Implementation of key establishment protocol using Signcryption for Secure RTP

Hyung Chan Kim[0], Jong Won Kim*, and Dong Ik Lee
Security Group, Concurrent System Research Lab. and Networked Media Lab.*
Department of Information and Communications,
Kwang-Ju Institute of Science and Technology (K-JIST)
{kimhc[0], jongwon, dilee}@kjist.ac.kr

Abstract

Real-time Transport Protocol (RTP) is widely used in VoIP stacks charging the multimedia data delivery. Concerning with payload protection of RTP packets, Secure RTP has been discussed in IETF AVT group to provide confidentiality and authentication features using block ciphering and message authentication coding. However, Secure RTP only concentrates on payload protection. Signcryption is a good candidate for key agreement. This paper proposes a key establishment protocol using Signcryption and shows example implementation of a secure VoIP application based on Secure RTP with the proposed scheme.

1. Introduction

A recent trend of Internet applications is multimedia. Especially, VoIP(Voice over IP) is one of central issues in networked multimedia. It enables real-time audio and video conferencing for one-to-one or group communications. Protocols for VoIP consist of signaling protocols and delivery protocols. Signaling protocol takes setup processes and controls of delivery. There are several signaling protocols such as H.323, SIP, SAP, RTSP and others. Delivery protocol is in charge of delivering media stream data. RTP/RTCP[1] is the most prevalent protocol for media delivery.

The demand for security in VoIP is very high because there are a lot of threats. Eavesdropping, replay attack, and denial of service are the representative dangers of multimedia data. The nature of multicast gives higher chances of eavesdropping and replay attack than before. Hence, it is essential to protect RTP packets which deliver media data. Secure RTP[2] is proposed to protect the payload of RTP packets using block ciphering and message authentication coding. However, there are no provisions of key establishment in Secure RTP. Instead, it delegates re-keying to other signaling protocols like SDP or H.235. Although there is a MD5-based method for key derivation from password[3], this is too weak to adopt.

Signcryption[4] seems to be a good candidate for the key establishment. Signcryption, which is proposed by Yuliang Zheng, is a public key cryptosystem and supports both signature and encryption simultaneously. This paper suggests a key establishment protocol using Signcryption to seed a master key for Secure RTP sessions. The cases are for the unicast and multicast. We also present an example implementation of a secure VoIP application with proposed protocol.

2. Background

2.1 Real-time Transport Protocol

Real-time Transport Protocol (RTP) specifies for the delivery of real-time data such as audio, video and simulation data. It defines RTP packet [Figure1] to support identification of payload type, sequence numbering, time-stamping and identification of source. It is an application level protocol which is on top of UDP in general case. Using IP multicast, RTP packets can reach to multiple destinations. However, it does not define specific underlying network layer. RTP Control Protocol (RTCP) which is specified in another section of RTP suggests the simple method for delivery monitoring.

The default level of security services for RTP is specified in RTP profile[3]. For confidentiality of payload, DES-CBC is assumed as default. Derivation of a key is done by MD5 from pass phrases.

2.2 Secure RTP

Secure RTP (SRTP) is ongoing draft and specifies a higher level of security mechanism than that of original RTP. It also fits into the RTP as a profile. The major goal of SRTP is the confidentiality and the integrity protection of RTP/RTCP payloads. SRTP also defines a packet format which is based on RTP [Figure 1], and just adds a master key identifier and a message authentication tag at the end of a RTP packet as options. In order to secure RTP over both wired and wireless links, it suggests an additive stream cipher for encryption and a keyed-hash function for the message authentication. As a default crypto algorithm, it refers AES (Advanced Encryption Standard) with counter mode for encryption and HMAC/SHA1 (Keyed-Hash Message Authentication Code/Secure Hash Algorithm 1) for the message integrity.

SRTP describes the outline of key derivation steps. For

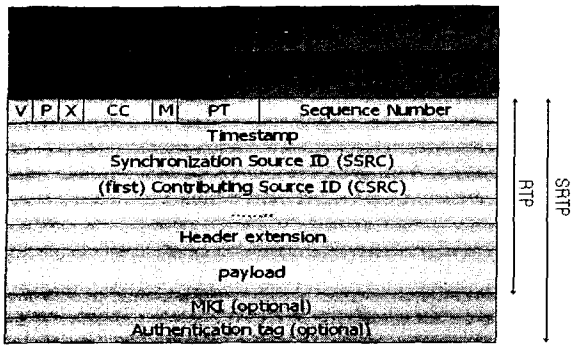

Figure 1. RTP and Secure RTP packet format

a given master key, a master salt and a packet index, it derives session keys for the encryption and the message authentication. Re-keying within a session is dependent on the key_derivation_rate value.

