Network Working Group   P. Saint-Andre
Internet-Draft   M. Miller
Intended status: Standards Track   Cisco Systems, Inc.
Expires: December 29, 2012   June 27, 2012

Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)

draft-saintandre-xmpp-dna-00

Abstract

This document defines a framework for improving the security of the Extensible Messaging and Presence Protocol (XMPP) in two respects. First, it introduces the concept of a prooftype for establishing a strong association between a domain name and an XML stream. Second, it provides guidelines for securely delegating a source domain to a derived domain, which is especially important in virtual hosting environments.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 29, 2012.

Table of Contents

1. Introduction

This document defines a framework for improving the security of the Extensible Messaging and Presence Protocol (XMPP) in two respects. First, it introduces the concept of a prooftype for establishing a strong association between a domain name and an XML stream (i.e., a domain name association or "DNA"). Second, it provides guidelines for securely delegating a source domain to a derived domain, which is especially important in virtual hosting environments.

The need to establish a strong association between a domain name and an XML stream arises in both client-to-server and server-to-server communication using XMPP, because XMPP servers are typically identified by domain names. However, a client or peer server needs to verify the identity of a server to which it connects. To date, such verification has been established based on information obtained from the Domain Name System (DNS), the Public Key Infrastructure (PKI), or similar sources. This document generalizes the model currently in use so that additional prooftypes can be defined, and also provides a basis for modernizing some prooftypes (e.g., Server Dialback [XEP-0220]) to reflect progress in several underlying technologies, especially DNS Security [RFC4033].

The process for resolving the domain name of an XMPP service into the IP address at which an XML stream will be negotiated (defined in [RFC6120]) can involve delegation of a source domain (say, im.example.com) to a derived domain (say, hosting.example.net). If such delegation is not done in a secure manner, then the domain name association cannot be authenticated. Therefore, this document also provides guidelines for defining secure delegation methods.

This document does not define any DNA prooftypes or secure delegation methods; such technologies are defined in companion documents.

2. Terminology

This document inherits XMPP-related terminology from [RFC6120] and [XEP-0220], DNS-related terminology from [RFC1034], [RFC1035], [RFC2782] and [RFC4033], and security-related terminology from [RFC4949] and [RFC5280]. The terms "source domain", "derived domain", "reference identity", and "presented identity" are used as defined in the "CertID" specification [RFC6125]. The terms "permissive federation", "verified federation", and "encrypted federation" are derived from [XEP-0238], although we substitute the term "authenticated federation" for the term "trusted federation" from that document.

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. Problem Statement

In XMPP, each party to a stream expects the other party to provide some proof of its identity. For example, in client-to-server streams the server expects the client to present some credentials (such as a username and password or a client certificate), and ideally the client also expects the server to provide a certificate that identifies the domain(s) of the server. Similar considerations hold true for server-to-server streams, also called "interdomain federation".

When the Jabber.org open-source community developed the precursor to XMPP in 1999, it defined methods for interdomain federation but no mechanisms for authenticating or checking the identity of peer servers. We could describe this as "permissive federation", which is clearly sub-optimal given the strong potential for domain spoofing. In the year 2000, the community filled the gap to some extent by defining a technology called Server Dialback (first documented in [RFC3920] and since moved to [XEP-0220]). Although Server Dialback does not provide a strong mechanism for identity checking without the use of DNSSEC, it does provide DNS-based verification and thus has effectively prevented most instances of domain spoofing on the XMPP network since late 2000. Also, because Server Dialback typically does not involve the use of server certificates, it does not result in an encrypted stream; thus we refer to it as a technology for "verified federation".

In 2002-2004, the IETF's XMPP Working Group hardened the original Jabber.org protocols by adding Transport Layer Security (TLS) and Simple Authentication and Security Layer (SASL), thus making it possible for two servers to engage in "authenticated federation" (i.e., when two peer servers present PKIX certificates anchored to trusted roots during negotiation of a server-to-server stream) or "encrypted federation" (i.e., when two peer servers present PKIX certificates that are self-signed or not anchored to trusted roots during negotiation of a server-to-server stream).

