Speech bandwith requirements in IPsec and TLS environment

MIROSLAV VOZNAK
CESNET, z.s.p.o.
Zikova 4, Prague
CZECH REPUBLIC
miroslav.voznak@vsb.cz

Abstract: - This paper deals with impact of security on bandwith requirements of IP telephony. There are presented the results of the analyzing of voice over secure communication links based on TLS and IPsec, especially on open-source solutions OpenVPN and OpenSwan. The paper explains how the implemented security mechanisms can affect RTP flows. The presented results are based on numerous experiments which have been performed in a real IP network. An ability to determine the bandwith requirements of RTP flows is important for the proper design of VoIP communication.

Key-Words: - Bandwith, RTP, TLS, IPsec

1 Introduction

The speech quality in IP environment is affected by many parameters, if we wanted to determine the network influence we would mention mainly the delay and the packet loss. The latter is caused by an insufficient ability of network to provide the required bandwith and the impact of packet loss is considerable because the speech quality is very sensitive to this issue. Packet loss is identified as the degradation most typical of VoIP. It is the reason why there is necessary to evaluate the ability of IP network to provide the voice services in appropriate quality. Virtual Private Network (VPN) is a technology to construct a private network over public networks. OpenVPN [1] and OpenSwan are the most popular software-based VPN products and have high flexibility. The usability of OpenVPN or OpenSwan is high because offers an open-source, cost-effective and widely testet solution, not requiring expert knowledge. Software VPN products are popular, because they don't need any appliance and provides such solution which is based on matured protocols. On the other side the using of VPN increases an overhead which is affected by encryption and this overhead can influence overall speech quality [2]. This paper contains a description of TLS and IPsec and their possibilities regarding a configuration, than there is explained a core of the TLS matter which is the splitting of a RTP packet to equally divided blocks.

This work was supported by CESNET, z.s.p.o. in a framework of its research plan MSM6383917201 financed by MSMT CR. This paper includes the result achieved by author in a research activity Multimedia transmissions and collaborative environment, http://www.ces.net/project/15/ .

2 TLS and IPsec mechanisms

TLS ensures a secured connection which is encrypted and decrypted with the keys negotiated during a phase of keys exchange. The key exchange and authentication algorithms are typically public key algorithms but subsequent data exchange is usually done by symmetric ciphers because of considerably faster processing. Of course, symmetric encryption is more suitable for IP telephony and this paper deals only with this type of ciphers [3]. TLS involves three main phases such as negotiation of supported algorithms, keys exchange and authentication and in the end symmetric encryption of transmitted data. IPsec is in fact a collection of standards that all deal with using cryptography to ensure authenticity and in almost all cases to also guarantee confidentiality of the content of the IP packets. Authentication Header (AH) is the first protocol of IPsec suite that only provides authentication and does not encrypt the payload. Encapsulated Security Payload (ESP) is the second protocol its task is not only to authenticate the packet, like AH, but also to add a security policy to the packet, and optionally encrypt it. Originally ESP provided no authentication, there was necessary to build an IP packet in ESP in AH to achieve integrity and privacy. ESP now provides for authentication as well, in a very similar form to AH.

2.1 OpenSwan

Openswan is an implementation of IPsec for Linux and can be considered an IPsec solution for all Linux distributions. IPsec is a peer-to-peer protocol. Not all IPsec peers are either clearly the client or the server. They could even be considered a client for one tunnel, and a server for another. For these reasons, the concepts of left and right are used At first the IPsec public keys have to be generated and subsequently are used as a leftrsasigkey and rightrsasigkey in the configuration file /etc/ipsec.conf.

```
conn example
left=158.196.81.116
right=158.196.81.103
auth=ah
auto=route
leftrsasigkey=
rightrsasigkey=
```

IPsec requires a key exchange of a secret this is mostly done automatically by so called IKE daemons pluto. We can verify that pluto is running, for this purpose we use a directive psec verify and eventually start up by directive ipsec pluto.

