A SECURE MEDIA STREAM COMMUNICATION FOR NEXT GENERATION NETWORK

Hao Wu, Zhangdui Zhong
Modern Telecommunication Research Center,
Bejing Jiaotong University, P.R. China

ABSTRACT

In NGN, the open interfaces and the IP protocol make the hazard of security aspect increased accordingly. Thereby, it is a very important premise for NGN network operation to afford a good secure media stream communication. In this paper, we will present a secure media stream communication for NGN. Then we will discuss the three parts of the media stream secure communication——media stream source authentication, secret key negotiation and distribution; media stream encryption/decryption in detail. It can effectively realize media stream end-to-end secure communication. Meanwhile, it also makes use of the expanding of former protocol during the secret key negotiation process.

Key Words: Media Stream, NGN, and Security Mechanism

INTRODUCTION

The next generation network（NGN）is based upon IP protocol, and provides with the guarantee of telecommunication level quality of service (QoS)[1]. From the point of view of network system architecture, hierarchy and opening are the essential characteristic of NGN[2,3]. Considering that NGN enhance the open interfaces, and take the IP as the uniform protocol, the hazard of security aspect is accordingly increased. Although IPv6 can afford more capacity address space, it does not thoroughly solve the security problem. Therefore, network security has

become one of the key technologies that are discussed by ITU-T and ETSI.

With the deployment of NGN and the continuous increase of data service, the secure problem of media stream is more and more important. In NGN, if the transmission of media stream is based on public IP network, the packages can be easily intercepted and eavesdropped. It will lead to being misused by some illegal or malicious users. Consequently, the malicious user will make the user cannot enjoy the service or lead to the QoS decreased; furthermore he will maliciously destroy and attack the service for legitimate user. Thereby, it is a very important premise for NGN network operation to afford a good secure media stream communication. In this paper, we will present a secure media stream communication for NGN.

The traffic in NGN includes two parts: signaling and media. Signaling can be relayed through multilevel concentrated proxy server or soft switch to setup the end-to-end calling; it is a client-server-client communication model. Whereas media in NGN does not need it, it is a client-client communication model, almost completely end-to-end IP package transport. Therefore, signaling and media need apply different secure solution, signaling security can be provided with segment, and media need be provided with end-to-end secure guarantee.

NGN NETWORK SECURE MECHANISM

In NGN, security can be taken into account as three layers: application layer security, transmission layer security and network layer security[4]. Application layer security means secure services integrated in the application layer security, it will take corresponding secure service according to different application, and it integrates the secure service into application protocols or application programs. The security protocol of transmission layer is based on transmission protocol; it can provide the upper application protocol with security guarantee. Now the transmission layer protocol usually adopts transmission layer security (TLS) protocol in IP networks. And network layer security often uses IPSec to solve the security problems in protocol communication process. These three security hierarchy mentioned above can all ensure the media stream security, transmission layer and network layer are mainly ensure the transmission process security, it uses per-segment protection. Because the media stream transmission in NGN is end-to-end, it should provide with end-to-end security service. If using per-segment protection, it needs consider segment secure key negotiation and distribution, segment encryption and decryption and so on. These will lead to the system performance burden, and not good for media

stream security guarantee completely. So media stream secure communication is better to take application layer security mechanism, which can implement by special end-to-end application layer security protocol, and the transmission node between two ends can be looked as transparent.

Media stream secure should include three parts: source authentication, secret key negotiation and encryption authentication. Source authentication is used for ensuing the trustiness ability of transmission client; end-to-end encryption authentication is used for ensuing the privacy and integrality of the media stream; secret key negotiation provides the end-to-end encryption authentication key of the media stream. From the practical point, this paper gives a new media stream secure communication solution. Then, we will separately give the solution of media stream source authentication, secret key negotiation and end-to-end encryption authentication.

