VOL. 12, NO. 2, JANUARY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

AN EFFICIENT REVOCATION SCHEME FOR STATELESS RECEIVER WITH LESS ENCRYPTION AND LESS KEY STORAGE

Abdullah Rashed[1] and Samir Hammami[2]
[1]Independent Researcher
[2]Dhofar University, Sultanate of Oman
E-Mail: abdullah.rashed@gmail.com

ABSTRACT

In the revocation scheme for stateless receivers, the center delivers information securely to the authorized users over a public channel, where the receivers do not update their state from session to session. This paper presents a view of multimedia Conditional Access Systems (CAS) one-way broadcasting and suggests a new approach. The proposed approach is an efficient revocation scheme for stateless receivers. It reduces the number of private keys used in traditional CAS and number of encryptions as it does not need to encrypt the ciphering keys. Furthermore, the presented approach eliminates the proposed key refreshment presented in (Zhang, Yang, Liu, Tian, 2009) and (Koo, Kwon, & Kim, 2005). The researchers applied the proposed system using AES algorithm. A numerical example is used to demonstrate the effectiveness of the presented approach.

Keywords: cryptography, broadcast encryption, conditional access systems, revocation.

INTRODUCTION

Copyright protection and access control is significant for broadcasting. Broadcasters use an encryption system so that the supplier would optimize bandwidth use by avoiding duplicating every channel on the network (Dardari, Martini, Mazzotti, and Chiani, 2004), Massoudi *et al*. (2008). Due to the communication explosion digital multimedia transmission security is very important Massoudi *et al*. (2008). PDAs, mobile phones, networks, public channels (cable, satellite, wireless networks, Internet, etc.) depend on this service (Dardari, Martini, Mazzotti, & Chiani, 2004). The limited batteries life of these devices obliges to reduce encryption computational complexity. Furthermore, channels need to use on access control systems to protect their content and the copyright. Standard cryptographic techniques guarantee high level of security but at the cost of expensive implementation and important transmission delays (Ajlouni, El-Sheikh, and Rashed, 2006). The alternative solution that aims to provide sufficient security with an important gain in computational complexity and delays Massoudi *et al*. (2008). Broadcasting encryption (BE) aims to transmit data to all authorized users simultaneously, in an efficiently way and securely (Zhang, Yang, Liu, Li, 2007).

Technically speaking, in the revocation scheme for stateless receivers, the center delivers information securely to the authorized users over a public channel, where the receivers do not update their state from session to session (Hwang, Kim, & Lee, 2004).

Figure-1 shows three level of encryption of CAS: the raw content is encrypted at the sender side by control word (CW) which is encrypted by service key (SK). SK is embedded into Entitlement Control Message (ECM) and it is encrypted using personal distribution key (PDK) of authorized user, which is embedded into entitlement management message (EMM). Scrambled content, ECM, EMM are broadcasted to public. SK is renewed at intervals of hours or days, while PDK is static and known only by the service provider and the user's secure module, being embedded into firmware. At the receiver side SK is decrypted and used to decrypt ECM, which allows to get CW, necessary to descramble the content (Zhang, Yang, Liu, Tian, 2009). For pay TV, many authors preferred building a separate key tree for each multicasting program (Abdalla, Shavitt, Wool, 2000).

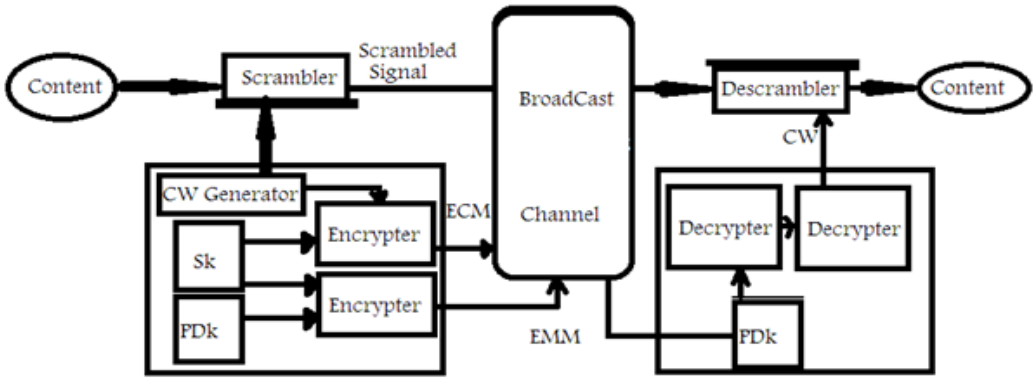

Figure-1. Typical conditional access system, adapted from (Zhang, Yang, Liu, Tian, 2009).

(Abdalla, Shavitt, Wool, 2000) studied how to communicate securely with a set of users over an insecure broadcast channel for application domains: satellite/cable pay TV and the Internet MBone. Their solution depends on maintaining single key structure such that receiver should keep a logarithm number of establishment keys and it is entire life time.

(Naor, Naor, and Lotspeich, 2001) studied the problem of a center sending a message to a group of the stateless receivers, such that some subset of the users is considered revoked and should not be able to obtain the content of the message. They provided sufficient conditions to guarantee the security of revocation schemes.

