CAROLINA TECHNOLOGY CONSULTANTS

Tech Brief

April 2009 *Architectural Issues in IT and Data Communications*

Topic

SRTP – Secure Real-Time Transport Protocol

Prepared By

Tyler R. Johnson

Summary

The Secure Real-time Transport Protocol (SRTP) is an extension of the RTP Audio/Video profile [RFC-3551] that provides encryption, message authentication and protection from replay attacks for RTP/RTCP.

SRTP

---

* Encryption of audio and video.
* Requires key management scheme.
* Guards message privacy.
* Ensures message authenticity.

Discussion

SRTP provides a default cryptographic scheme, but also supports algorithmic extensions, allowing for flexible implementation of new cryptographic transforms in the future.

SRTP protects the payloads of RTP/ RTCP packets, but does not protect the message headers. Message header confidentiality would require transport layer encryption.

The cryptographic algorithms employed in SRTP are designed for low computational cost and low latency, making them ideal for wired and wireless multimedia communication systems. The protocol is also designed for compact implementation so that it works well with embedded systems with limited resources.

SRTP uses both master keys and session keys. A master key is included in encrypted portion of the SRTP packet, and session keys are derived from it. Session keys may be regenerated at fixed rates throughout the communication. Thus, someone decrypting a part of a message would not have access to other parts of the message. If a master key is compromised, all session keys can be generated from it. Therefore, master keys must be kept confidential.

Note that the use of translators or mixers functions as a back to back agent and therefore comprises a man in the middle attack. End to end security in this mode is thus not possible.

SRTP does not specify key management. It suggests that MIKEY, KEYMGT and SDMS may be appropriate key management standards.

Strategy Considerations

SRTP is a reasonable, efficient and standardized method to encrypt media traffic and ensure message integrity for IP multimedia applications. Because it does not encrypt message headers, it may be possible to deduce certain information about a session just by inspecting the headers. SRTP requires a key management scheme to ensure both senders and receivers have access to a master key, which is traditionally a difficult implementation problem for encryption schemes.

For Further Information

1. IETF RFC-3550 *RTP: A Transport Protocol for Real-time Applications*. H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. July 2003.
2. IETF RFC-3551 *RTP Profile for Audio and Video Conferences with Minimal Control*. H. Schulzrinne, S. Casner. July 2003.
3. IETF RFC-3555 *MIME Type Registration of RTP Payload Formats*. S. Casner, P. Hoschka. July 2003.
4. IETF RFC-3711 *The Secure Real-time Transport Protocol (SRTP)*. M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. March 2004
5. IETF RFC-4383 *The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in the Secure Real-time Transport Protocol (SRTP)*. M. Baugher, E. Carrara. February 2006.
6. IETF RFC-4771 Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP). V. Lehtovirta, M. Naslund, K. Norrman. January 2007.