MEDIA STREAM SOURCE AUTHENTICATION

Before media stream transmission, the user firstly should perform the media stream source authentication, which uses the authentication mechanism based on AKA[5]. Client and authentication center share one secret key in this authentication mechanism, the secret key is the basis key of the whole system, which needs proper keeping. The network facility and terminal have the ability not leak out the key to third party and to resist illegal stealing. Between authentication center and client, the same authentication algorithm f1( ) is taken, its authentication procedure is described as below (also shown in figure 1):

1.Client sends the registration package to Soft Switch (SoftX) according to the protocol procedure;

2.SoftX sends the user authentication request to Authentication center (AuC), and affords the user Client ID;

3. From Client ID (IDc), AuC can acquire the key that is shared with Client and other authentication information，then AuC generates a challenge random number Rand, Rand，IDc and share secret key Kc all together generate the validate word Auth_C for Client;
Auth_C=f1(Rand, IDc, Kc)
AuC will take Rand, validate word Auth_C as the authentication request’s response, and

sends back to SoftX;

4.SoftX storages Auth_C，and sends Rand to Client;

5. Client takes out the share secret key Kc, IDc and Rand which is sent back from AuC, and computes the response word Res_C
Res_C=f1(Rand, IDc, Kc)
then the registration package is sent to SoftX, which includes the new validate word Res_C;

6.SoftX tests the Res_C which is sent by Client and Auth_C which is sent by AuC for validity, if
Auth_C!＝Res_C
the validate is unsuccessful, then it will restart the authentication procedure; if
Auth_C=Res_C
means the validate for client is successful, and send back the registration success response to Client.

The above procedure realizes the media stream source authentication.

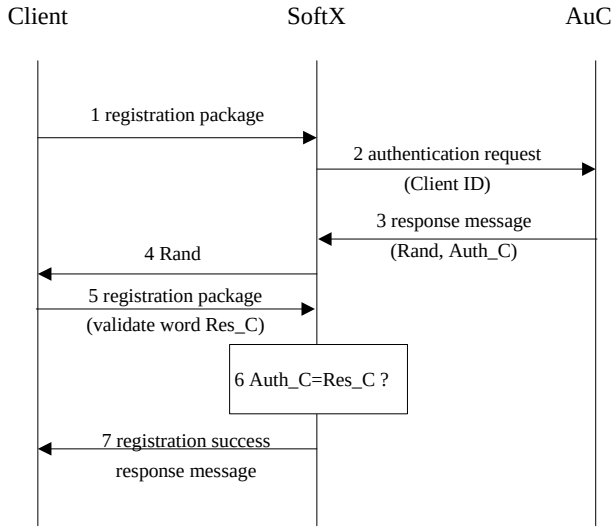

Figure 1: Media stream source authentication procedure

SECRET KEY NEGOTIATION MECHANISM

Generalization

The simplest secret key negotiation mechanism is pre-distributing the fixed secret key, if it uses fixed secret key to perform encryption during the media stream transmission process, illegal attackers may collect user communication information for a long time, and then analyze these information. So the user media channel secret key may be let out, the user private communication information may be eavesdropped, even the media information characteristic may be attacked. Therefore, it must be considered to set up relatively perfect secret key negotiation method in media stream secure mechanism for application layer[6].

In order to ensure the media stream end-to-end encryption in application layer, the secret key of packages security service, which are provided by media stream secure mechanism, are performed in application layer. For ensuring the usability of secure mechanism, the secret key negotiation of media stream application layer which is given in this paper should try its best to consult or expand the former procedure; meanwhile, it must try its best to reduce the modification of quondam standard protocol.

Realization Mechanism

In this paper, it carries out the media stream secret key negotiation mechanism by expanding session description protocol (SDP) ability in calling process. At one time, for ensuring end-to-end encryption in application layer, it uses the key distribution method which are produce by center and distributed separately After performed SDP Offer-Answer negotiation procedure by both sides, the soft switch facility determines the uniform encoding/decoding format of both sides, it takes the terminal security ability parameter (including encrypting and authenticating arithmetic, etc.) as the expanding of SDP, the negotiation is implemented during the session set up procedure, As the negotiation is completed, soft switch facility designates the session secret key and terminal source identifying information of media stream used in their communication for each other, and sends to terminal after it is encrypted by SP.

The media stream negotiation is between ClientA and ClientB, firstly, we will introduce the important parameters and algorithms related to negotiation procedure.

Kc, seed key pre-place.

