Information Technology Journal 3 (3): 311-314, 2004
ISSN 1682-6027


# Analysis of Real-time Transport Protocol Security

Junaid Aslam, Saad Rafique and S. Tauseef-ur-Rehman
Department of Computer Sciences, Faculty of Applied Sciences,
International Islamic University, Islamabad, Pakistan

**Abstract:** This study describes RTP and its security related features. The emphasis is on the effect and efficiency of the cryptographic and authentication algorithms recommended by RTP and its profiles. For judging efficiency of the recommended algorithms, a java based implementation was developed and a comparison between them was described. The study also describes in brief the security features that are available when RTP is used along with higher level protocols like SIP, SAP, SDP and H.323.

**Key words:** RTP, RTP security, security, RTP profile security

**Introduction to Real-time Transport Protocol (RTP):** Real-time Transport Protocol[1] is an application level protocol that is intended to transmit real-time data such as audio and video. RTP is used for multi-media sessions like business conferences and telemedicine sessions. Real-time transport protocol supports both the unicast and multicast sessions provided the underlying network is multicast capable. It facilitates network transport functions but does not guarantee timely delivery of packet.

RTP is an application level protocol that provides application level framing and is integrated into application processing rather being implemented as a separate protocol stack.

RTP consists of two parts, RTP and RTCP, where, RTP is responsible for providing media transmission, while RTCP provides the feedback information on transmission quality.

**Introduction to RTP Profiles:** RTP is never intended to be a complete protocol but rather as a framework for building application protocols[1] and thus in contrary to other protocols, it is usually implemented by each application according to its requirements for which profiles are defined. A profile defines extensions or modifications to RTP that are specific to a class of applications, services and algorithms that may be offered.

**Secure Real-time Transport Protocol (RTP):** The security features provided by RTP may not fulfill the needs of applications that require extensive security. Such applications can consider the use of Secure Real-time Transport Protocol (SRTP)[2]. SRTP is a RTP profile that is meant to provide more conventional security services that may be offered. It defines the set of additional cryptographic and authentication algorithms and allows introducing new ones.

**RTP profile for audio and video conferences with minimal control:** This profile[3] describes how audio and video data may be carried within RTP and describes the usage of fields left unspecified in RTP. This profile provides a framework for new profiles that may be defined. The SRTP profile is an extension to this profile since all aspects of this profile may apply with addition of SRTP security features.

**Security consideration:** Studies have shown that users may be more sensitive to privacy concerns with audio and video communication than they have been with more traditional forms of network communications[4]. RTP relies on services provided by lower layer protocols for most of its security requirements. However, some methods are described for authentication and some algorithms are specified for attaining confidentiality by RTP or its profiles.

**Confidentiality:** RTP sessions like business conferences and telemedicine sessions do require confidentiality. Confidentiality means that only the intended receiver can decode the received packet; for others, the packet contains no logical information. Confidentiality of the content is attained by encryption. RTP and its profiles have recommended few algorithms that may be used for encrypting RTP payload.

**Corresponding Author:** Saad Rafiq, Department of Computer Sciences, Faculty of Applied Sciences,
International Islamic University, Islamabad, Pakistan
Tel: 92 51 9266895 7 E-mail:saadrafique@hotmail.com

**DES:** Data Encryption Standard (DES) is the default cryptographic algorithm for RTP applications. The mode used is DES-CBC. The DES-CBC mode was chosen because it has shown to be easy and practical to use in experimental audio and video communication. The CBC mode has the advantage of having the random access property for decryption which guarantees that any lost packet could only prevent decoding of itself and the following packets of that specific block[5]. The remaining transmission is not affected by this loss.

DES is good choice as the overhead caused by it is hardly noticeable compared to the CPU requirements of modern compression algorithms of voice and video. Also, it is a fast to execute algorithm that is good for real time data. But DES has been found to be easily broken with specialized hardware[6]. Also, the DES is mainly designed for hardware implementation. It is difficult to implement efficiently on software and therefore, not an optimal choice for huge amount of time sensitive data.

**Triple DES:** Since DES has been easily broken, the usage of a stronger encrypting algorithm is recommended. The leading candidate for a replacement to DES is triple DES. Triple DES is a three level construct using DES at each level. Unfortunately the triple DES is much slower and takes a lot of processing time since it is encrypted three times over. Also the block size of triple DES is not bigger than DES, the 64 bit block size has security implications of its own. Triple DES fails to address the problems of manipulating individual bits of the following packets if an attacker manages to get a packet.

