XEP-0233: XMPP Server Registration for use with Kerberos V5

Matthew Miller
mailto:linuxwolf@outer-planes.net
xmpp:linuxwolf@outer-planes.net

Peter Saint-Andre
mailto:stpeter@stpeter.im
xmpp:stpeter@jabber.org
https://stpeter.im/

Joe Hildebrand
mailto:jhildebr@cisco.com
xmpp:hildjj@jabber.org

Mili Verma
mailto:mili.verma@isode.com
xmpp:mili.verma@isode.com

2017-03-16
Version 1.0.0

Status	Type	Short Name
Draft	Standards Track	kerberos5

This specification defines the Kerberos principal name of an XMPP server. It also details a method by which a connecting client can determine this Kerberos principal name when authenticating using the "GSSAPI" SASL mechanism.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

The Kerberos Network Authentication Service (V5) is described in RFC 4120 [1]. An application can call the Kerberos library through the Generic Security Services Application Programming Interface (GSS-API) described in RFC 4121 [2] or the proprietary Microsoft Windows Security Service Provider Interface (SSPI).
The Simple Authentication and Security Layer or SASL (RFC 4422 [3]) is a framework for adding authentication support to connection-based protocols. The SASL mechanism used in environments that make use of Kerberos V5 is called "GSSAPI" and is described in RFC 4752 [4]. Note that the RFC 4121 [5] API has a hyphen and the SASL mechanism does not.
Before using the "GSSAPI" SASL mechanism to authenticate to an XMPP server (which is referred to as the "acceptor" in Kerberos terminology), a connecting client needs to obtain a Kerberos ticket from the Key Distribution Centre (KDC). For this the client needs to determine the Kerberos principal name of the XMPP server. This scenario was not addressed in RFC 3920 [6] or RFC 6120 [7].
This specification sets out the rules that must be followed when registering the Kerberos principal name of an XMPP server. It also details how a client can determine the hostname of the XMPP server which can then be used to construct the Kerberos principal name.

2 Client Determination of Hostname

An XMPP client will initiate a connection to the XMPP server.
The XMPP server will communicate its hostname in a child element of the <mechanisms/> element during SASL negotation, as allowed by RFC 6120 [8] (see Section 6.3.5 and the schema for the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace in Appendix A.4).
This child element is <hostname/> qualified by the 'urn:xmpp:domain-based-name:1' namespace. (see Protocol Namespaces regarding issuance of one or more permanent namespaces).
The XML character data of the <hostname/> element specifies the fully-qualified name of the XMPP server. This should be used for constructing the Kerberos principal name and is independent of the usual rules that an XMPP client uses for establishing a network connection to the XMPP server which may use insecure DNS queries (also see RFC 4120 [9]).

[1] RFC 4120: The Kerberos Network Authentication Service (V5) <http://tools.ietf.org/html/rfc4120>.
[2] RFC 4121: The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2 <http://tools.ietf.org/html/rfc4121>.
[3] RFC 4422: Simple Authentication and Security Layer (SASL) <http://tools.ietf.org/html/rfc4422>.
[4] RFC 4752: The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism <http://tools.ietf.org/html/rfc4752>.
[5] RFC 4121: The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2 <http://tools.ietf.org/html/rfc4121>.
[6] RFC 3920: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc3920>.
[7] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[8] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[9] RFC 4120: The Kerberos Network Authentication Service (V5) <http://tools.ietf.org/html/rfc4120>.

3 Kerberos Principal Name in the GSS-API environment

When the XMPP server is implemented using GSS-API, the domain-based service name (RFC 5178 [10], RFC 5179 [11]) is used as the Kerberos principal name. Domain-based service names contain a domain name in addition to a hostname. This allows naming clustered servers after the domain which they service.
The domain-based service name is mapped to the Kerberos principal name following the format specified in RFC 5179 [12] (i.e., "service/hostname/domain@REALM") and setting the values as follows:

- The **service** string MUST be "xmpp".
- The **hostname** string MUST be the hostname of the XMPP server, as provided by the server in the XML character data of the <hostname/> element during SASL negotiation.
- The **domain** string MUST be the canonical name of the service. This is typically communicated by the client in the 'to' address of the initial stream header.
- The **REALM** string SHOULD be determined according to the network policies in effect (usually the domain name, in an uppercase mapping).

4 Kerberos Principal Name in the Microsoft SSPI environment

Microsoft Windows provides the proprietary SSPI to support the "GSSAPI" SASL mechanism. This section describes the Windows equivalent of the domain-based service name for an XMPP server.
In the Microsoft Windows environment, the concept of Service Principal Name (SPN) is used, which is specified in https://msdn.microsoft.com/en-us/library/ms677601%28v=vs.85%29.aspx. This format ("service class/host:port/service name") is similar to the one specified in RFC 5179 [13]. The SPN can be generated by setting the values as follows:

- The **service class** string MUST be "xmpp".
- The **host** string MUST be the hostname of the XMPP server, as provided by the server in the XML character data of the <hostname/> element during SASL negotiation.

