Source Authentication Protocol for IP-TV*

Kieun Shin[1] and Hyoung-Kee Choi[2]
[1] School of Information and Communication Engineering, Sungkyunkwan University
Suwon, South Korea
[2] School of Information and Communication Engineering, Sungkyunkwan University
Suwon, South Korea
E-mail: [1]keshin@hit.skku.edu, [2]hkchoi@ece.skku.ac.kr

Abstract: Presently, the demand for IP-TV, to satisfy a variety of goals, is exploding. IP-TV utilizes Conditional Access System (CAS), which controls the subscriber access to content. Although the current CAS scheme provides access control via subscriber authentication, there is no authentication scheme for the content provided by service providers. Thus, there is a vulnerability of security, through which an adversary can forge content between the service provider and subscribers. In this paper, based on a hash tree shceme, we proposed an efficient and strong source authentication protocol which removes the vulnerability of the current CAS.

1. Introduction

Presently, the demand for IP-TV, to satisfy a variety of goals, is exploding. IP-TV provides various services such as broadcasting, voice, and data services via a high-bandwidth IP infrastructure. IP-TV provides bidirectional service that improves the conventional one-way service broadcasting and transfers high quality video / audio. A subscriber utilizes channels and contents that he wishes to enjoy. To meet these requirements, IP-TV delivers diverse and subdivided contents via a high-bandwidth network. A service provider offers chargeable contents at a profit. He utilizes Conditional Access System (CAS) [1][2], which controls the subscriber access to content. For instance, a subscriber who pays for certain contents can only utilize that content. Although the current CAS scheme provides access control via subscriber authentication, there is no authentication scheme for the content provided by a service provider. Thus, there is a security vulnerability, whereby an adversary can forge content between the service provider and subscribers. For instance, it is possible for the adversary to forge the important stock quotes both profiting from this causing societal problems. In this paper, based on a hash tree scheme, we propose a novel source authentication protocol for a data stream provided by the service provider, which solves the problem of the vulnerability of the current CAS and provides the evidence through non-repudiation in the case of subsequent disputes.

The remaining part of this paper is organized as follows. In Section 2, we introduce the related work on source authentication protocol and requirements for IP-TV system. Section 3 presents CAS architecture and explain important signaling messages more detail for our protocol. Then in Section 4, we introduce Merkle tree (MT) [3] and our proposed protocol in detail. In Section 5, we analyze our proposed protocol from the view point of security and performance aspects. We finally conclude the paper in Section 6.

Table 1. Broadcast source authentication services

Service	Description
Data integrity	Receivers can check if transmitted data is modified.
Data source authentication	Recevers should be able to check if transmitted data comes from an authorized source.
Non-repudiation	A sender of data should not be able to deny sending the data where there is a dispute between the sender and receivers.

2. Related Work

Broadcasting is an efficient way to deliver multimedia resources such as real-time stock quotes or video to a group of receivers. Source authentication is an important topics in broadcast and prevents receivers from suffering forged resources. Generally, broadcast source authentication provides following services.

There were many studies about broadcast source authentication to date. J. M. Park et al. proposed EMS [4], to provide source authentication through signature amortization in spite of packet loss. However, verification involves buffering on the receiver side and a high computational overhead, which results in high processing latency and is unsuitable for real-time service. A. Perrig et al. introduced TESLA [5], which also provides a fast and light-weight verification scheme through hash chaining of symetric keys and later disclosure of those keys. However, TESLA doesn't provide a non-repudiation service and needs time synchronization between a sender and receivers. The length of hash chaning is limited, and hence to use TESLA with infinite streams such as video streams, the

* "This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2008-C1090-0801-0028)

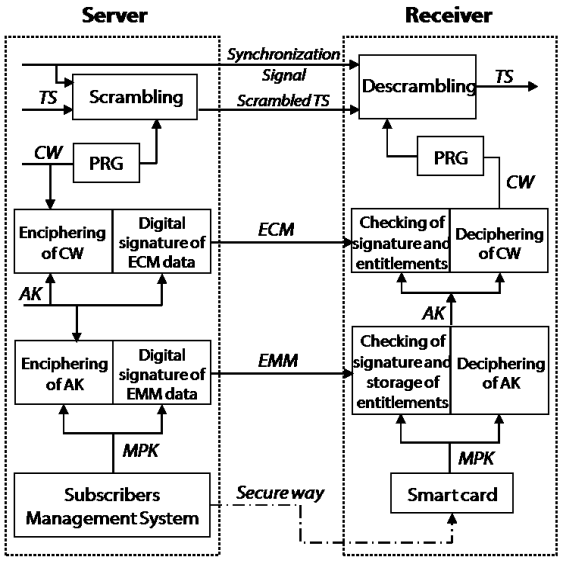

Figure 1. Structure of CAS

sender should commit the one-way key chain and broadcast it periodically.