2.3 Signcryption

Signcryption is a new concept of a cryptosystem which fulfills both digital signature and public key encryption simultaneously. Compared with signature-then-encryption scheme, it achieves lower cost of computational as well as smaller communication overhead, since shortened version of digital signature and private key encryption is used in Signcryption rather than combination of two public key based signature and encryption. There are some combinations in implementation of Signcryption. SCS1 and SCS2 are based on the computational difficulty of discrete logarithm with private key ciphering. And there is another combination based on intractability of an elliptic curve with a private key cryptosystem known as ECSCS1, ECSCS2[5].

Table 2 shows that Signcryption fits to key establishment of two parties, because a value can be shared by message m, or two parties can agree on one same value in deriving (k_1,k_2) as a master key.

3. Key establishment protocol for Secure RTP

3.1 Key establishment for the unicast

This section proposes the key establishment protocol based on Signcryption for Secure RTP. The established key is used for re-keying the master key or the master salt. Table 3 shows indirect key transport protocol for Secure RTP. This protocol is variation of indirect key transport protocol using a nonce (IKTUN)[5]. Because synchronization source (SSRC) is known to a receiver by other protocols such as SDP before streaming, it can be used as context information for the authenticated session key agreement. Typically, SSRC needs to expand to at least 40 bits as a nonce appeared in IKTUN.

After the key agreement is done, the given session uses the key as master key to derive session keys ek_i, ak_i and sk_i. If we define a function f and it is mapped to key

Table 1. Parameters for Signcryption

	Parameters public to all:
p	a large prime
q	a large prime factor of p-1
g	an integer with order q modulo p chosen randomly from [1,...,p-1]
hash	a one-way hash function
KH	a keyed one-way hash function
(E,D)	the encryption and decryption algorithms of a private key cipher
	Alice's keys:
x_a	Alice's private key, chosen uniformly at random from [1,...,q-1]
y_a	Alice's public key ($y_a = g^{x_a} \bmod p$)
	Bob's keys:
x_b	Bob's private key, chosen uniformly at random from [1,...,q-1]
y_b	Bob's public key ($y_b = g^{x_b} \bmod p$)

Table 2. Example implementation of Signcryption(SCS1)

Signcryption of m by Alice
$x \in_R [1,..., q-1]$
$(k_1, k_2) = hash\ (y_b^x \bmod p)$
$c = E_{k_1}(m), r = KH_{k_2}(m)$
$s = x/(r + x_a) \bmod q$
=> (c,r,s) =>
Unsigncryption of (c,r,s) by Bob
$(k_1, k_2) = hash\ ((y_a \cdot g^r)^{s \cdot x_b} \bmod p)$
$m = D_{k_1}(c)$
if $KH_{k_2}(m) = r$ then accept m

transformation for a key derivation, then its outputs are a set of encryption keys ek_i, authentication keys ak_i, and salting keys sk_i for a specified master key identifier MKI and a master key key. Salting key sk_i is used to make initialized vectors. After the encryption and the message authentication coding for a given payload, a media sender sends (c, MKI, a) triple to a receiver. This is mapped to the components of Secure RTP packet like below:

* c : encrypted portion of media/simulation data
* MKI : master key identifier
* a : authentication tag

This process is shown in Table 4.

3.2 Key establishment for the multicast

SCS1M and SCS2M are Signcryption method for multiple recipients[5]. Using these schemes, we can design indirect key transport protocol on multicast or broadcast. Table 5 and Table 6 show the example of indirect key transport protocol for multiple receivers. These schemes are based on SCS1M.

