INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 12, issue 07 (2025)

IMPACT OF SECURITY PROTOCOLS ON REAL-TIME MULTIMEDIA COMMUNICATION NETWORKS

Suyunov Muzaffarjon Nurmurot ugli

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Shaydullayevjahongir@gmail.com

Abstract: This article provides a comparative analysis of the IPsec, H.235, and SRTP protocols used to provide security in multimedia communications. IPsec is a network-layer security protocol that is mandatory for IPv6 and optional for IPv4. It provides data confidentiality, integrity, authentication, and protection against replay attacks. H.235 is a security mechanism in the ITU-T H.323 multimedia standard that provides protection for signaling and media streams. It has two security profiles: basic and signature-based. SRTP (Secure RTP) is designed to encrypt, authenticate, and protect against replay attacks in real-time multimedia streams.

Keywords : Multimedia security, IPsec, H.235, SRTP, RTP, RTCP, Cryptographic transformation, Confidentiality, Authentication, Integrity, Protection against replay attacks, VoIP, Packet filtering, Latency and efficiency, Message authentication, Digital signature, AES, HMAC, DoS attacks, Multimedia traffic.

Annotation: A comparative analysis of IPsec, H.235 and SRTP protocols, used for security and multimedia communication, is presented here. IPsec is a network-level security protocol that is mandatory for IPv6 and optional for IPv4. On obespechivaet konfidentialnost dannyx, tselostnost, authentificationatsiyu i zashchitu ot atak povtornogo vosproizvedeniya. H.235 is a security mechanism and multimedia standard ITU-T H.323, which provides support for signaling and streaming multimedia. It has two security profiles: basic and basic and signature. SRTP (Secure RTP) is designed for encryption, authentication and protection against replay attacks and multimedia streams in real time.

Key words: Bezopasnost multimedia, IPsec, H.235, SRTP, RTP, RTCP, cryptography, encryption, confidentiality, authentication, integrity, protection against replay attacks, VoIP, packet filtering, latency and efficiency, public authentication, digital signature, AES, HMAC, DoS-attack, multimedia traffic.

Abstract: : This article provides a comparative analysis of the IPsec, H.235, and SRTP protocols used to provide security in multimedia communications. IPsec is a network-layer security protocol that is mandatory for IPv6 and optional for IPv4. It provides data confidentiality, integrity, authentication, and protection against replay attacks. H.235 is a security mechanism in the ITU-T H.323 multimedia standard that provides protection for signaling and media streams. It has two security profiles: basic and signature-based. SRTP (Secure RTP) is designed to encrypt, authenticate, and protect against replay attacks in real-time multimedia streams.

Keywords: Multimedia security, IPsec, H.235, SRTP, RTP, RTCP, Cryptographic transformation, Confidentiality, Authentication, Integrity, Protection against replay attacks, VoIP, Packet filtering, Latency and efficiency, Message authentication, Digital signature, AES, HMAC, DoS attacks, Multimedia traffic.

There are various approaches to providing multimedia security. As an IP-level security protocol, IPsec is one possible candidate. SSL/TLS relies on TCP and is therefore not suitable for securing UDP-based multimedia communications. Two other application-level security mechanisms are the H.235 [6] and SRTP [7] standards. H.235 is part of the ITU-T H.323 umbrella standard. SRTP is currently an RFC being developed within the IETF.

IPsec

IPsec [8] is standardized within the IETF and provides security services for the Internet Protocol. It is mandatory for IPv6 and optional for IPv4. IPsec offers two security protocols that can be used independently:

- Encapsulated Security Payload (ESP). ESP provides security services with data confidentiality, integrity, anti -replay , and confidentiality of restricted traffic flows.
- Authentication Header (AH). The security services provided by AH are integrity and anti -replay services.

IPsec can be used to encrypt the media stream (IPsec in transport mode). H.245 capability exchange messages within H.323 indicate that IPsec is supported . Logical channel procedures when a media channel is opened indicate the use of IPsec. Another possibility is to establish a secure channel between two security gateways (IPsec in tunnel mode). In this case, the multimedia application is not aware of the SA and therefore no special signaling is required. The signaling path (RAS, H.225.0, H.245, SIP, RTSP) can also be protected with IPsec.

H.235

includes many ITU-T standards for multimedia communication. This makes it an umbrella standard. Not only signaling protocols (e.g. H.245, H.225.0) are part of H.323, but also codecs (e.g. G.711, H.261), transport protocols (RTP), etc. Finally, the H.235 [8] standard describes security services for H.323. H.235 addresses security services for signaling messages (RAS, H.225.0, and H.245) and media stream (RTP) transmission . Among the security services provided, several mechanisms or algorithms can usually be used to achieve a security service. This flexibility can lead to non-interoperable applications. Therefore, the ITU-T has defined two security profiles that require specific mechanisms and algorithms:

- Basic Security Profile. The Basic Security Profile provides message authentication and integrity for the signaling path . A variant of the Basic Security Profile is the Voice Encryption Profile, which offers encryption of the media stream.
- Signature Security Profile. The Signature Security Profile is recommended as a suitable option for large environments where it is not possible to assign mutual passwords or symmetric keys. The Signature Security Profile provides authentication, integrity, and non-repudiation for signaling messages using digital signatures. This profile can be used in conjunction with the Basic Security Profile.