E1, secret key generation algorithm, which is used for generating encryption secret key between SoftX and Client;

E2, secret key generation algorithm, which is used for generating authentication secret key between SoftX and Client;

f2, encryption algorithm, which is used for confidentiality protection of media stream secure parameters;

f3, authentication algorithm, which is used for integrality protection of media stream secure parameters;

f4, secret key generation algorithm, which is used for generating authentication algorithm secret key of media stream transmission information;

f5, secret key generation algorithm, which is used for generating encryption algorithm secret key of media stream transmission information;

f7, media stream authentication algorithm, which is used for integrality protection of media stream information;

f8, media stream authentication algorithm, which is used for integrality protection of media stream information;

As shown in Figure 2, media stream negotiation procedure implement in application layer is described:

1. Client A initiates the call request message M_Invite to soft switch facility (SoftX). In report package, except for terminal media stream capability information mA, it also contains terminal media stream secure parameters list information mAS.

M_Invite =（mA || mAS）

In order to ensure the security of these secure parameters list information, Client uses session secret key Kc, meanwhile it generates random number RandA, and educes the encryption secret key and authentication secret key. Then it uses the encryption secret key KSPA_C between SoftX and ClientA to encrypt secure parameters list. And it also uses the authentication secret key KSPA_A educed by Kc, SoftX and ClientA to realize the signaling packages' integrality and source protection.

KSPA_C=E1(Kc,RandA)

KSPA_A=E2(Kc,RandA)

CPs=f2(Kc, KSPA_C, mAS)

Sd=f3(Kc, KSPA_A, mA || mAS)

C_Invite ={mA || Sd || CPs}
Client A sends message C_Invite to SoftX.

2. SoftX receives the message C_Invite, and takes out the pre-stored Kc and KSPA_C, computes
XPs= f2(Kc, KSPA_C, CPS)
then computes
Xd= f3(Kc, KSPA_A, mA || XPS)
If Xd=Sd, it means this message is correct, and XPs is the decrypting secure parameters list mAS.

3. Then SoftX saves mAS, the secure parameters list information of ClientA, meanwhile, it initiates the call request package Invite to ClientB. it is unnecessary to carry the secure parameter information of ClientA in that package.

4. ClientB sends a response message to SoftX, the communication procedure between ClientB and SoftX is similar as 1-3 above. Finally ClientB sends the message mBS, which carries the media stream secure parameters list of ClientB, to SoftX. Accordingly, SoftX saves the media mBS.

5. From media stream secure parameters list of ClientA and ClientB, SoftX determines the appropriate media stream secure parameter mA,BS, such as encryption algorithm and authentication algorithm. Meanwhile, SoftX generates the encryption secret key and authentication secret key, which is used for this media stream communication. Generally, SoftX generates the later encryption secret key KcA,B and authentication secret key KaA,B. from secure parameters of ClientA and ClientB and variable parameter P (such as random number and counter number).
KcA,B=f5(mAS,mBS,P)
KaA,B=f4(mAS,mBS,P)

6.SoftX sends the response message to Client A, which carries the media stream secure parameters KcA,B and authentication secret key KaA,B determined by SoftX. For ensuring the signaling transmission security, the transmission information between SoftX and ClientA uses the similar security protection procedure as 2.

7. SoftX sends the response message to ClientB, the procedure is similar as 6.

8. Between ClientA and ClientB, it shares the encryption secret key KcA,B and authentication secret key KaA,B used for media stream transmission.

The above procedure provides one secret key once mechanism, when the media stream communication is finished, the applied encryption secret key and authentication secret key will be cancelled, and will be regenerated until next time media stream communication.