An IP-TV service must provide real-time broadcasting and non-repudiation service that prevents the service provider from denying sending the packet to the receiver where a dispute between the service provider and receivers arises. To meet these requirements, we should design a source authentication protocol that is efficient and cannot deny sending packets. We need a new scheme suited to IP-TV, instead of the above two protocols.

3. Conditional Access System

CAS provides the way to control the access of subscribers according to the payment. It manages subscribers to protect service provider profit through granting the entitlment to watch TV and controls these entitlments. The CAS security component consists of scrambling and encryption for access control. CAS protects the data stream via scrambling. Only valid subscribers paying for the service can use specified certain content. Figure 1 shows CAS structure.

The service provider scrambles the data stream, a type of MPEG-2 Transport Stream (TS), allows only the valid subscriber to view it. An authorized subscriber can generate original TSs via descrambling. Control Word (CW), which is a random number, is employed in order to scramble and descramble TSs. CW is updated via frequent, encrypted broadcasts, using an Authorization Key (AK) to restrict illegal viewing. It is sent with an Entitlement Control Message (ECM). AK, which is encrypted with Master Private Key (MPK) is transmitted to the subscriber with an Entitlement Management Message (EMM), which consists of information such as contract information for individual receivers, by broadcasting over a relatively long period. The service provider stores MPK in an IC card within each subscriber's Set Top Box. ECM and EMM are injected into TSs streams by the service provider to offer entitlement information and to update CW and AK. The subscriber

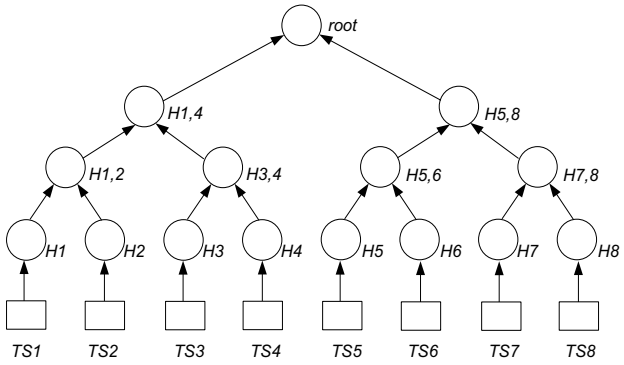

Figure 2. Structure of Merkle Tree

could descramble the content through obtaining CWs and AKs transmitted within ECM and EMM respectively.

Commonly, ECM and EMM are very important signaling messages enabling security and entitlement. Thus, the service provider signs these messages via a digital signature scheme to provide integrity and authenticity. The subscriber can check the validity of these messages through signature verification [1] and is granted use of specified content for which he pays.

4. The Proposed Protocol

Providing source authentication of the content transmitted to receivers is not simple, because of the IP-TV characteristics. Source authentication for IP-TV should be efficient both to the service provider and to the receiver to offer real-time broadcasting. The service provider and the subscriber have to be robust withstand a Denial of Service (DoS) attack and provide non-repudiation service for later disputes.

Generally, the means of authenticating a source is either a symmetric key, pre-shared between a sender and a receiver, or a digital signature via an asymmetric key. However, a sender and the remaining n group members should share n number of Pre Shared Keys (PSKs) in group communications and the sender has to construct n MACs (Message Authentication Codes). This is not applicable in the case of message broadcasting because the complexities of MAC computation and communication are $o(n)$. Thus, the predominant method of providing source authentication of broadcast messages is utilization of a digital signature scheme.

Digital signatures can provide adequate authentication services that include message integrity and non-repudiation service, but it is too expensive to generate and verify these signatures. There is high latency of verification on the receiver side that reduces the quality of service. Hence, An IP-TV service is a requested efficient source authentication protocol which enables real-time broadcasting. A very simple solution is to sign a minimum number of packets with digital signature scheme to minimize the number of verifications. IP-TV source authentication must provide packet authentications in spite of packet loss, and a non-repudiation service in the case of a dispute.

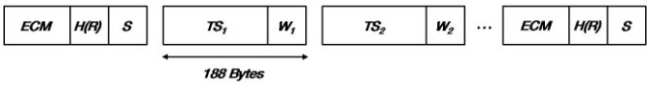

Figure 3. Stream of Proposed Protocol

Therefore, we propose source authentication for data streams transmitted by the service provider that satisfies the above requirements by MT. Figure 2 depicts the structure of MT. MT is generated via hash functions and concatenations. There is one leaf (a hash) per packet. Each internal node contains the hash value for both its right and left children, namely, concatenation. MT is constructed via this iterated process. To provide source authentication of transmitted packets via MT, the root of MT has to sign via digital signature scheme. When the packet is transmitted, the packet, the corresponding siblings and signature of root are transmitted together. For instance, TS3, $\{H_4, H_{1,2}, H_{5,8}\}$ and signature of root will be delivered together. The receiver can generate root through transmitted packet and authenticate packets by verifying of root's signature. Once the root is authenticated, the remaining packets that construct a MT can be verified through comparison of the root instead of checking the digital signature. However the communication overhead per packet of MT scheme is high due to siblings. Table 2 shows the depth of tree and the number of TSs that construct a MT according to the Bitrates when the ECM is transmitted per 0.1 second.