2.2 OpenVPN

The endpoints establishing VPN tunnel in OpenVPN are declared one as server and the other as client. Before establishing the VPN, the client first reaches the server on a specific port, whereas the server doesn't need to reach the client. Configuration files are located in directory /etc/openvpn as server.conf or client.conf. The tunnel can be established on UDP or TC P, unfortunately TCP protocol is more widespread although UDP is more effective because of real-time applications. The part regarding a configuration of TLS is listed below. The first Certificat Authority must be configured to sign certificates consequently is possible to generate keys which are used on user and client sides. The first testbed, where the infulence of OpenVPN on speech quality was observed, had been prepared between University of Ostrava and University of Milan through the broadband research network Géant2.

```
*Server.conf
proto udp
keepalive 10 60 dev tun persist-key persist-tun ifconfig-nowarn ca ca.cert cert ser.cert key server.key dh dh.pem
server 10.0.0.0 255.255.255.0
client-to-client
status openvpn-status.log
verb 0
```

The configuration of server side is mentioned above, the client side configuration is following:

```
*Client.conf
remote 159.149.153.68
dev tun
client 10.0.0.0 255.255.255.0
tls-client
ca ca.cert
cert cli.cert
key client.key
rport 4096
verb 4
ping 10
```

The most important information in configuration files is the type of cipher alghoritm because it affects the number of blocks and overhead as is shown in fig. 1.

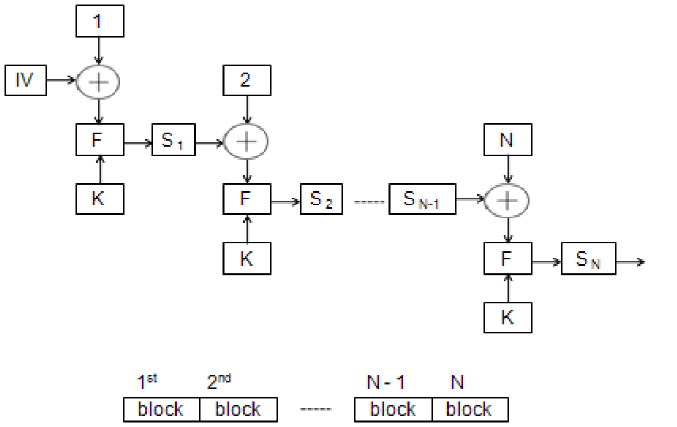

Fig. 1. The number of block affected by CBC mode..

3 Bandwith requirements

The basic steps of speech processing on a transmission side are encoding and packetizing [6], [7]. RTP packets are sent in dedicated times and a difference between them depends on timing [8]. This process of packetizing is given by the following basic equation:

$$\Delta t = \frac{P_S}{C_R} \qquad (1)$$

where Δt [s] is timing in seconds, P_S [b] is a payload size and C_R [kbps] represents a codec rate. The timing can be derived from content of RTP packet as a difference of two consecutive timestamps, see relation (2). Typical value of a sampling frequency is 8 KHz.

$$\Delta t = \frac{\text{timestamp}_{\{N+1\}} - \text{timestamp}_{\{N\}}}{\text{sampling\_frequency}} \qquad (2)$$

There is necessary to express a size of packet at application layer which might be defined by the following formula:

$$S_{AL} = H_{RTP} + P_S \qquad (3)$$

where S_{AL} [b] is the expected size that consists of RTP header H_{RTP} [b] and payload size P_S [b]. Equation (4) determines a size of frame S_F [b] at link layer.

$$S_F = S_{AL} + \sum_{j=1}^{3} H_j \qquad (4)$$

S_F [b] includes a packet at application layer and the sum of lower located headers of OSI model where H_1 [b] is media access layer header, H_2 [b] internet layer header and H_3 [b] is transport layer header.

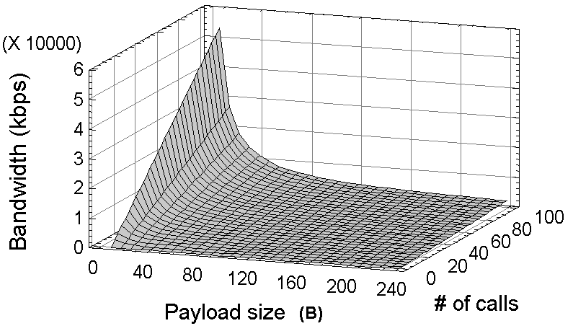

Figure 1. Bandwith as a function of payload size and concurrent calls.