**AES:** RTP profile SRTP recommends AES[7] with Counter Mode (CM) and f-8 mode. The f-8 mode is used for wireless transmission. AES overcomes the flaws of individual bit manipulation, introduced by CBC mode because it has the property that the encryption and decryption of one packet does not depends on preceding packets. The security of CM has been proven by Bellare[8]. Their analysis shows the security of CM can be better than that of CBC.

AES would be a good choice because it has a larger block size of 128 bits. AES offers larger encryption key. The key size can vary from 128,196 and 256 bit and can be used according to user requirements. In addition to increased security that comes with larger key sizes the AES can encrypt data much faster than triple DES, due to the reason that AES has a lot of inherent parallelism in implementation, making it easy to utilize processor resources efficiently.

**Efficiency comparison of recommended encryption algorithms:** A Java based implementation of real-time audio and video transmission "TranSecure" was developed to provide the encrypted transmission of real-time data. The data was encrypted using the recommended algorithms (Fig. 1) and the efficiency was noted for transmitting 1, 383 KB test file using a 1.GHz P-IV machine over a 100 Mbps fast Ethernet.

**Authentication:** Authentication means guarantee of originator and of electronic transmission. It is useful to verify the authentication of the receiver to assess the trustworthiness. RTP does not specify any authentication except that implicit authentication is assumed if encryption is present. However, its profiles specify some authentication methods.

**MD5:** This RTP profile[3] specifies hashing algorithm MD5 and describes a method that retrieves authentication key from the password that may be used for authentication[9]. The massage digest MD5 hash algorithm is considered to be as strong as 128 bit hash code so the difficulty of finding a message with a given digest is of the order $2^{128}$ operations.

**Secure hash algorithm:** The profile SRTP[2] recommends that each SRTP stream should be protected by SHA-1. The default session authentication key-length is 160-bits while the default authentication tag length shall be 80 bits. SRTP recommends that it should not be used without message authentication because the predefined encryption algorithms does not provide any message authentication[2]. The SRTP allows small authentication tags of 32 bits for 3G networks where under certain link technologies, even few additional bytes could result in significant result of efficiency[10]. The security provided by 32 bit tag is limited and is allowed for restricted set of applications.

**Comparison of MD5 and SHA-1:** 160-bit SHA-1 is 32 bit longer than 128-bit MD5, thus if neither algorithms contains any structural flaws that are vulnerable to cryptanalytic attack, then SHA-1 is a stronger algorithm.

The SHA involves more steps (80 vs 64) and must process 160 bit buffer compared to 128 bit buffer of MD5. Thus SHA should execute about 25% slower than MD5 on same hardware.

A comparison of both the authentication tags in the Java based implementation is given in Fig. 2.

**Security provided by underlying protocols:** RTP itself relies either on underlying protocols for security purposes or the higher level protocols that are implemented on RTP framework, which defines its own security features that may be used. Below here, we will discuss the protocols and the security that can be provided by them when used alongwith RTP.

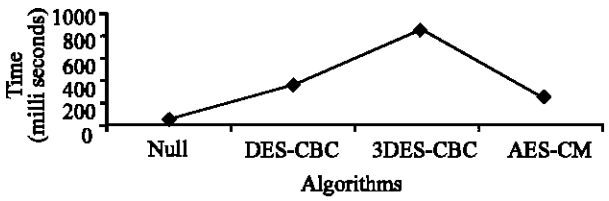


Fig. 1: Comparison of time taken by recommended algorithms

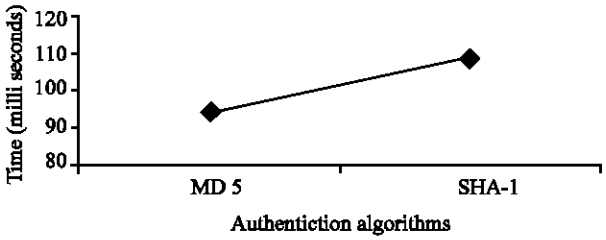


Fig. 2: Comparison of recommended authentication algorithms

**IPSec:** IPSec[11] is considered to be responsible for providing security features, as being the underlying protocol of RTP. It provides services for confidentiality and for authentication it uses its authentication header. IPSec is a comprehensive solution for unicast sessions but it has failed to specify the support for multicast sessions. Thus the higher level protocols need to define their own security services.

