates the server with the message of downloading AK encrypted with session key K. Since this protocol does not have a process authenticating the broadcasting station, it is possible that someone who has stolen a subscriber's password into tricking him or her into using the wrong AK. But, given that the password is the only means of authenticating the broadcasting station, this kind of attack is unavoidable. So there is no security disadvantage to eliminating the message a subscriber authenticates the broadcasting station.

3.1 The second proposed password based protocol

The second protocol is a 2-message protocol that reduces running time and computational complexity for practicality. In this case, the broadcasting station stores the subscriber's identity, W^B mod p and B. In this scheme, the broadcasting station does not store W to prevent a single password guessing attack (i.e. an attacker obtains a subscriber's password from the broadcasting station's database directly). Moreover, the broadcasting station always would use the same B for a particular subscriber, so reducing some of the computations.

-*Operation processes*: If someone requests to subscribe, the SMS issues an identity and *pwd* to the subscriber and stores the identity, W^B mod p and B(W=h(*pwd*), B being the subscriber-specific random number selected by the broadcasting station). When the subscriber inputs his or her identity and *pwd* by remote controller, the receiver's TV set-top box selects a random number A(1 A p-2, p being a large prime) and sends W^A mod p to the broadcasting station with the identity. Then, the SMS authenticates the identity and computes the session key $K=W^{AB}$ mod p using the received data W^A mod p and B(1 B p-2) stored at the beginning. The broadcasting station computes $Y=E_W(AK)$ and sends this encrypted value with K to the subscriber's TV set-top box with W^B mod p which would be stored at first

registration. Finally, the subscriber's TV set-top box computes K and gets AK using K and W. Fig.3 illustrates the above listed operations.

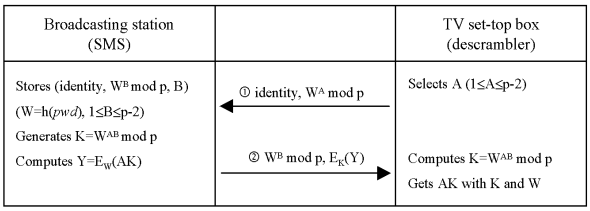

Fig.3 Second password-based protocol applicable to a new satellite CAS

-*Security*: This protocol is an optimized version of the first proposed protocol, which eliminated *salt*, R_{BS}, and the mutual authentication process between subscriber and SMS. Therefore, it is possible for this protocol to have some security problems that deem consideration. At first, there could be an attacker who impersonating a broadcasting station by getting . However without knowing A, he or she cannot obtain the session key K, *pwd* nor AK, even with knowledge of . Next, an attacker who impersonates the subscriber gets a single chance to verify the password guess in an unaudited way. If the wrong password is guessed, he or she will have no information about K, and therefore no information about Y. However, one gets one piece of information on the incorrect guess- that the guess he chose was indeed incorrect. The broadcasting station cannot tell if someone requesting the AK download is legitimate or not. But, it is important that this be only a single on-line password guess. Although a broadcasting station cannot distinguish a legitimate download from a password guess, it should become suspicious if the same subscriber request thousands of password downloads within a short time. Finally, there could exist a situation in which an attacker who wants to compromise files in a broadcasting station. But, even though this attacker gets W^B mod p in this way, he or she cannot obtain the password or hash value of the password directly.

4 Conclusion

We have proposed a new satellite CAS that would allow a subscriber usage knowing only identity and password, and not carrying a smart card. At first, we reviewed current satellite CAS using smart cards, and then examined some of its shortcomings. We also delved into the history of some password-based protocols, our central thesis, and have shown structures and modules for a new system. Finally, we have presented two password-based protocols applicable to the new system. Since this system does not need expensive CAD's, its implementation could reduce cost. Furthermore, this system would provide for the descrambler independence allowing for its use through any TV set-top box having a descrambler. So, with the realization of our proposed satellite CAS model, improvement and increased productivity can only but be the result.

References:

[1] S.M.Bellovin, M.Merritt, Encrypted Key Exchange: Password-based protocols secure against dictionary attacks, *Proc. of the IEEE Computer Society Conference on Research in Security and Privacy*, 1992

[2] S.M.Bellovin, M.Merritt, Augmented Encrypted Key Exchange: a Password-Based Protocol secure against dictionary attacks and password file compromise, *TR*, AT&T Bell Lab, 1994

[3] M.Fiat, A.Shamir, How to prove yourself : practical solution to identification and signature problems, *Proc. of Crypto'86*, Springer-verlag, LNCS Vol.263, 1986, pp.186-199

[4] D.P.Jablon, Strong Password-only authenticated key exchange, *ACM Computer Communications Review*, 1996

[5] D.P.Jablon, Extended password methods immune to dictionary attack, *In WETICE '97 Enterprise Security Workshop*, 1997

[6] K.S.Kim, A study on the cryptographic protocols for the Conditional Access System using smart card, *Ph.D. thesis*, Dept. of Information Engineering, Sungkyunkwan University, Korea, 1996

[7] K.S.Kim, S.J.Kim, D.H.Won, Conditional access system using smart card, *Proceeding of JCCI'96, The 6th Joint Conference on Communication & Information*, 1996, pp.180-183

[8] T.Kwon, J.Song, Efficient Key Exchange and Authentication Protocols Protecting Weak Secrets, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E81-A, No.1, 1998, pp.156-163

[9] T.Kwon, J.Song, Secure Agreement Scheme for g^xy via Password Authentication, *Electronics Letters*, Vol.35, No.11, 1999, pp.892-893

[10] T.Wu, The Secure Remote Password Protocol, *1998 Internet Society Symposium on Network and Distributed System Security*, 1998