Transport Layer Security Working Group J.Banes
Internet Draft C.Crall
Document: draft-ietf-tls-emailaddr-00.txt Microsoft
Expires: March 2004 September 2003

Update to Transport Layer Security (TLS) Extensions

Status of this Memo

Copyright Notice

Abstract

This document is an update to the Transport Layer Security (TLS) Extensions. This update provides an additional choice in the ServerName type of the Server_Name extension. The Server Name extension allows the client to specify the name of the server to which it is attempting to connect. The new choice specified in this document allows the client to specify an email name as the server name.

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 RFC-2119 [KEYWORDS][KEYWORDS].

Table of Contents

draft-ietf-tls-emailaddr-00.txt September 2003

1. Introduction

RFC 3546 [TLSEXT]provides a set of extensions to the Transport Layer Security (TLS) protocol. One of these extensions is the Server Name extension. The Server Name extension provides a mechanism for the client to specify the name of the server to which it is connecting. This extension is provided as part of the client hello message. RFC 3546 defines one Server Name type, ôhostnameö. This draft adds a second Server Name type, ôemailaddrö.

2. EmailAddr ServerName Indication

RFC 3546 defines a Server Name Indication as a mechanism for a client to tell a server the name of the server that it is contacting. The Server Name Indication information is helpful when a single server may be acting as multiple virtual servers.

RFC 3546 defines the structure shown below which is part of the extended client hello message.

```
struct {
    NameType name_type;
    select (name_type) {
        case host_name: HostName;
    } name;
} ServerName;

enum {
    host_name(0), (255)
} NameType;

opaque HostName<1..2^16-1>;
```

```
struct {
    ServerName server_name_list<1..2^16-1>
} ServerNameList;
```


This draft proposes a new NameType be added, ôemail_addrö. As with host_name, email_addr is used to identify the appropriate virtual server and therefore help the server select the appropriate certificate to return to the client. Therefore, the new structure looks like the following:

```
struct {
    NameType name_type;
    select (name_type) {
        case host_name: HostName;
        case email_name: EmailName;
    } name;
} ServerName;

enum {
    host_name(0), email_name(1),(255)
} NameType;

opaque HostName<1..2^16-1>;

opaque EmailName<1..2^16-1>;

struct {
    ServerName server_name_list<1..2^16-1>
} ServerNameList;
```

The syntax of EmailName MUST conform to email addresses as defined in RFC 822 [RFC822].

3. Error Alerts

The new alert, ôunrecognized_nameö defined in RFC 3546 should be returned by the server when the server name is unrecognized, whether the name is a HostName or an EmailName. As stated in RFC 3546, this error may be fatal.

4. Security Considerations

The security considerations for the new EmailName are similar to those of the HostName in RFC 3546.

The server receiving an extended client hello message with an EmailName MUST ensure the name does not cause a buffer overflow within the server.

The EmailName supports internationalized hostnames. However, this specification does not deal with security issues of internationalized names.

5. Acknowledgments

The authors wish to thank the authors of RFC 3546 for their help.

6. AuthorsÆ Addresses

John Banes
Microsoft
Email: jbanes@microsoft.com

Chris Crall
Microsoft
Email: ccrall@microsoft.com

7. Normative References

[KEYWORDS] Bradner, S., ôKey words for use in RFCs to Indicate Requirement Levelsö, BCP 14, RFC 2119, March 1997

[RFC822] Crocker, D., ôStandard for the Format of ARPA Internet Text Messagesö, RFC 822, August 1982

[TLSEXT] Blake-Wilson, S., Nystrom, M., Hopwwod, D., Mikkelsen, J. and Wright, T., ôTransport Layer Security (TLS) Extensionsö, RFC

3546, June 2003