[10] RFC 5178: Generic Security Service Application Program Interface (GSS-API) Internationalization and Domain-Based Service Names and Name Type <http://tools.ietf.org/html/rfc5178>.
[11] RFC 5179: Generic Security Service Application Program Interface (GSS-API) Domain-Based Service Names Mapping for the Kerberos V GSS Mechanism <http://tools.ietf.org/html/rfc5179>.
[12] RFC 5179: Generic Security Service Application Program Interface (GSS-API) Domain-Based Service Names Mapping for the Kerberos V GSS Mechanism <http://tools.ietf.org/html/rfc5179>.
[13] RFC 5179: Generic Security Service Application Program Interface (GSS-API) Domain-Based Service Names Mapping for the Kerberos V GSS Mechanism <http://tools.ietf.org/html/rfc5179>.

- The **port** is optional. It can be used to differentiate between multiple XMPP servers on a single host computer and should be omitted if the XMPP server uses the default port of 5222 for accepting client connections.
- The **service name** string MUST be the canonical name of the service. This is typically communicated by the client in the 'to' address of the initial stream header.

5 Interoperability between GSS-API and SSPI

The goal of this section is to help developers of applications so that clients and servers implemented over SSPI can interoperate with servers and clients implemented over GSS-API. Interoperability is achieved by the GSS-API system joining the Windows Active Directory domain or by having a cross-realm trust between the KDCs of the GSS-API and SSPI systems.
The SPN of the SSPI server does not specify a realm. A GSS-API client constucts the Kerberos principal name according to the rules in the GSS-API environment and adds a realm to the Kerberos principal name, but the Kerberos principal name is mapped to the correct XMPP server on SSPI.
When the server uses GSS-API, the SPN for the server needs to be created in the SSPI environment. The SPN constructed by the SSPI client according to the rules in the SSPI environment is then mapped to the correct GSS-API XMPP server.
The domain-based service name of GSS-API does not specify a port, so the port option of the SPN in SSPI should only be used in testing scenarios when both the XMPP client and the XMPP server are implemented using SSPI. The port SHOULD NOT be used in any other scenarios.
So in effect, whether an endpoint uses SSPI or GSS-API does not affect interoperability as long as the port in SSPI is not used.

6 Examples

Consider the example of an XMPP service "example.com" offered by the XMPP server located on the host "auth42.us.example.com", using the default port of 5222 for accepting client connections. When a client connects to the XMPP server, the server communicates its hostname along with supported SASL mechanisms as follows:

Listing 1: Communicating the hostname

```
<mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <mechanism>GSSAPI</mechanism>
  <mechanism>DIGEST-MD5</mechanism>
  <hostname xmlns='urn:xmpp:domain-based-name:1'>auth42.us.example.com
     </hostname>
</mechanisms>
```

To use the "GSSAPI" SASL mechanism, the client needs to determine the Kerberos principal name of the XMPP server, which will be:

- the domain-based service name "xmpp/auth42.us.example.com/example.com@EXAMPLE.COM" if the client is using GSS-API.
- the SPN "xmpp/auth42.us.example.com/example.com" if the client is using SSPI.

7 Security Considerations

The communication of the XMPP server's hostname during SASL negotiation is not known to introduce new security vulnerabilities, as long as it is done after the underlying channel has been secured using Transport Layer Security (TLS; RFC 5246 [14]) as described for XMPP in RFC 6120 [15]. For additional security considerations, refer to RFC 5178 and RFC 5179.

8 IANA Considerations

This document requires no interaction with the Internet Assigned Numbers Authority (IANA) [16].

9 XMPP Registrar Considerations

9.1 Protocol Namespaces

This specification defines the following XML namespace:

- urn:xmpp:domain-based-name:1

Upon advancement of this specification from a status of Experimental to a status of Draft, the XMPP Registrar [17] shall add the foregoing namespace to the registry located at <https://xmpp.org/registrar/namespaces.html>, as described in Section 4 of XMPP Registrar Function (XEP-0053) [18].

[14] RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2 <http://tools.ietf.org/html/rfc5246>.
[15] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[16] The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.
[17] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.
[18] XEP-0053: XMPP Registrar Function <https://xmpp.org/extensions/xep-0053.html>.

9.2 Protocol Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

10 XML Schema

```
<?xml version='1.0' encoding='UTF-8'?>

<xs:schema
    xmlns:xs='http://www.w3.org/2001/XMLSchema'
    targetNamespace='urn:xmpp:domain-based-name:1'
    xmlns='urn:xmpp:domain-based-name:1'
    elementFormDefault='qualified'>

  <xs:annotation>
    <xs:documentation>
      The protocol documented by this schema is defined in
      XEP-0233: http://www.xmpp.org/extensions/xep-0233.html
    </xs:documentation>
  </xs:annotation>

  <xs:element name='hostname' type='xs:string'/>

</xs:schema>
```

11 Acknowledgements

Thanks to Owen Friel, Shane Hannon, Seamus Kerrigan, Eliot Lear, Alexey Melnikov, Klaas Wierenga, and Dave Cridland for their comments.