Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 30, 2007

V. Lehtovirta
Ericsson Research NomadicLab

February 26, 2007

Infrastructure aspects to media security
draft-lehtovirta-rtpsec-infra-00

Status of this Memo

Copyright Notice

Abstract

This document discusses some infrastructure aspects that should be considered in the media security requirements work.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

Requirements related to the ongoing media security work are discussed for example in [I-D.wing-media-security-requirements].

This document discusses some infrastructure aspects that should be considered in the media security requirements work.

These aspects are:

- Termination of media security in a gateway
- Using shared keys to provide media security
- Setting up media security with the help of a third party
- Termination of media streams in different devices

3. Termination of media security in a gateway

A typical case of using media security is the one where two entities are having a VoIP conversation over IP capable networks. However, there are cases where the other end of the communication is not connected to an IP capable network. In this kind of setting, there needs to be some kind of gateway at the edge of the IP network which converts the VoIP conversation to format understood by the other network. An example of such gateway is a PSTN gateway sitting at the edge of IP and PSTN networks.

If media security (e.g. SRTP protection) is employed in this kind of gateway-setting, then media security and the related key management needs to be terminated at the gateway. The other network (e.g. PSTN) may have its own measures to protect the communication, but this means that from media security point of view the media security is not employed end-to-end between the communicating entities.

Therefore, media security solutions should cover the cases where media security is not employed end-to-end but is terminated in a gateway.

4. Using shared keys to provide media security

There are environments where the communicating endpoints set up shared keys with the network infrastructure. An example of such environment is the widely deployed GSM system and its 3G successor, the UMTS. It would be beneficial if the shared keys between the endpoints and the network infrastructure in these kind of systems could be re-used to provide shared keys also between the communicating endpoints.

Therefore, it might be justified to consider using shared keys in addition to public keys to provide media security in some environments.

5. Setting up media security with the help of a third party

Setting up a secured connection to an arbitrary peer requires that the communicating entities have in some way agreed on key management credentials, e.g. shared keys or certificates. From scalability point of view it is in practice not feasible to achieve this to an arbitrary peer without the help of some third party providing the credentials.

To enable a scalable solution that allows to set up a secure connection to an arbitrary peer seems to require the help of some third party.

6. Termination of media streams in different devices

In some cases, different media streams might be terminated in different devices. For example, the video part of a multimedia session could terminate in one device, while the audio part would terminate in another device. It should be possible to set up media security efficiently in such scenarios.

7. Security Considerations

None.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[I-D.wing-media-security-requirements] Wing, D., "Media Security Requirements", draft-wing-media-security-requirements-00 (work in progress), October 2006.

Author's Address

Vesa Lehtovirta
Ericsson Research NomadicLab
JORVAS FIN-02420
FINLAND

Phone: +358 9 299 1
Email: vesa.lehtovirta@ericsson.com

Full Copyright Statement

Intellectual Property

on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).