XEP-0165: Best Practices to Discourage JID Mimicking

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

2007-12-13
Version 0.6

Status	Type	Short Name
Deferred	Informational	N/A

This document recommends best practices to discourage mimicking of Jabber IDs.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

There are two forms of address spoofing: forging and mimicking.
In the context of Jabber/XMPP technologies, an address is *forged* when an entity is able to generate an XML stanza whose 'from' address does not correspond to the account credentials with which the entity authenticated onto the network -- for example, if an entity that authenticated as "stpeter@jabber.org" is able to send XML stanzas from "MaineBoy@jabber.org" or "peter@saint-andre.com".
Address forging is difficult in Jabber/XMPP systems given the requirement for sending servers to stamp 'from' addresses and for receiving servers to verify sending domains via server dialback or server-to-server authentication (see XMPP Core [1]). Difficult, but not impossible: a rogue server could forge JIDs at the sending domain by ignoring the stamping requirement and could even forge JIDs at other domains by means of a DNS poisoning attack. However, discussion of ways to deal with such rogue servers is out of scope for this document.
An address is *mimicked* when an entity provides legitimate authentication credentials for and sends XML stanzas from an account whose Jabber ID (JID) appears to a human user to be the same as another JID -- for example, in some clients "paypa1@jabber.org" (spelled with the number one as the final character of the node identifier) may appear to be the same as "paypal@jabber.org (spelled with the lower-case version of the letter "L"). [2] A more sophisticated example of address mimicking (which may not render correctly in all browsers) is the following:

```
@.org
```

That JID is not an uppercase version of "stpeter@jabber.org" in US-ASCII characters, but a fake JID made up mostly of Cherokee characters, namely:

```
U+13DA U+13A2 U+13B5 U+13AC U+13A2 U+13AC U+13D2
  @
  U+13AB U+13AA U+13F4 U+13F4 U+13AC U+13D2 .org
```

In this example, it is unlikely that the average user could tell the difference between the real JID and the fake JID. [3]
By contrast with address forging, it may be relatively easy to mimic (some) JIDs in Jabber/XMPP systems, especially because JIDs can contain almost any Unicode character. The possibility of address mimicking introduces security vulnerabilities of the kind that have also plagued the World Wide Web, specifically the phenomenon known as phishing. [4] To combat

[1] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[2] This phenomenon is sometimes called "typejacking".
[3] Naturally, there is no way to distinguish with full certainty which is the fake JID and which is the real JID. For example, in some communication contexts, the Cherokee JID may be the real JID and the US-ASCII JID may thus appear to be the fake JID.
[4] Phishing has been defined by the Financial Services Technology Consortium Counter-Phishing Initiative as "a broadly launched social engineering attack in which an electronic identity is misrepresented in an attempt

those vulnerabilities, this document recommends a set of best practices to minimize the potential impact of address mimicking on the Jabber/XMPP network. [5]

2 Recommendations

2.1 Presentation of JIDs

Every human user of Jabber/XMPP technologies presumably has a preferred language (or, in some cases, a small set of preferred languages), which an XMPP application SHOULD gather either explicitly from the user or implicitly via the operating system of the user's device. Furthermore, every language has a range of characters normally used to represent that language in textual form. Therefore, an XMPP application SHOULD warn the user when presenting a JID that uses characters outside the normal range of the user's preferred language(s). [6]

2.2 The Roster as a Petname System

As explained in Introduction to Petname Systems [7], no one naming or address scheme can provide names that are simultaneously global, memorable, and unique. However, certain *combinations* of names and addresses can provide all three properties, and such combinations are commonly called "petname systems". In particular, the information contained in a user's roster (see XMPP IM [8]) can be combined with information provided by a user's contacts to construct a petname system. Consider the following combination of names:

1. The JID "stpeter@jabber.org" is globally unique on the Jabber/XMPP network, but it is not necessarily memorable.

2. The nickname "psa" (asserted by the user associated with the address "stpeter@jabber.org") is globally memorable but not necessarily unique; see User Nickname (XEP-0172) [9] for more information about user-asserted nicknames.

to trick individuals into revealing personal credentials that can be used fraudulently against them"). To be precise, the current document (1) does not assume that such attacks will be broadly launched and (2) focuses on the misrepresentation of Jabber IDs (not any other identifiers) within the context of Jabber/XMPP systems.

[5] This document does not cover handling of non-XMPP addresses, for example HTTP URLs. Jabber/XMPP clients SHOULD handle such addresses in accordance with best practices for the relevant non-XMPP technology.

[6] This recommendation is not intended to discourage communication across language communities; instead, it simply recognizes the existence of such language communities and encourages due caution when presenting unfamiliar character sets to human users.

[7] Introduction to Petname Systems <http://www.skyhunter.com/marcs/petnames/IntroPetNames.html>.

[8] RFC 6121: Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence <http://tools.ietf.org/html/rfc6121>.

[9] XEP-0172: User Nickname <https://xmpp.org/extensions/xep-0172.html>.

3. The handle or petname "that protocol dude" (assigned by a contact who adds "stpeter@jabber.org" to her contact list) is privately memorable and unique [10] but is by no means global since it has meaning only to the person who assigns it; for consistency with User Nickname (XEP-0172) [11] and XMPP IM [12] we refer to this as a "handle". [13]

A client SHOULD require an end user to assign a handle for every contact added to the person's roster, which SHOULD be stored in the roster as the value of the <item/> element's 'name' attribute (see the Security Considerations section of this document for further discussion). A client SHOULD then present that handle instead of or in addition to the contact's JID or nickname (e.g., in the user's roster and in chat interfaces). This will help to discourage mimicked addresses from being presented as equivalent to the address that is being mimicked.