**Session initiation protocol:** This protocol has the particular ability of distributing the encryption keys and other security parameters. It supports various encryption algorithms and methods, that can provide security to RTP when used with it.

**Session announcement protocol:** This protocol is intended for broadcast information. It has variety of authentication methods such as PGP. Since it is intended for public session announcement, encryption is discouraged.

**Session description protocol:** This protocol may be considered as the high level protocol than SIP and SAP and consequently it usually works in conjunction with SIP and SAP to transport itself. Keys for RTP are distributed using SDP. SDP itself is neither encrypted nor authenticated and usually uses SIP and SAP for such services.

**H. 323:** This is the most widely used protocol for applications such as telephony and VOIP. It has profile like RTP that describes security services (Table 1). The

Table 1: Common RTP configuration

| | RTP | RTP+IPSec | RTP+SDP | SRTP+H.323 |
|---|---|---|---|---|
| Key/algorithm setup | No | Yes | Yes | Yes |
| Confidentiality | Yes | Yes | Yes | Yes |
| Session authentication | Implicit | Yes | Yes | Yes |
| Session integrity | Some | Yes | Some | Yes |
| Transmitter authentication | Unicast | Unicast | Unicast | Multicast |
| Multicast support | Yes | No | Yes | Yes |

possible security services have been defined by ITU-T[12] which describes that H.323 be used with SRTP instead and hence provides security services that also supports multicast sessions.

**Conclusion:** Security facilities provided by the RTP protocol alone are inadequate. RTP has an excellent design since it provides a framework for high level protocol which in turn can implement their own security services that may eventually provide benefit to RTP itself. RTP cannot rely on underlying network just because it is transmitted over IP and considering IPSec will consequently provide the security services. Services provided by IPSec are not useful for protocol other than IP and also it doesn't support multicast sessions. RTP is network independent and could use other protocols like ATM/AAL5 for transmission of real-time data for which IPSec won't be viable. Services provided by RTP are quite comprehensive, though it still has failed to provide adequate authentication for wireless networks and the key distribution mechanism. Authentication with SHA may be useful but the key size may be burdensome for wireless networks.

RTP is a flexible protocol and allows new encoding techniques that may provide secure communication that may solve these problems. RTP in conjunction with other protocols can also be used for security purposes that may eventually solve most of the problems.

## REFERENCES

1. Schulzrinne, H., S. Casner, R. Frederick and V. Jacobson, 2003. RTP: A transport protocol for real-time applications, RFC3550, July 2003.
2. Baugher, M., R. Blaom, E. Carrara, D. McGrew, M. Naslund, K. Norman and D. Oran, 2004. Secure Real-time transport protocol: RFC 3711, March 2004.
3. Schulzrinne, H. and S. Casner, 2003. RTP profile for audio and video conferences with minimal control: RFC 3551, July 2003.
4. Stubblebine, S., 1993. Security services for multimedia conferencing. In 16th National Computer Security Conference, (Baltimore, Maryland), pp: 391-395, September, 1993.

5. Bruce, S., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons, Inc., New York, NY, USA, 2nd Edn., 1996.
6. Electronic Frontier Foundation. Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design. O'Reilly and Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA.
7. NIST, Advanced Encryption Standard (AES), FIPS PUB 197, http://www.nist.gov/aes/
8. Bellare, M., A. Desai, E. JokiPii and P. Rogaway, 1997. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation. Proceedings 38th Symp. Found. Computer Science, IEEE, 1997. A revised version is available online at http://www-cse.ucsd.edu/users/mihir.
9. Ville, H., 2004. Real-time transport protocol security, Tik-110.501 Seminar on Network Security HUT TML 2000.
10. Svanbro, K., J. Wiorek and B. Olin, 2000. Voice-over-IP-over-wireless. Proc. PIMRC 2000, London, Sept. 2000.
11. Kent, S. and R. Atkinson, 1998. Security architecture for the internet protocol: RFC 2401, November 1998.
12. ITU-T Standard H.235v2, Security and Encryption for H-series (H.323 and Other H.245 Based) Multimedia Terminals.