Network Working Group
Internet-Draft
Updates: 6120 (if approved)
Intended status: Standards Track
Expires: August 13, 2014

T. Alkemade

February 9, 2014

# Validating Info/Query (IQ) stanzas in the Extensible Messaging and Presence Protocol (XMPP)
## draft-alkemade-xmpp-iq-validation-00

Abstract

This document provides security recommendations for the validation and generation of Info/Query (IQ) stanzas in the Extensible Messaging and Presence Protocol (XMPP). This document updates RFC 6120.

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 August 13, 2014.

Table of Contents

1. Introduction . . . . . 3
2. Terminology . . . . . 3
3. Discussion Venue . . . . . 3
4. Recommendations . . . . . 3
4.1. No 'from' . . . . . 3
4.2. Rejecting spoofed replies to queries . . . . . 4
4.3. Preventing presence leaks . . . . . 4
5. IANA Considerations . . . . . 4
6. Security Considerations . . . . . 5
7. Normative References . . . . . 5
Author's Address . . . . . 5

## 1. Introduction

The Extensible Messaging and Presence Protocol (XMPP) [RFC6120] uses Info/Query (IQ) stanzas as a "request-response" mechanism. The semantics of IQ enable an entity to make a request of, and receive a response from, another entity. The interaction is tracked by the requesting entity through use of the 'id' attribute. Thus, IQ interactions follow a common pattern of structured data exchange such as get/result or set/result (although an error can be returned in reply to a request if appropriate).

However, it was found not all implementations properly verify the origin of IQ responses. This documents provides recommendations on how to avoid spoofed responses.

## 2. Terminology

Various security-related terms are to be understood in the sense defined in [RFC4949].

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. Discussion Venue

The discussion venue for this document is the mailing list of the XMPP Working Group, for which archives and subscription information can be found at <https://www.ietf.org/mailman/listinfo/xmpp>.

## 4. Recommendations

### 4.1. No 'from'

Section 8.1.2.1. of [RFC6120] specifies that IQ stanzas sent on behalf of the user's own account MUST either (a) include no 'from' attribute or (b) use the user's bare JID as 'from' address (i.e., <localpart@domainpart>). For compatibility with incorrect servers and servers still following [RFC3920], implementations MAY additionally accept a reply with either (a) a 'from' address equal to the full JID of the client (i.e., <localpart@domainpart/resourcepart>) or (b) a 'from' address equal to the domainpart of the JID of the account (i.e., <domainpart>).

### 4.2. Rejecting spoofed replies to queries

'id' attributes are used as end-to-end identifiers of stanzas: the same 'id' attribute is used across every hop. When delivered, the receiver will see the same 'id' value as the sender specified. As described in Section 8.1.3. of [RFC6120], it is REQUIRED to include 'id' values on IQ stanzas and RECOMMENDED for all other stanza types. The entity creating a stanza needs to ensure the 'id' values it generates are unique.

After sending an IQ stanza with type "get" or "set", an entity may store the 'id' and 'to' of the outgoing <iq/> element to identify the response. When an IQ stanza comes in with a matching 'id' and type "result" or "error", the entity MUST verify that the 'from' attribute on the <iq/> matches the 'to' of the outgoing stanza. If the 'from' and 'to' attributes do not match, the entity MUST ignore the stanza. As is mandatory in response to IQ stanzas of type "result" or "error", the entity MUST NOT return an error.

For queries where the intended recipient is the server acting on behalf of the user's own account entities MAY apply the exceptions in Section 4.1.

### 4.3. Preventing presence leaks

Many implementations use a counter to generate new 'id' attributes for stanzas to guarantee their uniqueness. However, this may leak presence information of the user: it can give an approximation of how long a client has been running and how many stanzas it has sent since a previous stanza. This could, for example, give an indication of how many messages a user has sent in a certain time. Therefore clients SHOULD NOT include a counter in the 'id' attribute.

Additionally, it is RECOMMENDED to use randomly or pseudo-randomly generated 'id' attributes. Implementations using [RFC4122] to generate Universally Unique IDentifiers (UUIDs) to use as 'id' attributes MUST use version 4 UUIDs, which are randomly or pseudo-randomly generated and carry no identifying information. Implementations using a pseudo-random generator, either directly or for generating UUIDs, SHOULD make sure that future values are hard to predict. For more information see [RFC4086].

## 5. IANA Considerations

This document requests no actions of the IANA.

## 6. Security Considerations

This document covers security.

## 7. Normative References

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

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

[RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, July 2005.

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

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

Author's Address

Thijs Alkemade

Email: me@thijsalkema.de