XEP-0268: Incident Handling

Artur Hefczyc
mailto:artur.hefczyc@gmail.com
xmpp:artur.hefczyc@tigase.org

Florian Jensen
mailto:admin@flosoft.biz
xmpp:admin@im.flosoft.biz

Mickaël Rémond
mailto:mickael.remond@process-one.net
xmpp:mremond@process-one.net

Peter Saint-Andre
mailto:xsf@stpeter.im
xmpp:peter@jabber.org
http://stpeter.im/

Matthew Wild
mailto:mwild1@gmail.com
xmpp:me@matthewwild.co.uk

2012-05-29
Version 0.6

Status	**Type**	**Short Name**
Deferred	Standards Track	NOT_YET_ASSIGNED

This specification defines methods for incident reporting among XMPP server deployments using the IODEF format produced by the IETF's INCH Working Group.

Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 – 2018 by the XMPP Standards Foundation (XSF).

Permissions

Permission is hereby granted, free of charge, to any person obtaining a copy of this specification (the ”Specification”), to make use of the Specification without restriction, including without limitation the rights to implement the Specification in a software program, deploy the Specification in a network service, and copy, modify, merge, publish, translate, distribute, sublicense, or sell copies of the Specification, and to permit persons to whom the Specification is furnished to do so, subject to the condition that the foregoing copyright notice and this permission notice shall be included in all copies or substantial portions of the Specification. Unless separate permission is granted, modified works that are redistributed shall not contain misleading information regarding the authors, title, number, or publisher of the Specification, and shall not claim endorsement of the modified works by the authors, any organization or project to which the authors belong, or the XMPP Standards Foundation.

Warranty

NOTE WELL: This Specification is provided on an ”AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE.

Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall the XMPP Standards Foundation or any author of this Specification be liable for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising from, out of, or in connection with the Specification or the implementation, deployment, or other use of the Specification (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if the XMPP Standards Foundation or such author has been advised of the possibility of such damages.

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF’s Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy> or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

Contents

1 Introduction

As XMPP technologies have been deployed more widely, the open XMPP network has become a more significant target for attacks. This specification defines ways for XMPP server deployments to share information with each other and therefore to handle such attacks in a more real-time fashion. In particular, it defines a way to use the IODEF format (defined in RFC 5070 [1] and produced by the IETF's INCH Working Group) as the basis for sharing incident reports among XMPP server deployments. (For some related considerations, see RFC 2350 [2] and RFC 3067 [3].)

2 Interactions

This document defines several interactions (similar to those in RID, see RFC 6045 [4]) between XMPP server deployments with respect to incident handling. These interactions are transported using the XMPP <iq/> stanza as described below, where each element (qualified by the 'urn:xmpp:incident:2' namespace) is used as a wrapper for IODEF data.

1. The <report/> element (contained in an <iq/> stanza of type "set") describes the nature of an incident and also flags the 'status' of the incident as "new", "updated", or "resolved"; it is sent from one server to another for informative purposes but without requesting assistance (for which see the <request/> element). This element is similar to a RID message type of "Report".

2. The <inquiry/> element (contained in an <iq/> stanza of type "get") asks for information about an incident; it is expected that the reply will contain a <report/> element. This element is similar to a RID message type of "IncidentQuery".

3. The <request/> element (contained in an <iq/> stanza of type "get") asks for assistance in resolving an incident, e.g., by requesting that the server take some action. This element is similar to a RID message type of "Investigation" or "TraceRequest".

4. The <response/> element (contained in an <iq/> stanza of type "set") provides assistance in resolving an incident. This element is similar to a RID message type of "Result".

[1] RFC 5070: The Incident Object Description Exchange Format <http://tools.ietf.org/html/rfc5070>.

[2] RFC 2350: Expectations for Computer Security Incident Response <http://tools.ietf.org/html/rfc2350>.

[3] RFC 3067: TERENA's Incident Object Description and Exchange Format Requirements <http://tools.ietf.org/html/rfc3067>.

[4] RFC 6045: Real-time Inter-network Defense (RID) <http://tools.ietf.org/html/rfc6045>.

3 Report Format and Processing

When one server wants to send information about an incident, it sends a incident report to another server. The report consists of an XMPP <iq/> stanza of type ”set” containing a <report/> element that in turn contains an IODEF document. An example is shown below.