As mentioned earlier, ECM and EMM are signed by the service provider to authenticate their sources. The transmission period of ECM is shorter than that of EMM. So, it is suitable for the service provider to sign ECM to authenticate TSs between ECMs. The sender constructs MT with leaf nodes that are hashes of TSs. The sender signs the root with ECM to authenticate the MT root. That is, the equivalent of signing entire TSs is achieved by signing the root. The service provider concatenates the set of siblings of the nodes along the path from the TS to the root, with the corresponding TS, and transmits these generated packets. Figure 3 depicts the stream of the proposed protocol and W_i is the set of siblings that corresponds to the TS_i. TSs with the corresponding a set of siblings and ECMs are transmitted to the subscriber.

The receiver can check whether or not these TSs are valid comparing the root delivered via ECM with the root generated by the receiver. If those TSs are not valid, the receiver may discard those packets without buffering.

5. Security and Performance Analysis

Table 3 depicts the advantages of our proposed protocol. Our proposed protocol does not need an additional signing process due to signing both ECM and the root of hash together, and utilizes a very efficient hash function. Thus, the proposed protocol satisfies the demands of IP-TV, essential for a real-time service. Though some packet loss might be occur, it is possible to authenticate the remaining packets, due to the set of siblings transmitted with TSs. On the subscriber side, buffering of TSs is not required, because of the fast authentication via short hash and concatenation. Hence, our proposed protocol is resilient to a DoS attack. It is possible to verify the set of packets together via a Batch Signature scheme [6] to reduce the number of verifications.

Finally, in the proposed scheme, time synchronization is not required, essential in TESLA. Thus, it is highly scalable, because our protocol offers a source authentication service independent of the number of users.

Table 2. Depth of MT and the number of TSs

Bitrates (Mbps)	Number of TSs	Tree depth
5	349	9
10	697	10
20	1394	11

Table 3. Proposed source authentication protocol

Digital signature	No additional signing
Tolerance of packet loss	Perfect
Resilience to DoS Attack	Strong
Fast authentication latency	1 public key verification and some hash operation per a tree
Non-repudiation	Yes
Communication overhead	Medium

6. Conclusions

We proposed a source authentication protocol for a IP-TV system. To the best of our knowldege, this is a first protocol to suggest source authentication for IP-TV. Until now, most proposed IP-TV protocols are for service provider and contents provider to protect their profit. We propose a scheme to achieve subsriber rights to enjoy authorized contents via source authentication of transmmited streams and to offer legal evidence for subsequent disputes between the service provider and the subscribers. Our proposed protocol is very efficient both to the service provider and the recievers, because there is no additional signing and verification process. It also offers QoS for the contents due to packet loss tolerace and prevents the subscribers from suffering DoS attack and does not need time synchronization that is essential for TESLA protocol.

These characteristics of our protocol are strong advantages, since during the next year demand for an IP-TV service may rapidly increase.

Despite of these advantages, our protocol has a drawback. As we mentioned in Section 4, the communication overhead of our protocol is slightly higher because of the

set of siblings transmitted with packets. Thus we are studying how to reduce communication overhead through the shortening the hash output size. However the relationship between the hash output size and the security strength of hash function is trade-off. Thus we are trying to find the reasonable hash output size and the seucurity strength of hash function to meet the QoS of IP-TV system.

References

[1] T. Yoshimura, "Conditional Access System for Digital Broadcasting in Japan" *Proc. of IEEE*, pp. 318-322, Jan. 2006

[2] B. Lu et al., "A Scalable Key Distribution for conditional Access System in Digital Pay-TV system" *IEEE Trans. On consumer Electronics*, pp. 632-637 May. 2004

[3] R. Merkle, "Protocols for Public Key Cryptosystems", *Proc. IEEE Symp. Security and Privacy*, Apr. 1980

[4] J. M. Part et al., "Efficient Multicast Packet Authentication using Signature amortization" *Proc. IEEE Symp. Security and Privacy*, pp. 227-240, May. 2002

[5] A. Perrig et al., "Efficient and Secure Source Authentication for Multicast" *Net. And Distrib. Sys. Sec. Symp.*, pp.35-46, Feb. 2001

[6] Y. Zhou et al., "Multimedia Broadcast Authentication Based on Batch Signature" *IEEE Communications Magazine*, pp.72-77, Aug. 2007