

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

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on June 21, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

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.

Internet-Draft

TLS Extractors

December 2007

Table of Contents

- [1. Introduction](#) [3](#)
- [2. Conventions Used In This Document](#) [3](#)
- [3. Signalling Extractors](#) [3](#)
- [4. Extractor Definition](#) [3](#)
- [5. Security Considerations](#) [4](#)
- [6. IANA Considerations](#) [4](#)
- [7. Acknowledgments](#) [5](#)
- [8. References](#) [5](#)
 - [8.1. Normative References](#) [5](#)
 - [8.2. Informational References](#) [5](#)
- [Author's Address](#) [5](#)
- [Intellectual Property and Copyright Statements](#) [6](#)

[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:

- o Both client and server need to be able to extract the same EKM value.
- o EKM values should be indistinguishable from random by attackers who don't know the `master_secret`.
- o It should be possible to extract multiple EKM values from the same TLS/DTLS association.
- o 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:

- o A disambiguating label string
- o 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

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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).