Figure 1 illustrates the relation between bandwith, payload size and number of concurrent calls.

$$BW_M = \sum_{i=1}^{M} \frac{S_{Fi}}{\Delta t_i} \qquad (5)$$

Total bandwith BW_M [kbps], which is required in case of M concurrent calls, we express in relation (5) and if we apply the relations (1), (2) and (4) to the relation (5) so we obtain the following result (6).

$$BW_M = M \cdot C_R \cdot \left(1+\frac{H_{RTP}+\sum_{j=1}^{3} H_j}{P_S}\right) \qquad (6)$$

We have to realize that TLS is located between two layers of OSI model, between application and transport layer and therefore we apply S_{TLS} instead of S_{AL}. This replacement should be done in respect of explained location of TLS and we define a new parameter S_{TLS}, size at TLS layer. S_{TLS} is expressed in relation (7).

$$S_{TLS} = C_0 + \left\lceil \frac{S_{AL}}{B_S} \right\rceil \cdot B_S \qquad (7)$$

We use a symbol $\lceil x \rceil$ to denote the ceiling function where $\lceil x \rceil = \min\{n \in \mathbb{Z} \mid x \le n\}$, it means that ceiling function of x gives the smallest integer greater than or equal to x. The ceiling function was defined by M. Schroeder in 1991 [9] and the symbol was coined by K. Iverson in 1994. The parameter B_S represents a block size which has been explained in figure 1, its value is 64 or 128 bits and depends on applied cipher alghoritm (AES, DES, Triple DES or Blow Fish). C_0 is a constant and equals to zero in case of clear TLS unfortunately OpenVPN adds supplementary overhead that is included in C_0. The value has been achieved by performed experiments. We can claim that this constant $C_0 = 83$ bytes in case of block size 128 bits and $C_0 = 75$ bytes in case of block size 64 bits.

4 Conclusion

Formulas stated in the previous chapter have been proven by experiments.

Table 1 The required bandwith of one call, valid for AES cipher with CBC.

codec	timing [ms]	payload [B]	RTP in Ethernet [kbps]	RTP encapsulated in IPsec [kbps]	RTP encapsulated in OpenVPN [kbps]
G.711	20	160	90,4	117,6	106,64
G.729	10	10	60,8	112	208,8
G.729	20	20	34,4	60	83,6
G.723.1 / 6,3	30	24	24	41,07	50,68
G.723.1 / 6,3	60	48	15,2	23,73	23,03
G.723.1 / 5,3	30	20	22,93	40	50,4
G.723.1 / 5,3	60	40	14,13	22,67	22,89

The formulas presented in this paper help us to understand how secure environment can affect the bandwidth of calls. The contribution of this paper is the presented method of bandwidth calculation. The results obtained were confirmed in a testbed. The bandwidth of any particular call is affected by the length of a cipher block and does not depend on the key size. The results correspond with the formulas stated in chapter 3. This paper is an extension of previous works on the impact of security on the quality of VoIP calls [10]-[12].

References:

[1] OpenVpn,The OpenVpn Project. Available: http://openvpn.net/

[2] M. Vozňák, M. Neuman. The Monitoring and Measurement of Voice quality in VoIP Environment. Technical report 18/2006, CESNET, November 2006. Available http://www.cesnet.cz/doc/techzpravy/2006/voice-quality/

[3] M. Voznak, Impact of security on speech quality, Invited lecture at University of Milan, July.2008. Available http://www.dsi.unimi.it/seminario.php?id=383

[4] Ixia, IxChariot.Available http://www.ixiacom.com

[5] Wireshark, Sniffer. Available http://www.wireshark.org/

[6] M. Halas, B. Kyrbashov, M. Voznak . Factors influencing voice quality in VoIP technology, In: 9th International Conference on Informatics‘ 2007, pp. 32-35, Bratislava, June 2007

[7] M. Vozňák, E. Rocha, B.Kyrbashov. End-to-end delay in VoIP. In proceedings Conference RTT 2007, University of Žilina, 2007, p. 466-469, September 2007.

[8] I. Baroňák, M.Halás, M.Orgoň. Mathematical model of VoIP connection delay. In: Telecommunications, Networks and systems, Conference in Lisboa, 3-8 September, 2007.

[9] M, Schroeder, Fractals, Chaos, Power Laws: Minutes from an Infinite Paradise. New York: W. H. Freeman, p. 57, 1991.

[10] Vozňák M., Nappa A.Performance evaluation of VoIP infrastructure. In FreeVoice, November 2007.

[11] A.Nappa, D. Bruschi, A. Rozza, M.Voznak, Analysis and implementation of secure and unsecure Voice over IP environment and performance comparison using OpenSER. Technical report, 84 pages, published at Universita degli studi di Milano, December, 2007.

[12] M. Voznak, A. Rozza,A. Nappa,Performance comparison of secure and insecure VoIP environments.TERENA Networking Conference 2008, Brugge, Belgium, 19-22 May, 2008.