Listing 1: A report of trouble

```
<iq from=’jabber.org’ id=’vk2x91g47’ to=’im.flosoft.biz’ type=’set’>
  <report xmlns=’urn:xmpp:incident:2’>
    <Incident xmlns=’urn:ietf:params:xml:ns:iodef-1.0’
              purpose=’reporting’>
      <IncidentID name=’jabber.org’>4BF5D2CE-7C90-4860-BEF2-43
         A7D777D5FF</IncidentID>
      <StartTime>2009-04-13T19:05:20Z</StartTime>
      <EndTime>2009-04-13T19:27:22Z</EndTime>
      <ReportTime>2009-04-13T19:31:07Z</ReportTime>
      <Description xml:lang=’en’>lots of MUC spammers from clueless.
         lit!</Description>
      <Contact role=’admin’ type=’person’>
        <AdditionalData>
          <jid xmlns=’urn:xmpp:incident:2’>stpeter@jabber.org</jid>
        </AdditionalData>
      </Contact>
      <Contact role=’admin’ type=’person’>
        <AdditionalData>
          <jid xmlns=’urn:xmpp:jid:0’>stpeter@jabber.org</jid>
        </AdditionalData>
      </Contact>
      <Contact role=’ext-type’ ext-type=’chatroom’>
        <AdditionalData>
          <jid xmlns=’urn:xmpp:jid:0’>operators@muc.xmpp.org</jid>
        </AdditionalData>
      </Contact>
      <RelatedActivity>
        <IncidentID name=’im.example.com’>133BCE2E-E669-4ECE-B0F8-766
           B9E65630D</IncidentID>
      </RelatedActivity>
      <Assessment>
        <Impact lang=’en’ severity=’medium’ completion=’succeeded’
           type=’dos’/>
      </Assessment>
      <EventData>
        <Flow>
          <System category=’source’>
            <Node>
              <Address category=’ext-category’ ext-category=’xmpp’>
                 abuser@clueless.lit</Address>
              <Counter type=’ext-type’ ext-type=’xmpp-presence’>123</
```

```
                  Counter>
            </Node>
            <Node>
              <Address category=’ext-category’ ext-category=’xmpp’>
                  luser27@clueless.lit</Address>
              <Counter type=’ext-type’ ext-type=’xmpp-presence’>47</
                  Counter>
            </Node>
          </System>
          <System category=’target’>
            <Node>
              <Address category=’ext-category’ ext-category=’xmpp’>
                  jdev@conference.jabber.org</Address>
              <Address category=’ext-category’ ext-category=’xmpp’>
                  jabber@conference.jabber.org</Address>
              <NodeRole category=’ext-category’ ext-category=’xmpp-muc
                  ’/>
            </Node>
          </System>
        </Flow>
      </EventData>
    </Incident>
  </report>
</iq>
```

If the recipient is able to process the report, it MUST return an <iq/> stanza of type ”result”; if not, it MUST return an <iq/> stanza of type ”error” (error handling will be defined in a future version of this specification).

4 Inquiry Format and Processing

When one server wants to find out more information about an incident, it sends an inquiry to another server (not necessarily the server where the incident occurred).

Listing 2: An inquiry about an incident

```
<iq from=’tigase.org’ id=’br6a31m9’ to=’im.flosoft.biz’ type=’get’>
  <inquiry xmlns=’urn:xmpp:incident:2’>
    <Incident xmlns=’urn:ietf:params:xml:ns:iodef-1.0’
              purpose=’traceback’>
      <IncidentID name=’jabber.org’>4BF5D2CE-7C90-4860-BEF2-43
         A7D777D5FF</IncidentID>
    </Incident>
  </inquiry>
</iq>
```

If the recipient is able to process the inquiry, it MUST return an <iq/> stanza of type ”result” and then send a report about the incident using an <iq/> stanza of type ”set” as defined above; if not, it MUST return an <iq/> stanza of type ”error” (error handling will be defined in a future version of this specification).

5 Request Format and Processing

When one server wants to ask for assistance in resolving an incident, it sends a request to another server (not necessarily the server where the incident occurred).
Here, the server where the attack occurred requests that the server where the attack originated will disable the offending accounts (via the ”block-host” value for the ’action’ attribute of the IODEF <Expectation/> element).