H.235 also provides an anti-spam mechanism to detect flooding in traffic.

SRTP. Real-time Transport Protocol (RTP) [10] is the most widely used protocol for real-time data. Almost every Internet multimedia application relies on RTP to package data by codecs. RTP itself does not provide any security mechanisms beyond encrypting the packet payload. Secure RTP (SRTP) [7] provides confidentiality and authentication for RTP and RTCP instead . It also provides protection against replay attacks. SRTP is defined as an RTP profile in the Audio Video Profiles (AVP) and is registered as "RTP/SAVP".

Encryption of SRTP or SRTCP packets is optional, while authentication is mandatory for RTCP but optional for RTP.

Security scope. IPsec provides authentication of the IP payload and encryption of the IP header and IP payload. All layers above use IPsec security services. H.235 only considers confidentiality and antispam for RTP. SRTP offers confidentiality, message authentication, and replay protection for RTP and RTCP.

Confidentiality. IPsec's Encapsulating Security Payload (ESP) provides confidentiality for IP datagrams. The format is designed to support a variety of encryption algorithms . The only mandatory cipher is DES operating in cipher block chaining (CBC) mode.

To encrypt RTP packets, H.235 uses the following algorithms in CBC mode: RC2, DES, and 3DES.

SRTP generates a pseudo-random key stream that is XORed with the payload to encrypt the payload of RTP packets. AES [11] is the standard encryption scheme used to generate the key stream in Segmented Integer Counter (SIC) mode. AES in f8 mode is additionally defined. Both modes operate in block cipher encryption mode, but SRTP can be extended to any other transform.

Data integrity and message authentication. To improve the usability of the statistical values provided by RTCP reports, it is important to ensure the integrity of these values, such as the jitter between arrivals and the packet loss rate. The authenticity of control messages, such as the BYE packet, is even more important. Therefore, message authentication and data integrity cannot be compromised . Since real-time multimedia systems require minimal latency of media packets, in the case of bit errors and missing encodings in the RTP payload , it is more advantageous to use corrupted data than to discard it as invalid instead of retransmitting it. However, it is difficult to distinguish between spurious content and simple bit errors .

The AH security protocol within IPSec provides data integrity and message authentication for IP packets. Message authentication is based on the use of Message Authentication Codes (MAC). AH must support two MAC algorithms : HMAC/MD5 (96 bits) and HMAC/SHA-1 (96 bits) [12]. The MAC is calculated from IP header fields that do not change during transmission and payload .

The integrity of RTP and RTCP streams in H.235 is for further study . If an attacker modifies the RTP payload , the receiver decrypts the encrypted portion of the packet and processes the payload using the media codec regardless of whether the packet has been modified or not.

The authenticated part of an SRTP packet consists of the RTP header followed by the (encrypted) payload of the SRTP packet. Thus, if the header or payload is modified , SRTP discards the packet. HMAC/SHA-1 [12] is the standard algorithm for ensuring integrity and message authentication in SRTP. The problem with HMAC/SHA-1 is the fixed and large size of the MAC (20 octets). In SRTP, it is truncated to the leftmost 32 bits. As [12] points out, truncating the output of an HMAC to less than half increases the possibility of attacking the MAC due to the birthday attack. SRTP does not force the MAC to 32 bits. Alternatively, other MAC algorithms can be used.

Packet source authentication and user authentication. Not all schemes provide a way to authenticate the packet source. None of the analyzed security protocols has a mechanism to

provide source authentication in multicast configurations. Several schemes have been published and proposed to solve this problem, but no standardization has been achieved.

supports several authentication methods, such as pre-shared key authentication and public key encryption , they do not support perfect user authentication.

In H.235, authentication is done using pre-shared secrets. This can be a static password or other information . Digital certificates can be used.

As with IPsec , user authentication in SRTP depends on a separate protocol. Typical tasks include negotiating cryptographic parameters, mutual authentication, exchanging session keys, and establishing a secure session. The Multimedia Internet Key (MIKEY) [13] protocol has been proposed for this, but any other suitable protocol can be used .

Replay protection. AH in IPsec protects against replay attacks. This is done by maintaining a replay list on the receiving side that contains the indexes of all received authenticated packets.

In H.235 , the receiver does not check the index of the incoming packet against the replay list. Replay protection in H.235 is for further study .

In SRTP, RTP header and payload authentication provides indirect replay protection by authenticating the sequence number. In fact, replay protection is only possible if integrity protection is present . When message authentication is enabled , SRTP protects against this attack by using a replay list that is similar to the list used in IPsec.

DoS protection. IPsec and SRTP have no countermeasures against message flooding.