To propose efficient revocation methods for stateless receivers; Asano (2002) used the Master Key technique with an a-ary key tree structure in order to reduce the number of keys each receiver stores and the number of ciphertexts broadcast, respectively. The first method required receivers to store only one key. Second method was supposed to reduce the computational overhead of receivers in exchange for an increase in the number of master keys they store. He discussed the security of his methods and some techniques used in his methods.

(Hwang, Kim, & Lee, 2004) used a logical hierarchical key tree to present an efficient revocation scheme for stateless receivers. They used hierarchical key binary tree, the found that it had the same message length as the SD scheme.

(Koo, Kwon, & Kim, 2005) suggested key refreshment management scheme for CAS in DTV broadcasting. They found that their scheme performed dynamic entitlement management securely and efficiently and reduced a key generation and encryption load for CAS.

A selection encryption of image and video scheme was introduced by Massoudi *et al*. (2008) to reduce the amount of encrypted data and achieving the security goals. Their approach divides the process into public and protected parts. There is no encryption in public part, and all users can access that data. In contrast, encryption process is necessary in protected part and only authorized users can access data.

A novel solution is introduced by (Zhang, Yang, Liu, Li, 2007) to solve the tradeoff problem about communication, storage and computation overhead of BE scheme. Getting rid of the computation overhead that come from broadcast key generation is suggested. Their scheme based on Subset Difference (SD) and RSA accumulator. User side device is separated into private and public parts. The public device's functionality would minimize the storage and computation overhead of the private device, and make BE scheme more implementation-oriented.

Shirazi *et al* (2008) proposed a system that includes the message handling subsystem with what so-called 'Follow-Me' service, which proposed to extend mobility and personalization concepts on Pay-TV services. Subscriber management and subscriber authentication subsystems would respond to subscribers' interaction (via mobile phone) issuing them the corresponding rights. Their system is supposed to reduce the cost for service provider and end-users by respectively cutting down the service deployment cost and eliminating the requirement of additional receiver as changing the service provider.

Based on the well-known used trees based broadcast encryption schemes; Eagle *et al*. (2008) studied the number of encryptions necessary to revoke group of user. Their study focused on proving a normal limiting distribution for the number of encryptions, as the number of users became large. They took into consideration the combined number of encryptions and number of privileged users in a random privileged set.

Kirkels, Maas, & Roelse, 2008) introduced security architecture for a Pay-TV conditional access system. They focused on the design constraints related to a conditional access client in the design of the architecture and maximum amount of bandwidth available for the transmission of conditional access messages. They presented the design and analysis of their efficient injector model based on queuing theory, conditional access messages into the broadcast stream. They presented a numerical example with real-world values in order to demonstrate the effectiveness of the presented approach.

(Zhang, Yang, Liu, Tian, 2009) presented a CAS model for encryption scheme for one-way broadcasting and protection application. They compared it with traditional conditional access systems. They discussed the advantages and challenges of BE.

PROPOSED SYSTEM

The proposed system aims to protect the copyright and avoid changing both the system or the keys. Moreover, users do not need to change their state as every block is encrypted using different schedule key to increase the level of security.

The process would be as following: Users should register at the site and would be granted the personal distribution key (PDK). Then the raw content would be compressed. Private Ciphering Key (CK) is generated and expanded. Expanded CK is used to encrypt the compressed raw data. Finally, both CK and encrypted data (C). The private cipher key would be scrambled with ciphered block in special way the only legitimated receiver can extract them. Then receiver would be able to do the inverse cipher phase and get the plain text.

SCRAMBLING ALGORITHM: STARTING RANDOM

To determine the start with ciphered data block or ciphering key; the system would randomly generate a random number that can be either zero or one. If it's one that means system would start the scrambling selecting the ciphered block otherwise start would be the cipher key.

Algorithm scrambling
Input: ciphered data block, ciphering key
Output: Scrambled Token (ST).
Function Scrambling

Begin
Generate start, using lookup table
for i=0 to block Cipher size-1 step by 1
ST $_{2i+1+\text{start}}$ += ciphered data block $_i$
ST $_{2i+\text{start}}$ += ciphering key $_i$
end for
ST= the rest of the ciphering key
end function Scrambling

A pre-defined location is determined for ST. It is dedicated starting byte, so this location start =0 that means that second location (index=1) should be filled with byte from ciphered data block whereas the third location (index=2) would be filled with first byte of the ciphering key. Otherwise (start =1) the second location should be filled with first byte from ciphering key and the next from ciphered data block and so on.

ILLUSTRATIVE EXAMPLE USING AES ALGORITHM

Assuming that the predefined location is first byte in string therefore, if start =0, it means that first location would be filled from ciphered data block.

Assuming that Nb=4, Nk=4, Nr =10 and random start=0
Ciphering key = 4173696d204120456c2d536865696b68
Ciphered data block: a6d9f3603953ff11136e03067f8a57fa
Output Block:
0a641d973f369606d39205341ff201145136c6e2d
035306687f658a69576bfa68

Figure-2: Ciphered data block and ciphering key mixed together with first byte to determine from where the first byte should be.