Listing 3: A request for assistance

```
<iq from='jabber.org' id='kq62vx31' to='clueless.lit' type='get'>
  <request xmlns='urn:xmpp:incident:2'>
    <Incident xmlns='urn:ietf:params:xml:ns:iodef-1.0'
              purpose='mitigation'>
      <IncidentID name='jabber.org'>4BF5D2CE-7C90-4860-BEF2-43
         A7D777D5FF</IncidentID>
      <StartTime>2009-04-13T19:05:20Z</StartTime>
      <EndTime>2009-04-13T19:27:22Z</EndTime>
      <ReportTime>2009-04-13T19:31:07Z</ReportTime>
      <Description xml:lang='en'>lots of MUC spammers from clueless.
         lit!</Description>
      <Contact role='admin' type='person'>
        <AdditionalData>
          <jid xmlns='urn:xmpp:incident:2'>stpeter@jabber.org</jid>
        </AdditionalData>
      </Contact>
      <Contact role='admin' type='person'>
        <AdditionalData>
          <jid xmlns='urn:xmpp:jid:0'>stpeter@jabber.org</jid>
        </AdditionalData>
      </Contact>
      <Contact role='ext-type' ext-type='chatroom'>
        <AdditionalData>
          <jid xmlns='urn:xmpp:jid:0'>operators@muc.xmpp.org</jid>
        </AdditionalData>
      </Contact>
      <RelatedActivity>
        <IncidentID name='im.example.com'>133BCE2E-E669-4ECE-B0F8-766
           B9E65630D</IncidentID>
      </RelatedActivity>
      <Assessment>
```

```
        <Impact lang='en' severity='medium' completion='succeeded'
           type='dos'/>
      </Assessment>
      <EventData>
        <Flow>
          <System category='source'>
            <Node>
              <Address category='ext-category' ext-category='xmpp'>
                 abuser@clueless.lit</Address>
              <Counter type='ext-type' ext-type='xmpp-presence'>123</
                 Counter>
            </Node>
            <Node>
              <Address category='ext-category' ext-category='xmpp'>
                 luser27@clueless.lit</Address>
              <Counter type='ext-type' ext-type='xmpp-presence'>47</
                 Counter>
            </Node>
          </System>
          <System category='target'>
            <Node>
              <Address category='ext-category' ext-category='xmpp'>
                 jdev@conference.jabber.org</Address>
              <Address category='ext-category' ext-category='xmpp'>
                 jabber@conference.jabber.org</Address>
              <NodeRole category='ext-category' ext-category='xmpp-muc
                 '/>
            </Node>
          </System>
        </Flow>
        <Expectation action='block-host'/>
      </EventData>
    </Incident>
  </request>
</iq>
```

If the recipient is able to process the report, it MUST return an <iq/> stanza of type ”result”; if not, it MUST return an <iq/> stanza of type ”error” (error handling will be defined in a future version of this specification).

6 Response Format and Processing

When one server provides assistance in resolving an incident, it sends a response to another server (not necessarily the server where the incident occurred).
Here, the server where the attack originated informs the server where the attack occurred that it has disabled the offending accounts (via the IODEF <HistoryItem/> element).