H.235 defines a mechanism for media anti-spam. The sender calculates the MAC from the first block of the RTP header and adds it to the RTP packet. The receiver can quickly determine whether the RTP packet originated from an unauthorized source. This can also be seen as lightweight packet authentication .

used in IPsec and SRTP to provide message authentication are very similar to the media anti-spam described in H.235. The only difference is the amount of information that goes into MAC calculation and verification.

Error propagation. In the case of CBC, a transmission error affects two plaintext blocks. Suppose that one RTP packet has two frames (24 octets per frame) and the encryption algorithm has a block size of 16 octets . If a single bit error occurs in the first encryption block during transmission, the receiver will lose the first frame and 8 octets of the second frame after decryption .

In the case of SRTP , the process of encrypting a packet by XORing it with the key stream does not lead to error propagation.

In all cases, the propagation of the error is limited to the corrupted packet.

additional latency due to encryption and MAC generation/verification .

Sending side:

$IPsec calculation delay = Enc(UDP header || RTP header || RTP payload) + GenMAC(ESP header || UDP header || RTP header || RTP payload)

Receiving side:

IPsec calculation delay = Dec(UDP header || RTP header || RTP payload) + VerMAC(ESP header || UDP header || RTP header || RTP payload)

H.235 encrypts and decrypts the payload of each RTP packet. It also calculates and verifies the MAC in a small part of the RTP header.

Sending side:

H.235 calculation delay = Enc (RTP payload) + GenMAC (RTP header)

Receiving side:

H.235 calculation delay = Dec (RTP payload) + VerMAC (RTP header)

In SRTP, the packet encryption/decryption process consists of XORing this key stream. Furthermore, the MAC is calculated from the RTP header and the (encrypted) RTP payload.

Sending side:

SRTP calculation delay = Enc (RTP payload) + GenMAC (RTP header || RTP payload)

Receiving side:

SRTP calculation delay = Dec(RTP payload) + VerMAC(RTP header || RTP payload)

Packet filtering support . Since multimedia communication is protected end-to-end, the use of IPsec prevents packet filtering. A packet filter cannot decrypt the IPsec-protected payload to analyze addresses and ports on the way from sender to receiver.

H.235 and SRTP do not affect packet filtering because encryption is done at OSI layer 7.

Table 1 below compares IPsec, H.235, and SRTP protocols:

Table 1.

Brief description of features

	IPsec	H.235	SRTP
Key management	+	+	-
User authentication	+	+	-
RTP payload integrity	+	-	+
RTCP protection	+	-	+
Pre-calculation	-	-	+
Error propagation	+	+	-

Expand data volume	+ (Top)	+ (Medium)	+ (Low)

Latency . After implementation , we took steps to understand how much latency was introduced by H.235 and SRTP due to cryptographic changes and how to adjust QoS parameters if necessary. Since both tested protocols use only symmetric cryptography, the additional latency is reasonably kept. Table 2 shows some results collected on an Intel Pentium II system with a frequency of 350 MHz, 128 MB RAM and MS Windows operating system .

Table 2 .

Delay time measurement results

Cryptographic transformation	GSM-1 (33 octets)	GSM-4 (132 octets)	G.711-1 (240 octets)	G.711-5 (1200 octets)
AES/SIC	Enc: 0.08 ms Dec: 0.08 ms	Enc: 0.12 ms Dec: 0.12 ms	Enc: 0.16 ms Dec: 0.16 ms	Enc: 0.52 ms Dec: 0.52 ms
AES/f8	Enc: 0.11 ms Dec: 0.11 ms	Enc: 0.16 ms Dec: 0.16 ms	Enc: 0.18 ms Dec: 0.18 ms	Enc: 0.52 ms Dec: 0.52 ms
3DES/CBC	Enc: 0.48 ms Dec: 0.48 ms	Enc: 0.80 ms Dec: 0.80 ms	Enc: 0.94 ms Dec: 0.94 ms	Enc: 2.5ms Dec: 2.5 ms
HMAC/MD5	Gene: 0.09 ms Time: 0.09 ms	Gene: 0.11 ms Time: 0.12 ms	Gene: 0.15 ms Time: 0.15 ms	Gene: 0.27 ms Time: 0.28 ms
HMAC/SHA-1	Gene: 0.21 ms Time: 0.23 ms	Gene: 0.27 ms Time: 0.29 ms	Gene: 0.30 ms Time: 0.31 ms	Gene: 0.55 ms Time: 0.55 ms

adds a total of 0.6 ms to the final latency when applied to a VoIP application using the GSM codec (1 frame per RTP packet) and standard algorithms (AES/SIC, HMAC/SHA-1) .

References:

1.R. I.Isayev , D.Khibatova. “Multimedia communication networks”. Tashkent University of Information Technologies, Tashkent, 2019.

2. ITU-T Recommendation H.235 Version 2: Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals (2000).

3.Y. Kim, A. Perrig and G. Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups", ACM CCS'2000, 2000.

4. E. Bresson , O. Chevassut, D. Pointcheval and J. Quisquater, "Provably Authenticated Group Die-Hellman Key Exchange", Proc. of the 8th ACM CCS'01, 2001.