INTERNET-DRAFT
Updates: 2246, 4346 (once approved)
Intended Category: Standards track
Expires October 2006
April 2006

S. Santesson (Microsoft)
A. Medvinsky (Microsoft)
J. Ball (Microsoft)

TLS User Mapping Extension
<draft-santesson-tls-ume-06.txt>

Status of this Memo

Abstract

This document specifies a TLS extension that enables clients to send generic user mapping hints in a supplemental data handshake message defined in RFC TBD. One such mapping hint is defined, the UpnDomainHint, which may be used by a server to locate a user in a directory database. Other mapping hints may be defined in other documents in the future.

(NOTE TO RFC EDITOR: Replace "RFC TBD" with the RFC number assigned to draft-santesson-tls-supp-00.txt)

Table of Contents

1. Introduction

This specification defines a TLS extension and a payload for the SupplementalData handshake message, defined in RFC TBD [N6], to accommodate mapping of users to their user accounts when using TLS client authentication as the authentication method.

This specification specifies one new user mapping hint type, providing means to send Domain Name hints and User Principal Name hints. Other hint types may be defined in other documents in the future.

The User Principal Name (UPN) represents a name which specifies a user's entry in a directory in the form of userName@domainName. Traditionally Microsoft has relied on such name form to be present in the client certificate when logging on to a domain account. This has however several drawbacks since it prevents the use of certificates with an absent UPN and also requires re-issuance of certificates or issuance of multiple certificates to reflect account changes or creation of new accounts. The TLS extension in combination with the defined hint type provide a significant improvement to this situation as it allows a single certificate to be mapped to one or more accounts of the user and does not require the certificate to contain a UPN.

The new TLS extension (user_mapping) is sent in the client hello message. Per convention defined in RFC 4366 [N4], the server places the same extension (user_mapping) in the server hello message, to inform the client that the server understands this extension. If the server does not understand the extension, it will respond with a server hello omitting this extension and the client will proceed as normal, ignoring the extension, and not include the UserMappingDataList data in the TLS handshake.

If the new extension is understood, the client will inject UserMappingDataList data in the SupplementalData handshake message prior to the Client's Certificate message. The server will then parse this message, extracting the client's domain, and store it in the context for use when mapping the certificate to the user's directory account.

No other modifications to the protocol are required. The messages are detailed in the following sections.

1.1 Terminology

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 RFC 2119 [N1].

The syntax for the TLS User Mapping extension is defined using the TLS Presentation Language, which is specified in Section 4 of [N2].

1.2 Design considerations

The reason the mapping data itself is not placed in the extension portion of the client hello is to prevent broadcasting this information to servers that don't understand the extension.

2 User mapping extension

A new extension type (user_mapping(TBD)) is added to the Extension used in both the client hello and server hello messages. The extension type is specified as follows.

```
enum {
     user_mapping(TBD), (65535)
} ExtensionType;
```

The "extension_data" field of this extension SHALL contain "UserMappingTypeList" with a list of supported hint types where:

```
struct {
      UserMappingType user_mapping_types<1..2^8-1>
} UserMappingTypeList;
```

Enumeration of hint types (user_mapping_types) defined in this document is provided in section 3.

The list of user_mapping_types included in a client hello SHALL signal the hint types supported by the client. The list of user_mapping_types included in the server hello SHALL signal the hint types preferred by the server.

If none of the hint types listed by the client is supported by the server, the server SHALL omit the user_mapping extension in the server hello.

When the user_mapping extension is included in the server hello, the list of hint types in "UserMappingTypeList" SHALL be either equal to, or a subset of, the list provided by the client.

3 User mapping handshake exchange

The underlying structure of the SupplementalData handshake message, used to carry information defined in this section, is defined in RFC TBD [N6].

A new SupplementalDataType [N6] is defined to accommodate communication of generic user mapping data. See RFC 2246 (TLS 1.0) [N2] and RFC 4346 (TLS 1.1) [N3] for other handshake types.

The information in this data type carries one or more unauthenticated hints, UserMappingDataList, inserted by the client side. Upon receipt and successful completion of the TLS handshake, the server MAY use this hint to locate the user's account from which user information and credentials MAY be retrieved to support authentication based on the client certificate.

The hint defined in this specification (upn_domain_hint) specifies two fields, user_principal_name and domain_name. The domain_name field MAY be used when only domain information is needed, e.g. where a user have accounts in multiple domains using the same username name, where that user name is known from another source (e.g. from the client certificate). When the user name is also needed, the user_principal_name field MAY be used to indicate both username and domain name. If both fields are present, then the server can make use of whichever one it chooses.

```
   struct {
         SupplementalDataType supp_data_type;
         select(SupplementalDataType) {
            case user_mapping_data: UserMappingDataList;
            }
   } SupplementalDataEntry;
```

```
      enum {
            user_mapping_data(TBD), (65535)
      } SupplementalDataType;
```

The user_mapping_data(TBD) enumeration results in a new supplemental data type UserMappingDataList with the following structure:

```
      enum {
             upn_domain_hint(0), (255)
      } UserMappingType;

      struct {
             opaque user_principal_name<0..2^16-1>;
             opaque domain_name<0..2^16-1>;
      } UpnDomainHint;

      struct {
             UserMappingType user_mapping_version
             select(UserMappingType) {
                   case upn_domain_hint:
                        UpnDomainHint;
             }
      } UserMappingData;

      struct{
         UserMappingData user_mapping_data_list<1..2^16-1>;
      }UserMappingDataList;
```

The user_principal_name field, when specified, SHALL be of the form "user@domain", where "user" is a UTF-8 encoded Unicode string that does not contain the "@" character, and "domain" is a domain name meeting the requirements in the following paragraph.

