On the Use of Channel Bindings to Secure Channels
draft-altman-tls-channel-bindings-01

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/1id-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 16, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2006).
Abstract

This document defines a form of channel bindings for TLS (Transport Layer Security), namely the concatenation of the initial client and server "finished" messages for a TLS connection.

Table of Contents

1. Conventions used in this document .................................. 3
2. Naming TLS Connections ............................................... 4
3. Recommended Application Programming Interfaces .................. 5
4. IANA Considerations ................................................... 6
5. Security Considerations ................................................. 7
6. Normative References ................................................... 8

Authors’ Addresses .......................................................... 9

Intellectual Property and Copyright Statements ......................... 10
1. 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].
2. Naming TLS Connections

Whenever a "name" is needed for a TLS connection such that the "name" is cryptographically bound to the said TLS [RFC4346] connection (its pre-master secret, negotiation, messages, etc...) such a name may be constructed as described below; we term this a "channel binding."

The channel bindings for TLS connections consist of the concatenation of the initial client and server "finished" TLS messages section 7.4.9 [RFC4346] (note: the unencrypted messages). The initial TLS finished messages are the first pair of TLS finished messages exchanged after TLS channel establishment. It is irrelevant whether the TLS channel was established with a previous SessionID section 7.4.1.2 [RFC4346] or not.

Application protocols MAY specify which of the two initial finished messages, or combination of both of them, to use. If this is not specified, the concatenation of the client and the server finished TLS messages are used. (client finished message first.)

The process by which applications perform "channel binding," that is, the process by which applications establish that the channel bindings for a given TLS connection are observed to be the same at both application ends of the TLS connection is not described here.
3. Recommended Application Programming Interfaces

TLS implementations supporting the use of initial TLS finished messages as channel bindings should provide application programming interfaces to enable higher level protocol implementations to obtain the initial TLS finished messages for both the client and server endpoints.

It is acceptable for the API to provide access to the most recent finished messages although doing so will require that the application be aware of TLS renegotiations in order to ensure that the correct set of TLS finished messages are used.
4. IANA Considerations

There are no IANA considerations for this document.
5. Security Considerations

The TLS finished messages section 7.4.9 [RFC4346] are known to both TLS endpoints and can therefore be safely used as a channel binding provided that the higher level protocol binding to the TLS channel provides integrity protection for the TLS finished messages and only communicates the TLS finished messages across the TLS channel that it is binding to.

If there is an active man-in-the-middle attack, the attacker will already possess knowledge of the TLS finished messages for both inbound and outbound TLS channels. Therefore, there is no additional information obtained by the attacker via the use of the TLS finished messages as a channel binding.

The Security Considerations section of "draft-williams-on-channel-binding" applies to this document.
6. Normative References

[I-D.williams-on-channel-binding]
Williams, N., "On the Use of Channel Bindings to Secure Channels", draft-williams-on-channel-binding-00 (work in progress), August 2006.


Authors’ Addresses

Jeffrey Altman
Secure Endpoints Inc.
255 W 94TH ST PHB
NEW YORK, NY  10025
US

Email: jaltman@secure-endpoints.com

Nicolas Williams
Sun Microsystems Inc.
5300 Riata Trace Ct
Austin, TX  78727
US

Email: Nicolas.Williams@sun.com