Assuming that there are $t(1 \le i \le t)$ receivers. v_i is a random number for a i-th recipient. x_i and y_i are secret key and public key, respectively. The whole process is

Table 3. Indirect Key Transport Protocol for Secure RTP

$x \in_R [1,..., q-1]$
$(k_1, k_2) = hash\ (y_b^x \bmod p)$
$r = KH_{k_2}(SSRC), s = x/(r + x_a) \bmod q$
=> (r,s) =>
$(k_1, k_2) = hash\ ((y_a \cdot g^r)^{s \cdot x_b} \bmod p)$
$key = k_1$
accept key only if $KH_{k_2}(SSRC) = r$

Table 4. Encryption and Decryption in a SRTP session

$ek_i, ak_i, sk_i \in f(MKI, key)$
$c = E_{ak_i, sk_i}(m), a = KH_{ak_i}(SSRC, m)$
=> (c,MKI,a) =>
$ek_i, ak_i, sk_i \in f(MKI, key)$
$m = D_{ek_i, sk_i}(c)$
accept m only if $KH_{ak_i}(SSRC, m) = a$

Table 5. Indirect Key Transport Protocol on multicast

$v_i \in_R [1,..., q-1]$
$k_i = hash\ (y_i^{v_i} \bmod p)$
$(k_{i,1}, k_{i,2}) = k_i$
$r_i = KH_{k_{i,2}}(SSRC), s_i = v_i/(r_i + x_a) \bmod q$
$=>(r_i, s_i)=>$
$k_i = hash((y_a \cdot g^{r_i})^{s_i \cdot x_i} \bmod p)$
$(k_{i,1}, k_{i,2}) = k_i$
$key_i = k_{1,i}$
accept key_i only if $KH_{k_{i,2}}(SSRC) = r_i$

Table 6. Encryption and Decryption on multicast

$ek_{i,j}, ak_{i,j}, sk_{i,j} \in f(MKI, key_i)$
$c_i = E_{ek_{i,j}, sk_{i,j}}(m)$
$a_i = KH_{ak\,i,j}(SSRC, m)$
$=>(c_i, MKI, a_i)=>$
$ek_{i,j}, ak_{i,j}, sk_{i,j} \in f(MKI, key_i)$
$m = D_{ak_{i,j}, sk_{i,j}}(c_i)$
accept m only if $KH_{ak_{i,j}}(SSRC, m) = a_i$

very similar with that of on unicast.

We are developed secure VoIP application (SeeCure Phone) based on proposed protocol [Figure 2]. For implementing Signcryption based key transport scheme, we use Crypto++ 4.2 [6] under Windows system.

4. Analysis

Confidentiality of proposed scheme is dependent on the given block cipher algorithm. In Secure RTP, AES with a counter mode takes the responsibility. SSRC is known

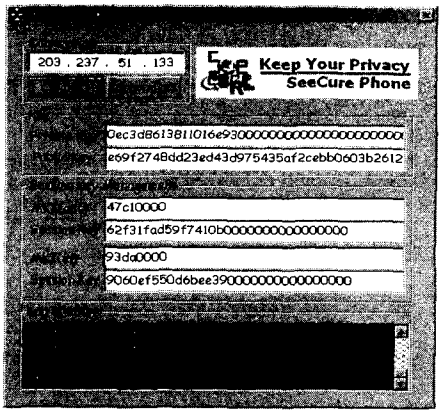

Figure 2. Secure VoIP application

for each party. Hence, The receiver can authenticate the sender by receiving and verifying r for key establishment and a for media data session. The security of a key is assured by the security of Signcryption. The freshness of a session key and a master key is dependent on key_derivation_rate value and the variation of SSRC value. Computational cost for key establishment is affected by two modular exponentiations. There are no modular exponentiations for SRTP packetization.

5. Conclusion

To give functions of confidentiality and authentication, we choose Secure RTP approach. Secure RTP needs to negotiate master key or master salt for the session key transformation. Hence we have described the implementation of key establishment protocol using Signcryption. Signcryption based key transport protocol gives benefit of authentic key establishment between sender and receiver.

6. References

[1] Audio-Video Transport Working Group, H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. " RTP: A Transport Protocol for Real-Time Applications " , IETF RFC 1889, January 1996

[2] M Baugher, and David McGrew, " The Secure Real Time Transport Protocol" , IETF Draft, May 2002

[3] Audio-Video Transport Working Group, and H. Schulzrinne. " RTP Profile for Audio and Video Conferences with Minimal Control " , IETF RFC 1890, January 1996

[4] Yuliang Zheng. " *Digital Signcryption or how to achieve cost*(signature & encryption) << cost(signature) + cost(encryption)" , In CRYPTO '97, vol. 1294 of LNCS, p165 - 179. Springer-Verlag, 1997.

[5] Yuliang Zheng, " Shortend digital signature, sigcryption and compact and unforgeable key agreement schemes" , IEEE1363P Standard for Public Key Cryptography: Additional Technique, July, 1998

[6] Crypto ++ 4.2,http://www.eskimo.com/~weidai/cryptlib.html