Unfortunately, authenticated federation has not been widely deployed on the XMPP network (indeed, even encrypted federation is not widely deployed because verified federation is perceived as "good enough"); one of the primary reasons is that it is feasible (although not always easy) for single-domain servers to obtain the proper

certificates, but much more difficult (or practically impossible) for large XMPP hosting providers to do so. The primary challenge here is operational: it is highly unlikely that an organization (say, example.com) wishing to delegate its XMPP service (say, im.example.com) to a hosting provider (say, hosting.example.net) will hand over its private key to the hosting provider. Even if that were feasible, further operational challenges (e.g., maintaining large numbers of certificates for hosted domains, and configuring XMPP software to present the correct certificate based on the 'to' address of the initial stream header) have also discouraged deployment of authenticated federation in virtual hosting environments, which happen to be a common deployment scenario.

Furthermore, the prevalence of delegation to hosting providers leads to one additional shortcoming, caused by the use of DNS SRV records [RFC2782] in XMPP: if DNSSEC is not used, the act of delegation is inherently insecure. Unfortunately, no existing documentation explains how to use DNSSEC for secure delegation, with the result that clients and servers often take a "leap of faith" if using an SRV record to determine that when communicating with, say, im.example.com they actually need to connect to, say, hosting.example.net.

In order to meet the requirements for strong security [RFC3365], both authenticated federation and secure delegation are needed so that the association between a domain name and an XML stream can be trusted by XMPP entities. Unfortunately, authenticated federation is uncommon and secure delegation is unheard of on the XMPP network today. Because the current situation is clearly sub-optimal, this document defines a framework for both authenticated federation and secure delegation in XMPP.

4. Framework

In essence, we need to establish an association between a domain and an XML stream: is the XMPP server to which a client or peer server connects "allowed" to accept stanzas for or send stanzas from a given domain? If so, we say that there is a domain name association ("DNA") for the stream.

For TLS in general, the TLS client has some expectations about the identity of the TLS server (in the language of the "CertID" specification [RFC6125], the TLS client has a "reference identity"), and then checks some material presented by the TLS server (the "presented identity" within the server certificate) to verify that its expectations have been met. In XMPP, Server Dialback follows a similar model, except that the verification material takes the form of a token instead of a certificate. The DNS-Based Authentication of

Named Entities protocol [DANE], at least in some of its modes, adds another kind of verification material: not the presented identity within a PKIX certificate, but a complete certificate or hash thereof. And other kinds of verification material could be envisioned (e.g., OpenPGP keys, Kerberos tickets, OAuth tokens), although they are not considered here.

No matter what kind of verification material is used, an XMPP client or peer server that wishes to verify a domain name association needs a way to obtain the verification material it will refer to when establishing the association. For instance, when a server presents a PKIX certificate during TLS negotiation, the connecting client or peer server has traditionally obtained its verification material out of band or via configuration from a certification authority (i.e., in the form of a root certificate contained in a certificate bundle). In the Server Dialback protocol, the verification material is a token that is obtained over XMPP itself. In DANE, the verification material is obtained from the Domain Name System. In the PKIX Over Secure HTTP ("POSH") method described in an accompanying specification, the verification material is obtained over secure HTTP. And other methods for obtaining verification material could be envisioned (e.g., IPsec), although they are not considered here.

Furthermore, the matching rules for checking the verification material will depend on the nature of that material; for example, [RFC6120] defines a profile of the rules from the "CertID" specification [RFC6125], Server Dialback [XEP-0220] typically performs a character-for-character comparison of tokens, DANE might compare the SubjectPublicKeyInfo data or the full certificate, and so on.

Finally, given the relationship between XMPP and the DNS (XMPP services are usually identified by domain name, not IP address), it is important to make it clear whether a given verification method can (or must) be used only with secure DNS or also with insecure DNS.

Putting these pieces together, we define a "DNA prooftype" as follows.

prooftype: A mechanism for proving an association between a domain name and an XML stream, where the mechanism defines (1) the verification material to be used, (2) the matching rules for comparing the reference version and presented version of the material, (3) how the verification material is obtained, and (4) whether the mechanism depends on secure DNS.

