Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 21, 2010

S. Josefsson
SJD AB

August 20, 2009

Channel Bindings for TLS based on the PRF
draft-josefsson-sasl-tls-cb-02

Status of this Memo

Copyright Notice

Abstract

This document specify how to compute data, "channel bindings", that is cryptographically bound to a specific Transport Layer Security (TLS) session. The intention is to use this data as a name of the secure channel for the purpose of a channel binding. The channel bindings can be used by authentication protocols to avoid tunneling attacks and security layer re-use. The data is derived using the TLS Pseudo-Random Function (PRF).

Table of Contents

1. Introduction

Binding authentication to a specific encrypted session can protect from certain attacks [mitm]. It can also help to improve performance by having peers agree to re-use a secure channel rather than to set up a new.

This document describe how to generate data that can be used by application protocols to bind authentication to a specific TLS [RFC5246] session.

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 [RFC2119].

3. Channel Bindings Syntax

The channel bindings is computed using the TLS Pseudo-Random Function (PRF). The PRF takes three inputs, a secret, a fixed label, and a seed. Here the label will be "EXPORTER Channel Binding". The key will be the master secret in a TLS session. The seed is the concatenation of the client/server random and finished messages as described below. We will use the first 32 octets computed by the PRF.

Using the terminology, conventions and and pseudo-language in TLS [RFC5246] and [I-D.ietf-tls-extractor], the channel bindings is computed as follows:

```
TLS_channel_bindings = PRF(SecurityParameters.master_secret,
                           "EXPORTER Channel Binding",
                           SecurityParameters.client_random +
                           SecurityParameters.server_random +
                           Finished) [0..31]
```

The seed will be the concatenation of the current TLS session's client/server random with the client's TLS Finished message from the first handshake of the connection.

The derived data MUST NOT be used for any other purpose than channel bindings as described in [RFC5056].

4. IANA Considerations

The IANA is requested to allocate a string "EXPORTER Channel Binding" in the TLS Exporter Label registry as per [I-D.ietf-tls-extractor].

The IANA is requested to register this channel binding using the following templates and the process described in [RFC5056].

Subject: Registration of channel binding TLS

Channel binding unique prefix (name): tls-unique-prf

Channel binding type: unique

Channel type: TLS

Published specification (recommended, optional): This document

Channel binding is secret (requires confidentiality protection): no

Description (optional if a specification is given; required if no Published specification is specified): See earlier in this document.

Intended usage: COMMON

Person and email address to contact for further information: simon@josefsson.org

Owner/Change controller name and email address: simon@josefsson.org

Expert reviewer name and contact information:

5. Security Considerations

For the intended use and other important considerations, see [RFC5056].

We claim that by appropriately using a channel binding an application can protect itself from the attacks in [mitm]. To guarantee this property, the derived data is only to be used for the intended purpose.

The security considerations in TLS should be considered. In particular, the TLS master secret must be protected.

6. Acknowledgements

Thanks to Eric Rescorla and Sam Hartman who pointed out a problem with the construct used in earlier versions of this document when TLS server authentication is not used or checked.

7. References

7.1. Normative References

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

[RFC5056] Williams, N., "On the Use of Channel Bindings to Secure Channels", RFC 5056, November 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[I-D.ietf-tls-extractor] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", draft-ietf-tls-extractor-06 (work in progress), July 2009.

7.2. Informative References

[mitm] Asokan, N., Niemi, V., and K. Nyberg, "Man-in-the-Middle in Tunneled Authentication", WWW http://www.saunalahti.fi/~asokan/research/mitm.html.

Author's Address

Simon Josefsson
SJD AB

Email: simon@josefsson.org