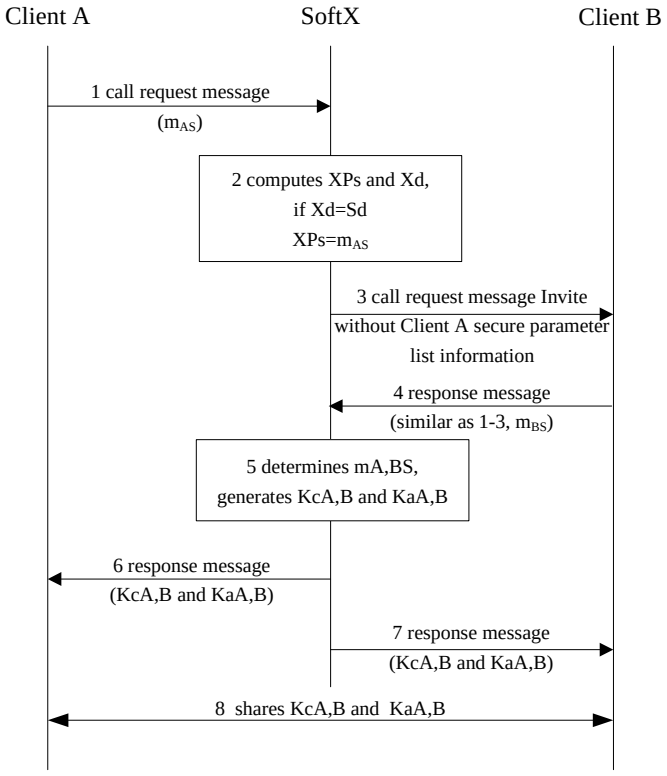

Figure2: Media stream secret key negotiation procedure

ENCRYPTING AND DECRYPTING MECHANISM OF MEDIA STREAM

According to the encrypting or authenticating algorithms and media stream communication secret key during the negotiation procedure, terminals encrypt the packages or perform packets integrality protection. While both sides communicate, transmitting end performs authentication and decryption with each other by means of the same algorithm and secret key that are

negotiated with receiving end. Consequently, it realizes the end-to-end media stream security guarantee function.

Encrypting and decrypting process are relatively simple, when arrived secure start-up time, the secure procedure between ClientA and ClientB is as following:

1.Client A sends media stream message MA,B to ClientB, the following process will be performed:
CA,B=f8(KcA,B, MA,B)
AuthA,B=f7(KaA,B,CA,B)
then Client A sends media stream message (CA,B||AuthA,B) to ClientB.

2.Carries through encryption in application layer, so the message is transmitted transparently though the network, it means that the message will entirely transmit to ClientB.

3.Client B receives the media stream message (CA,B||AuthA,B)，then performs the later procedure
takes out KaA,B, and computes
ResA,B= f7(KaA,B,CA,B)
If AuthA,B=ResA,B, it means the message verification is correct, then takes out decryption secret key KcA,B , computes
RA,B= f8(KcA,B, CA,B)
Finally it gets the media stream message MA,B transmitted by ClientA.

4、While ClientB transmits message to ClientA, it uses the similar procedure.

In NGN application, for ensuring the performance generality, the package format of media stream packagez being encrypted and authenticated may refer the expanded RTP package format[7,8]. This package format is similar with the RTP package format, but the package encryption range, authentication range and the location of encryption and authentication information are added in the package.

CONCLUSIONS

Through the method we discussed above, this paper can effectively implement media stream end-to-end secure communication. It uses the method similar to AKA to realize the media stream source authentication, and generates the secret key by soft switch to provide one secret key once negotiation mechanism during the media stream communication between clients. The later media stream communication utilizes secret key distributed by soft switch, and effectively realizes the end-to-end confidentiality and integrality protection for information transmission.

Moreover, this paper also makes use of the expanding of former protocol during the secret key negotiation process. In encrypting and decrypting mechanism, it can ensure the better scalability and realizable ability by applying the standard format.

References

1 Han L., Duan X.D., Zeng Z.M.&Ding W., "Research on the adaptive QoS paradigm of wireless broadband applications in NGN," International Conference on Communication Technology Proceedings, Volume: 2 ,pp. 905-908, Beijing, China, 9-11 April, 2003.

2 Modarressi, A.R.&Mohan, S., "Control and management in next-generation networks: challenges and opportunities," IEEE Communications Magazine, IEEE ,Volume: 38 ,Issue: 10 ,Oct. 2000, pp. 94 – 102.

3 Kyung-Hyu Lee Kyu-Ok Lee &et. al, "Architecture to be deployed on strategies of next-generation networks," IEEE International Conference on Communication, pp. 819 – 822, Anchorage, Alaska, 11-15 May, 2003

4 "NGN barrier network security". ctiforum.com/forum/2003/02/forum03_0204.htm, 10 Feb, 2003.

5 Boman, K., Horn, G., Howard, P.&Niemi, V., "UMTS security," Electronics & Communication Engineering Journal , Volume: 14 , Issue: 5 , Oct. 2002, pp. 191 – 204.

6 Borella, M.S., "Methods and protocols for secure key negotiation using IKE," IEEE Network Magazine, Volume: 14 , Issue: 4 , July-Aug. 2000, pp. 18 – 29.

7 "Security Mechanism Agreement for the Session Initiation Protocol (SIP),"IETF RFC3329 January, 2003.

8 V. Hallivuori, "Real-time Transport Protocol (RTP) Security. Seminar on Network Security," Helsinki Univ. of Technology (FI), 2000.