SASL And Channel Binding
draft-ietf-sasl-channel-bindings-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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 October 11, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

This document specifies the semantics of channel binding for the Simple Authentication and Security Layers (SASL) framework, mechanisms and applications.

Table of Contents

1. Introduction ............................................ 3
   1.1. Conventions used in this document .............. 3
2. Channel Binding Semantics and Negotiation for SASL .... 4
3. IANA Considerations ..................................... 5
4. Security Considerations ................................. 6
5. References ................................................ 7
   5.1. Normative References ............................... 7
   5.2. Informative References ............................. 7
Author’s Address ............................................. 8
1. Introduction

The introduction of the Salted Challenge Response (SCRAM) SASL mechanism [I-D.newman-auth-scram] and GS2 family of SASL mechanisms [I-D.ietf-sasl-gs2] requires the introduction into SASL of an abstract interface to channel binding [RFC5056].

1.1. 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. Channel Binding Semantics and Negotiation for SASL

In order to use SASL [RFC4422] with channel binding the client and server applications MUST provide a channel binding type and channel binding data to the selected SASL mechanism before the first mechanism’s authentication message is produced (client side) or consumed (server side). Channel binding failure MUST cause authentication failure.

Use of channel binding must be negotiable. The client need not use channel binding, and the server may not support the use of channel binding. But because channel binding is all or nothing we need a method for negotiating its used. We accomplish this by using a convention by which the server can indicate whether it supports channel binding in its mechanism list. That is, we overload the mechanism negotiation to obtain channel binding negotiation.

The convention is that the specification for any SASL mechanism that supports channel binding MUST specify two mechanism names: one that indicates server support for channel binding, and one that indicates the opposite. We RECOMMEND the use of a mechanism name suffix, specifically "-PLUS" to indicate server support for channel binding.

A client MUST NOT use channel binding if it lists the server’s mechanisms and does not find a suitable mechanism that supports channel binding in that list. A server MUST NOT advertise mechanism names indicating support for channel binding if the server application or the mechanism implementations do not support channel binding. Conversely, the server MUST advertise mechanism names indicating support for channel binding if the server application and the mechanism implementations do support channel binding.

To prevent downgrade attacks each mechanism that supports channel binding MUST provide downgrade attack detection. To do this the client application MUST provide the name of the selected mechanism, or the server’s entire mechanism list, as an input to the mechanism prior to producing the mechanism’s first authentication message. The mechanism MUST securely indicate to the server whether the client a) chose to use channel binding, b) would have chosen to use channel binding if the server had supported it, c) cannot do channel binding. In the case of (c) the server MUST fail authentication if the server does actually support channel binding.
3. IANA Considerations

This document changes the procedures for registration of SASL mechanism names. Henceforth any SASL mechanism registration MUST indicate a) whether the mechanism supports channel binding, and, if it does, b) two mechanism names and an indication of which name indicates server support for channel binding.
4. Security Considerations

For general security considerations relating to channel bindings see [RFC5056].
5. References

5.1. Normative References


5.2. Informative References


Internet-Draft            SASL Channel Binding                April 2009

Author’s Address

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

Email: Nicolas.Williams@sun.com