Network Working Group M. Miller
Internet-Draft P. Saint-Andre
Intended status: Standards Track Cisco Systems, Inc.
Expires: January 14, 2013 July 13, 2012

Using PKIX over Secure HTTP (POSH) as a Prooftype for XMPP Domain Name Associations
draft-miller-xmpp-posh-prooftype-01

Abstract

This document defines a prooftype involving PKIX over Secure HTTP (POSH) for associating a domain name with an XML stream in the Extensible Messaging and Presence Protocol (XMPP). It also defines a method involving HTTPS redirects (appropriate for use with the POSH prooftype) for securely delegating a source domain to a derived domain in XMPP.

Table of Contents

1. Introduction

The [XMPP-DNA] specification defines a framework for secure delegation and authenticated domain name associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP). This document defines a prooftype for DNA, using PKIX certificates obtained over secure HTTP ("POSH"), as well as a secure delegation method, based on HTTPS redirects, that is appropriate for use with the POSH prooftype.

The rationale for POSH is driven by current operational realities. It is effectively impossible for a hosting service to provide and maintain PKIX certificates [RFC5280] that include the appropriate [RFC6125] identifiers for each hosted domain. It is true that DNS-based technologies are emerging for secure delegation, in the form of DNS Security [RFC4033] and [DANE]); however, these technologies are not yet widely deployed and might not be deployed in the near future for domains outside the most common top-level domains (e.g., ".COM", ".NET", ".EDU"). Because the XMPP community wishes to deploy secure delegation and authenticated domain name associations as widely and as quickly as possible, this document specifies how to use secure HTTP [RFC2616] and PKIX certificates [RFC5280] to verify that a domain is delegated to a hosting provider and authenticate an assocation between a domain name and an XML stream.

2. Terminology

This document inherits XMPP-related terminology from [RFC6120] and security-related terminology from [RFC5280]. The terms "source domain", "derived domain", "reference identifier", and "presented identifier" are used as defined in the "CertID" specification [RFC6125].

This document is applicable to connections made from an XMPP client to an XMPP server ("_xmpp-client._tcp") or between XMPP servers ("_xmpp-server._tcp"). In both cases, the XMPP initiating entity acts as a TLS client and the XMPP receiving entity acts as a TLS server. Therefore, to simplify discussion this document uses "_xmpp-client._tcp" to describe both cases, unless otherwise indicated.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Prooftype

POSH stands for PKIX Over Secure HTTP: the verification materials consist of a PKIX certificate [RFC5280], they are obtained by retrieving the certificate over HTTPS [RFC2818] from a well-known URI [RFC5785], the certificate is checked according to the rules from [RFC6120] and [RFC6125], and secure DNS is not necessary since the HTTPS retrieval mechanism relies on the chain of trust based on the public key infrastructure.

The process for retrieving a PKIX certificate over secure HTTP is as follows.

1. The initiating entity performs an HTTPS GET at the source domain to the path "/.well-known/posh._<service>._tcp.cer"; where "_<service>" MUST be either "_xmpp-client" for XMPP client-to-server connections or "_xmpp-server" for XMPP server-to-server connections:

```
HTTP GET /.well-known/posh._xmpp-server._tcp.cer HTTP/1.1
Host: im.example.com
```

2. If the source domain HTTPS server has a certificate for the requested path, it MUST respond with a success status code, with the message body as the DER certificate (optionally encoded as base64 [RFC4684]) that the XMPP server at the source domain will present during the TLS negotiation phase of XMPP stream setup:

```
HTTP/1.1 200 OK
Content-Type: application/pkix-cert
Content-Length: 839
```


```
-----BEGIN CERTIFICATE-----
MIICPTCCAaYCCQDDVeBaBmWC/jANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJV
UzERMA8GA1UECBMIQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEXMBUGA1UEChMO
aW0uZXhhbXBsZS5jb20xFzAVBgNVBAMTDmltLmV4YW1wbGUuY29tMB4XDTEyMDYx
MTIxNTQ0NFoXDTIyMDYwOTIxNTQ0NFowYzELMAkGA1UEBhMCVVMxETAPBgNVBAgT
CENvbG9yYWRvMQ8wDQYDVQQHEwZEZW52ZXIxFzAVBgNVBAoTDmltLmV4YW1wbGUu
Y29tMRcwFQYDVQQDEw5pbS5leGFtcGxlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA4hoKhi/B07eQH+1NB9gWiNFDT//AbTHQOEC0AOr4Gh/o9PUp7kD0
gklU4uv7rSAhAyCe4WaOiQ/HShzEryGfHiZmWht0BaYmj19iuPWRecZOXWqKZji9
NtAxn9l3kdon/YLJcrPGyNTGK66+ggNaqy8LkQQpI4rff60yHHZ/0XkCAwEAATAN
BgkqhkiG9w0BAQUFAAOBgQDcwiu30bSMlykWYz+tTDSlQ3wLSVB9RsR8jXmJvMo7
y7icXwg54a9M3xipjZtrfAhYM5I5iqUTQPki6s26n9SQpRm5bonEFDA3WGwrwma3
5biP9+NSBWzSaDF8AztwFNKXXl6/U6hWwG05G/NdeS11gpww9NUDraJgVoDpRK04
tg==
-----END CERTIFICATE-----
```