The domain_name field, when specified, SHALL contain a domain name in the usual text form: in other words, a sequence of one or more domain labels separated by ".", each domain label starting and ending with an alphanumeric character and possibly also containing "-" characters. This field is an "IDN-unaware domain name slot" as defined in RFC 3490 [N7] and therefore, domain names containing non-ASCII characters have to be processed as described in RFC 3490 before being stored in this field.

The UpnDomainHint MUST at least contain a non empty user_principal_name or a non empty domain_name. The UpnDomainHint MAY contain both user_principal_name and domain_name.

The UserMappingData structure contains a single mapping of type UserMappingType. This structure can be leveraged to define new types of user mapping hints in the future. The UserMappingDataList MAY carry multiple hints; it is defined as a vector of UserMappingData structures.

No preference is given to the order in which hints are specified in this vector. If the client sends more then one hint then the Server SHOULD use the applicable mapping supported by the server.

4 Message flow

In order to negotiate to send user mapping data to a server in accordance with this specification, clients MUST include an extension of type "user_mapping" in the (extended) client hello, which SHALL contain a list of supported hint types.

Servers that receive an extended client hello containing a "user_mapping" extension, MAY indicate that they are willing to accept user mapping data by including an extension of type "user_mapping" in the (extended) server hello, which SHALL contain a list of preferred hint types.

After negotiation of the use of user mapping has been successfully completed (by exchanging hello messages including "user_mapping" extensions), clients MAY send a "SupplementalData" message containing the "UserMappingDataList" before the "Certificate" message. The message flow is illustrated in Fig. 1 below.

```
Client                                               Server

ClientHello
 /* with user_mapping ext */ -------->

                                                ServerHello
                                /* with user-mapping ext */
                                               Certificate*
                                         ServerKeyExchange*
                                        CertificateRequest*
                             <--------      ServerHelloDone

SupplementalData
 /* with UserMappingDataList */
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                     -------->
                                         [ChangeCipherSpec]
                             <--------             Finished
Application Data             <------->     Application Data
```

Fig. 1 - Message flow with user mapping data

* Indicates optional or situation-dependent messages that are not always sent according to RFC 2246 [N2] and RFC 4346 [N3].

The server MUST expect and gracefully handle the case where the

client chooses to not send any supplementalData handshake message even after successful negotiation of extensions. The client MAY at its own discretion decide that the user mapping hint it initially intended to send no longer is relevant for this session. One such reason could be that the server certificate fails to meet certain requirements.

5 Security Considerations

The user mapping hint sent in the UserMappingDataList is unauthenticated data that MUST NOT be treated as a trusted identifier. Authentication of the user represented by that user mapping hint MUST rely solely on validation of the client certificate. One way to do this is to use the user mapping hint to locate and extract a certificate of the claimed user from the trusted directory and subsequently match this certificate against the validated client certificate from the TLS handshake.

As the client is the initiator of this TLS extension, it needs to determine when it is appropriate to send the User Mapping Information. It may not be prudent to broadcast this information to just any server at any time, as it can reveal network infrastructure the client and server are using.

To avoid superfluously sending this information, clients SHOULD only send this information if the server belongs to a domain to which the client intends to authenticate using the UPN as identifier.

In some cases, the user mapping hint may itself be regarded as sensitive. In such case the double handshake technique described in [N6] can be used to provide protection for the user mapping hint information.

6 References

Normative references:

[N1] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[N2] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[N3] T. Dierks, E. Rescorla, "The TLS Protocol Version 1.1", RFC 4346, January 2006.

[N4] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, February 2006.

[N5] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[N6] S. Santesson, "TLS Handshake Message for Supplementary Data", RFC TBD (currently: draft-santesson-tls-supp-02, Date 2006.

[N7] P. Faltstrom, P. Hoffman, A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003

[N8] T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, October 1998

7 IANA Considerations

IANA needs to take the following actions:

1) Create an entry, user_mapping(TBD), in the existing registry for ExtensionType (defined in RFC 4366 [N4]).

2) Create an entry, user_mapping_data(TBD), in the new registry for SupplementalDataType (defined in draft-santesson-tls-supp-02).

3) Establish a registry for TLS UserMappingType values. The first entry in the registry is upn_domain_hint(0). TLS UserMappingType values in the inclusive range 0-63 (decimal) are assigned via RFC 2434 [N8] Standards Action. Values from the inclusive range 64-223 (decimal) are assigned via RFC 2434 Specification Required. Values from the inclusive range 224-255 (decimal) are reserved for RFC 2434 Private Use.

Authors' Addresses

Stefan Santesson
Microsoft
Finlandsgatan 30
164 93 KISTA
Sweden

EMail: stefans(at)microsoft.com

Ari Medvinsky
Microsoft
One Microsoft Way
Redmond, WA 98052-6399
USA

Email: arimed(at)microsoft.com

Joshua Ball
Microsoft
One Microsoft Way
Redmond, WA 98052-6399
USA

Email: joshball(at)microsoft.com

Acknowledgements

The authors extend a special thanks to Russ Housley, Eric Resocorla and Paul Leach for their substantial contributions.

Disclaimer

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 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.

Copyright Statement