2.3 Associating Security Credentials with Roster Items

Although a Jabber ID can be considered globally unique, the petname system in which it is embedded can be strengthened by associating that JID with a key that can be used for signing and encryption (such as an OpenPGP key, X.509 certificate, or RSA key), preferably a key that encapsulates the associated XMPP address. A client SHOULD associate a key with the user of that client, and SHOULD generate such a key if the user does not have one.
Unfortunately, cryptographic identities such as keys, certificates, and fingerprints are even less memorable than JIDs, which makes assigning a handle even more important. Therefore, if a contact provides such a cryptographic identity, a client MUST reliably associate it with the contact in a user's roster (including, as mentioned, a handle for each contact) in order to further strengthen the petname system.

2.4 Referrals

In order to strengthen the web of interaction and trust between Jabber/XMPP users, it is helpful for them to share roster items. In particular, when a user wants to subscribe to the presence of a potential contact, the user SHOULD seek a referral from a third person who knows both the user and the contact. Such a referral consists of a roster item sent from the third person to the potential contact, encapsulated using the Roster Item Exchange (XEP-0144) [15] protocol:

Listing 1: A Basic Referral

[10] If not shared or leaked, it may even be securely unique.
[11] XEP-0172: User Nickname <https://xmpp.org/extensions/xep-0172.html>.
[12] RFC 6121: Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence <http://tools.ietf.org/html/rfc6121>.
[13] In RFC 6121 [14] this was referred to as an "alias".
[15] XEP-0144: Roster Item Exchange <https://xmpp.org/extensions/xep-0144.html>.

```
<message from='peter@saint-andre.com' to='MaineBoy@jabber.org'>
  <x xmlns='http://jabber.org/protocol/rosterx'>
    <item jid='stpeter@jabber.org' name='Peter␣Saint-Andre'/>
  </x>
</message>
```

Here, the 'name' attribute encapsulates what in petname systems is known as an "alleged name", that is, the name for an entity proposed by a third party.
Such a referral SHOULD also include the user's nick as understood by the third person (encapsulated in the format defined in XEP-0172) and fingerprint of the user as understood by the third person (encapsulated in the format defined in Public Key Publishing (XEP-0189) [16]):

Listing 2: Referral With Nickname and Public Key

```
<message from='peter@saint-andre.com' to='MaineBoy@jabber.org'>
  <x xmlns='http://jabber.org/protocol/rosterx'>
    <item jid='stpeter@jabber.org' name='Peter␣Saint-Andre'>
      <nick xmlns='http://jabber.org/protocol/nick'>psa</nick>
      <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
        <KeyName>stpeterRSAkey1</KeyName>
        ...
      </KeyInfo>
      <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
        <KeyName>stpeterX509cert1</KeyName>
        ...
      </KeyInfo>
    </item>
  </x>
</message>
```

The third person MUST NOT simply copy the key as communicated by the user but instead MUST validate it against the public key of the user.

2.5 Subscription Requests

We have seen that, at a minimum, three names or address types are needed to provide a petname system for XMPP: a JID, a nickname, and a handle (preferably strengthened by inclusion of a fingerprint derived from a key). However, at present a subscription request contains only the JID of the sender:

Listing 3: A Basic Subscription Request

```
<presence from='stpeter@jabber.org' to='MaineBoy@jabber.org' type='
    subscribe'/>
```

[16] XEP-0189: Public Key Publishing <https://xmpp.org/extensions/xep-0189.html>.

Naturally, based on the JID, it is possible to pull information about the sender from a persistent data store such as an LDAP database, vcard-temp (XEP-0054) [17] node, or future profile system (see User Profile (XEP-0154) [18]). However, to speed interactions, this document recommends that when a client sends a subscription request, it SHOULD include the preferred nickname of the sender (encapsulated via the format specified in User Nickname (XEP-0172) [19]) and the sender's key or keys.

Listing 4: Subscription Request With Nickname and Key

```
<presence from='stpeter@jabber.org' to='MaineBoy@jabber.org' type='
    subscribe'>
  <nick xmlns='http://jabber.org/protocol/nick'>psa</nick>
  <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
    <KeyName>stpeterRSAkey1</KeyName>
    ...
  </KeyInfo>
  <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
    <KeyName>stpeterX509cert1</KeyName>
    ...
  </KeyInfo>
</presence>
```

If one or more referrals have been received, the user or client MUST check the key or keys provided in the subscription request against the key or keys provided in the referral or referrals.

3 Security Considerations

A client should not allow a user to assign as a handle the alleged name received in a referral. In order for a user-assigned handle to strengthen the security of the petname system, the user must not shared the handle with other individuals. If the handle is stored in the user's roster, the handle may be compromised since roster storage is not necessarily a secure medium (e.g., the handle could be read by a server administrator). If the server is not trusted by the user, the client should store the handle locally on the user's device rather than in the roster.
A user should not place more trust in a referral than he or she places in the person who sends it.

[17] XEP-0054: vcard-temp <https://xmpp.org/extensions/xep-0054.html>.
[18] XEP-0154: User Profile <https://xmpp.org/extensions/xep-0154.html>.
[19] XEP-0172: User Nickname <https://xmpp.org/extensions/xep-0172.html>.

4 IANA Considerations

This document requires no interaction with the Internet Assigned Numbers Authority (IANA) [20].

5 XMPP Registrar Considerations

This document requires no interaction with the XMPP Registrar [21].

[20] 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/>.

[21] 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/>.