4. Secure Delegation

When PKIX Over Secure HTTP (POSH) is the DNA prooftype, it is possible to use HTTPS redirects in determining if a domain is securely delegated, as follows:

1. The initiating entity performs an HTTPS GET at the source domain to the path "/.well-known/posh._<service>._tcp.cer"; where "_<service>" MUST be either "_xmpp-client" for XMPP client-to-server connections or "_xmpp-server" for XMPP server-to-server connections. Here is an example:

```
GET /.well-known/posh._xmpp-server._tcp.cer HTTP/1.1
Host: im.example.com
```

2. If the source domain HTTPS server has delegated to a derived domain, it MUST respond with one of the redirect mechanisms provided by HTTP (e.g., using the 302, 303, or 307 response). The 'Location' header MUST specify an HTTPS URL, where the hostname and port is the derived domain HTTPS server, and the path MUST match the pattern "_<service>._tcp.cer"; where "_<service>" MUST be identical to the "_<service>" portion of the original request (line breaks added for readability):

```
HTTP/1.1 302 Found
Location: https://hosting.example.net/.well-known
          /posh._xmpp-server._tcp.cer
```

3. The initiating entity performs an HTTPS GET to the URL specified in the 'Location' header:

```
GET /.well-known/posh._xmpp-server._tcp.cer HTTP/1.1
Host: hosting.example.net
```

4. If the derived domain HTTPS server has a certificate, it MUST respond with a success status code, with the message body as the DER certificate (optionally encoded as base64 [RFC4684]) that the XMPP server at the derived domain will present during the TLS negotiation phase of XMPP stream setup:

```
HTTP/1.1 200 OK
Content-Type: application/pkix-cert
Content-Length: 863
```


```
-----BEGIN CERTIFICATE-----
MIICUTCCAboCCQCtNQRNu3194zANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJV
UzERMA8GA1UECBMIQ29sb3JhZG8xDzANBgNVBAcTBkRlbnZlcjEcMBoGA1UEChMT
aG9zdGluZy5leGFtcGxlLm5ldDEcMBoGA1UEAxMTaG9zdGluZy5leGFtcGxlLm5l
dDAeFw0xMjA2MTEyMTQ1MjZaFw0yMjA2MDkyMTQ1MjZaMG0xCzAJBgNVBAYTAlVT
MREwDwYDVQQIEwhDb2xvcmFkbzEPMA0GA1UEBxMGRGVudmVyMRwwGgYDVQQKExNo
b3N0aW5nLmV4YW1wbGUubmV0MRwwGgYDVQQDExNob3N0aW5nLmV4YW1wbGUubmV0
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDi46kMWnCfg0DTrlcTc6AQUci5
Lu1f2RKRWPEhz8qyt/CO0N5VpxKQMlGp6TApQzFdAfxCUA3rniYFpMq4Hemw2S74
v1LRoWvROKviKRzunDP3EhPXf6GbgnHRlfBx4yvZtcR1BMnkxgJtbTAJu4/wTRXY
RE5FKk3xT4IBXTIQFwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAvRohCXSfSnHXjv
84beqmFSYKcZvhVymgxQfhB2ZLNFQvfTO3Qsp/MR0hRRXrJ25n86t49EEXicjC0r
EdmWaIhdDFhw7hva2byYziww7fJuelD0tpL9nfF5uOIMp3JYyXCBn/FKJhi9HMR1
d8avm8gJ5Iu7L96qosWzL3epHYW7
-----END CERTIFICATE-----
```


5. Caching Results

Ideally, the initiating entity relies on the expiration time of the certificate obtained via POSH, and not on HTTP caching mechanisms. To that end, the HTTPS servers for source and derived domains SHOULD specify a 'Cache-Control' header indicating a short duration (e.g., max-age=60) or "no-cache" to indicate the response (redirect or content) is not appropriate to cache at the HTTP level.

6. Examples

Detailed examples will be provided in a future version of this specification.

7. Security Considerations

This document supplements but does not supersede the security considerations provided in [RFC2616], [RFC2818], [RFC6120], and [RFC6125].

Specifically, communication via HTTPS depends on checking the identity of the HTTP server in accordance with [RFC2818].

8. IANA Considerations

8.1. The "posh._xmpp-client._tcp.cer" Well-Known URI

This specification registers the "posh._xmpp-client._tcp.cer" well-known URI in the Well-Known URI Registry as defined by [RFC5785].

URI suffix: posh._xmpp-client._tcp.cer

Change controller: IETF

Specification document(s): RFCXXXX.

8.2. The "posh._xmpp-server._tcp.cer" Well-Known URI

This specification registers the "posh._xmpp-server._tcp.cer" well-known URI in the Well-Known URI Registry as defined by [RFC5785].

URI suffix: posh._xmpp-server._tcp.cer

Change controller: IETF

Specification document(s): RFCXXXX.

9. References

9.1. Normative References

[XMPP-DNA]
Saint-Andre, P. and M. Miller, "Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)", draft-saintandre-xmpp-dna-00 (work in progress), June 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC4684] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S.,

Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, April 2010.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

9.2. Informative References

[DANE] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", draft-ietf-dane-protocol-23 (work in progress), June 2012.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, May 2005.

Authors' Addresses

Matthew Miller
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
USA

Email: mamille2@cisco.com

Peter Saint-Andre
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
USA

Email: psaintan@cisco.com