Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 21, 2008

E. Rescorla
Network Resonance

December 19, 2007

Keying Material Extractors for Transport Layer Security (TLS)
draft-ietf-tls-extractor-00.txt

Status of this Memo

Copyright Notice

Abstract

A number of protocols wish to leverage Transport Layer Security (TLS) to perform key establishment but then use some of the keying material for their own purposes. This document describes a general mechanism for allowing that.

Table of Contents

1. Introduction

A number of protocols wish to leverage Transport Layer Security (TLS) [4] or Datagram TLS (DTLS) [5] to perform key establishment but then use some of the keying material for their own purposes. A typical example is DTLS-SRTP [6], which uses DTLS to perform a key exchange and negotiate the SRTP [3] protection suite and then uses the DTLS master_secret to generate the SRTP keys.

These applications imply a need to be able to extract Exported Keying Material (EKM) from TLS/DTLS. This mechanism has the following requirements:

- Both client and server need to be able to extract the same EKM value.
- EKM values should be indistinguishable from random by attackers who don't know the master_secret.
- It should be possible to extract multiple EKM values from the same TLS/DTLS association.
- Knowing one EKM value should not reveal any information about the master_secret or about other EKM values.

The mechanism described in this document is intended to fill these requirements.

2. Conventions Used In This Document

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 [1].

3. Signalling Extractors

Other protocols which wish to use extractors SHOULD have some way for

the peers to signal that an extractor will be used. An example is a TLS extension, as used in DTLS-SRTP.

4. Extractor Definition

An extractor takes as input two values:

- A disambiguating label string
- A length value

It then computes:


```
PRF(master_secret, label,
    SecurityParameters.client_random +
    SecurityParameters.server_random)[length]
```

The output is a pseudorandom bit string of length bytes generated from the master_secret.

Label values MUST be registered via Specification Required as described by RFC 2434 [2]. Note that extractor labels have the potential to collide with existing PRF labels. In order to prevent this, labels SHOULD begin with "EXTRACTOR". This is not a MUST because there are existing uses which have labels which do not begin with this prefix.

5. Security Considerations

Because an extractor produces the same value if applied twice with the same label to the same master_secret, it is critical that two EKM values generated with the same label be used for two different purposes--hence the requirement for IANA registration. However, because extractors depend on the TLS PRF, it is not a threat to the use of an EKM value generated from one label to reveal an EKM value generated from another label.

6. IANA Considerations

IANA is requested to create (has created) a TLS Extractor Label

registry for this purpose. The initial contents of the registry are given below:

Value	Reference
client finished	[RFC4346]
server finished	[RFC4346]
master secret	[RFC4346]
key expansion	[RFC4346]
client EAP encryption	[RFC2716]
ttls keying material	[draft-funk-eap-ttls-v0-01]

Future values are allocated via RFC2434 Specification Required policy. The label is a string consisting of printable ASCII characters. IANA MUST also verify that one label is not a prefix of any other label. For example, labels "key" or "master secretary" are forbidden.

7. Acknowledgments

Thanks to Pasi Eronen for valuable comments and the contents of the IANA section.

8. References

8.1. Normative References

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

[2] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[3] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[4] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[5] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

8.2. Informational References

[6] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)", draft-ietf-avt-dtls-srtp-01 (work in progress), November 2007.

Author's Address

Eric Rescorla
Network Resonance
2064 Edgewood Drive
Palo Alto, CA 94303
USA

Email: ekr@networkresonance.com

Full Copyright Statement

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information 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).