0	1	2	3	4	5
0	C_0	Ck_0	C_1	Ck_1	C_2

6	7	8	9	10	11
Ck_2	C_3	Ck_3	C_4	Ck_4	C_5

12	13	14	15	16	17
Ck_5	C_6	Ck_6	C_7	Ck_7	C_8

18	19	20	21	22	23
Ck_8	C_9	Ck_9	C_{10}	Ck_{10}	C_{11}

24	25	26	27	28	29
Ck_{11}	C_{12}	Ck_{12}	C_{13}	Ck_{13}	C_{14}

30	31	32
Ck_{14}	C_{15}	Ck_{15}

Figure-2. Ciphered block & ciphering key.

CONCLUSIONS

We introduce a new efficient approach for multimedia Conditional Access Systems (CAS) as revocation scheme for stateless receivers where the center can deliver information securely to the authorized users over a public channel, where the receivers do not update their state from session to session. The proposed approach uses dynamic key generation. Our approach is efficient with respect of the number of keys stored and transmitted and used to encrypt the data and the encryptions number. It is efficient and reduces the complexity of the old ones as it does not need to encrypt the ciphering keys. It uses fewer keys to reduce the storage and scramble the transmitted data to reduce encrypting the keys. Furthermore, the presented approach eliminates the proposed key refreshment presented in (Zhang, Yang, Liu, Tian, 2009) and (Koo, Kwon, & Kim, 2005). The researchers applied the proposed system using AES algorithm suggested by (Ajlouni, Rashed, 2004) and key expansion suggested by (Rashed & Sana, 2007). A numerical example is used to demonstrate the effectiveness of the presented approach.

REFERENCES

Abdalla M., Shavitt Y. and Wool A. 2000. Key management for restricted multicast using broadcast encryption. IEEE/ACM Transactions on Networking. *8*(4): 443-454.

Ajlouni N. M., El-Sheikh A. and Rashed A. A. 2006. A New Approach in Key Generation and Expansion in Rijndael Algorithm. Int. Arab J. Inf. Technol. *3*(1): 35-41.

Ajlouni N., Rashed A. 2004. An Extended Rijndael Block Cipher Using Java. International Conference on software Engineering Research and practice, Las Vegas. 21-24.

Asano T. 2002, December. A revocation scheme with minimal storage at receivers. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 433-450. Springer Berlin Heidelberg.

Dardari D., Martini M. G., Mazzotti M. and Chiani M. 2004. Layered video transmission on adaptive OFDM wireless systems. EURASIP Journal on Applied Signal Processing. 2004, 1557-1567.

Eagle C., Gao Z., Omar M., Panario D. and Richmond B. 2008. Distribution of the number of encryptions in revocation schemes for stateless receivers. In: Fifth Colloquium on Mathematics and Computer Science. pp. 195-206. Discrete Mathematics and Theoretical Computer Science.

Hwang Y. H., Kim C. H. and Lee P. J. 2004. June. An efficient revocation scheme for stateless receivers. In: European Public Key Infrastructure Workshop. pp. 322-334. Springer Berlin Heidelberg.

Kirkels B., Maas M. and Roelse P. 2007, October. A security architecture for pay-per-view business models in conditional access systems. In Proceedings of the 2007 ACM workshop on Digital Rights Management. pp. 1-9. ACM.

Koo H. S., Kwon O. H. and Kim J. M. 2005. Key Refreshment Management for Conditional Access System in DTV Broadcasting. In: Int. Conf. Consumer Electronics 2005 (pp. 29-30).

Massoudi A., Lefebvre F., De Vleeschouwer C., Macq B. and Quisquater J. J. 2008. Overview on selective encryption of image and video: challenges and perspectives. EURASIP Journal on Information Security. 1: 1.

Naor D., Naor M., and Lotspeich J. 2001. Revoking and Tracing Scheme of Stateless Receiver, Proceedings of Crypto01. LNCS 2139. pp. 29-30.

Rashed A. A. and Sana Y. 2007. Using Modified Genetic Algorithm to Replace AES Key Expansion Algorithms. In: The International Conference on Information Technology (ICIT'2007) at Al-Zaytoonah University, Jordan on May. pp. 9-11.

Shirazi H., Cosmas J., Cutts D., Birch N. and Daly P. 2008, September. Security architectures in mobile integrated pay-TV conditional access system. In: 13th IEEE International Telecommunications Network Strategy and Planning Symposium, Networks. pp. 1-15.

Zhang, Y. C., Yang, C., Liu, J. B. and Tian J. Y. 2009, May. Broadcast encryption scheme and its implementation on conditional access system. In: Proceedings of the 2009 International Symposium on Web Information Systems and Applications WISA'09.

Zhang Y., Yang C., Liu J. and Li J. 2007, August. A Novel Broadcast Encryption Scheme Based on SD Scheme Reconstruction. In: Communications and Networking in China, 2007. CHINACOM'07. Second International Conference on. pp. 387-391. IEEE.