The following sections outline several prooftypes that are used, or could be used, in XMPP; detailed definitions are provided in separate

specifications.

Note: So far, our definition of a prooftype does not include the exact protocol mechanism that is used to assert a domain name; this is explained further under Section 6.

5. Prooftypes

5.1. PKI

The PKI prooftype is a DNA proof that follows the rules from [RFC6120]: that is, the verification materials consist of a PKIX certificate that is checked according to a profile of the matching rules from [RFC6125], the client's verification materials are obtained out of band in the form of a trusted root, and secure DNS is not necessary.

5.2. DANE

In the DANE prooftype, the verification materials consist of a PKIX certificate that is compared as an exact match or a hash of either the SubjectPublicKeyInfo or the full certificate, and the verification materials are obtained via secure DNS. See the accompanying [XMPP-DANE] spec for complete discussion and examples.

5.3. POSH

POSH stands for PKIX Over Secure HTTP: the verification materials consist of a PKIX certificate, it is obtained by retrieving it over HTTPS at 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 from the public key infrastructure. See the accompanying [XMPP-POSH] spec for complete discussion and examples.

5.4. Dialback Keys

The Dialback Keys prooftype formalizes the existing Server Dialback protocol: the verification materials consist of a token obtained over XMPP, the token is checked by the authoritative server for a given domain using implementation-specific methods such as character-by-character comparison, and secure DNS is needed in order to place significant trust in such tokens, although it is known that at the time of this writing many domains use Dialback Keys even in the absence of secure DNS.

6. Assertion Mechanisms

An assertion is a server's statement that an XML stream is to be associated with the asserted domain.

6.1. TLS

During TLS negotiation, an XMPP server acting as a TLS server sends its certificate to the connecting client or peer server acting as a TLS client. This certificate is interpreted as an assertion of the server's identity.

6.2. SASL

During SASL negotiation after TLS negotiation, an XMPP server acting as a TLS server can include an authorization identity; such an authzid is an assertion of the server's identity.

6.3. <db:result>

When two servers use the Server Dialback protocol [XEP-0220], the originating server asserts its identity by sending a <db:result/> element to the receiving server, where the 'from' attribute specifies the domain name being asserted by the originating server.

Note: Although historically the <db:result/> element has contained a dialback key as XML character data, the <db:result/> element can also be used without dialback keys as a mere assertion; this usage is sometimes colloquially referred to as "dialback without dialback".

6.4. A Note about Stream Attributes

XML streams include 'to' and 'from' attributes. However, these are not assertions of identity, and are merely early indications of the identity that a client or server will later assert during TLS negotiation, SASL negotiation, or Server Dialback negotiation.

7. Delegation Methods

Although domain name associations are closely tied to delegation in some scenarios, delegation is irrelevant when the source domain is exactly the same as the hostname of the XMPP service, as is often the case with single-domain services. There are two methods for secure delegation: DNSSEC (see the [XMPP-DANE] spec) and HTTPS Redirect (see the [XMPP-POSH] spec).

8. Security Considerations

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

9. IANA Considerations

This document has no actions for the IANA.

10. References

10.1. Normative 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.

[XMPP-DANE] Miller, M. and P. Saint-Andre, "Using DNS Security Extensions (DNSSEC) and DNS-based Authentication of Named Entities (DANE) as a Prooftype for XMPP Domain Name Associations", draft-miller-xmpp-dnssec-prooftype-02 (work in progress), June 2012.

[XMPP-POSH] Miller, M. and P. Saint-Andre, "Using PKIX over Secure HTTP (POSH) as a Prooftype for XMPP Domain Name Associations", draft-miller-xmpp-posh-prooftype-00 (work in progress), June 2012.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61,

RFC 3365, August 2002.

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

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[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.

[XEP-0220] Miller, J., Saint-Andre, P., and P. Hancke, "Server Dialback", XSF XEP 0220, August 2011.

10.2. Informative References

[RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, October 2004.

[XEP-0238] Saint-Andre, P., "XMPP Protocol Flows for Inter-Domain Federation", XSF XEP 0238, March 2008.

Authors' Addresses

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

Email: psaintan@cisco.com

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

Email: mamille2@cisco.com