Listing 4: A response to a request for assistance

```
<iq from='clueless.list' id='ic1fa53v' to='jabber.org' type='set'>
  <response xmlns='urn:xmpp:incident:2'>
    <Incident xmlns='urn:ietf:params:xml:ns:iodef-1.0'
              purpose='mitigation'>
      <IncidentID name='jabber.org'>4BF5D2CE-7C90-4860-BEF2-43
         A7D777D5FF</IncidentID>
      <StartTime>2009-04-13T19:05:20Z</StartTime>
      <EndTime>2009-04-13T19:27:22Z</EndTime>
      <ReportTime>2009-04-13T19:31:07Z</ReportTime>
      <Description xml:lang='en'>lots of MUC spammers from clueless.
         lit!</Description>
      <Contact role='admin' type='person'>
        <AdditionalData>
          <jid xmlns='urn:xmpp:incident:2'>stpeter@jabber.org</jid>
        </AdditionalData>
      </Contact>
      <Contact role='admin' type='person'>
        <AdditionalData>
          <jid xmlns='urn:xmpp:jid:0'>stpeter@jabber.org</jid>
        </AdditionalData>
      </Contact>
      <Contact role='ext-type' ext-type='chatroom'>
        <AdditionalData>
          <jid xmlns='urn:xmpp:jid:0'>operators@muc.xmpp.org</jid>
        </AdditionalData>
      </Contact>
      <RelatedActivity>
        <IncidentID name='im.example.com'>133BCE2E-E669-4ECE-B0F8-766
           B9E65630D</IncidentID>
      </RelatedActivity>
      <Assessment>
        <Impact lang='en' severity='medium' completion='succeeded'
           type='dos'/>
      </Assessment>
      <EventData>
        <Flow>
          <System category='source'>
            <Node>
              <Address category='ext-category' ext-category='xmpp'>
                 abuser@clueless.lit</Address>
              <Counter type='ext-type' ext-type='xmpp-presence'>123</
                 Counter>
            </Node>
            <Node>
              <Address category='ext-category' ext-category='xmpp'>
                 luser27@clueless.lit</Address>
              <Counter type='ext-type' ext-type='xmpp-presence'>47</
                 Counter>
            </Node>
          </System>
          <System category='target'>
            <Node>
              <Address category='ext-category' ext-category='xmpp'>
                 jdev@conference.jabber.org</Address>
              <Address category='ext-category' ext-category='xmpp'>
                 jabber@conference.jabber.org</Address>
              <NodeRole category='ext-category' ext-category='xmpp-muc
                 '/>
            </Node>
          </System>
        </Flow>
        <Expectation action='block-host'/>
      </EventData>
      <History>
        <HistoryItem action='blockquote'>
          <DateTime>2009-04-13T19:47:11Z</DateTime>
          <Description>Account disabled</Description>
        </HistoryItem>
      </History>
    </Incident>
  </response>
</iq>
```

If the recipient is able to process the report, it MUST return an <iq/> stanza of type ”result”; if not, it MUST return an <iq/> stanza of type ”error” (error handling will be defined in a future version of this specification).

7 Definition of IODEF Extensions

This document defines the following IODEF extensions, described in accordance with the guidelines in Guidelines for Defining Extensions to IODEF [5].

7.1 Contact

This specification defines an extended Contact role of ”chatroom”, i.e., a new enumerated value for the Contact@role attribute. This value specifies a text conference where discussion of the incident can take place, e.g., an IRC channel or an XMPP Multi-User Chat (XEP-0045) [6] room. Since there are many different chatroom technologies, the address of the chatroom shall be specified as the child of an <AdditionalData/> element. For XMPP chatrooms, the

[5] Guidelines for Defining Extensions to IODEF <http://tools.ietf.org/html/draft-ietf-mile-template>. Work in progress.

[6] XEP-0045: Multi-User Chat <https://xmpp.org/extensions/xep-0045.html>.

address is the XML character data of a <jid/> element qualified by the 'urn:xmpp:jid:0' namespace.
Note: Definition of the <jid/> element might be moved to a separate specification.

7.2 Address

This specification defines an extended Address category of "xmpp", i.e., a new enumerated value for the Address@category attribute. This value specifies the JabberID of a network entity, in conformance with RFC 6122 [7] or its successor.

7.3 NodeRole

This specification defines several extended NodeRole categories, i.e., new enumerated values for the NodeRole@category attribute:

- "xmpp" -- the network role of an XMPP service or core router as defined by RFC 6120 [8] and RFC 6121 [9]
- "xmpp-bytestreams" -- the network role of an XMPP SOCKS5 byestreams service as defined by SOCKS5 Bytestreams (XEP-0065) [10]
- "xmpp-muc" -- the network role of an XMPP multi-user chat service as defined by XEP-0045
- "xmpp-pubsub" -- the network role of an XMPP pubsub service as defined by Publish-Subscribe (XEP-0060) [11]

7.4 AdditionalData

This specification defines an AdditionalData element of <jid/> qualified by the 'urn:xmpp:jid:0' namespace. The XML character data of this element is a JabberID (i.e., an XMPP address) that conforms to RFC 6122 or its successor.
Note: Definition of the <jid/> element might be moved to a separate specification.

[7] RFC 6122: Extensible Messaging and Presence Protocol (XMPP): Address Format <http://tools.ietf.org/html/rfc6122>.

[8] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.

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

[10] XEP-0065: SOCKS5 Bytestreams <https://xmpp.org/extensions/xep-0065.html>.

[11] XEP-0060: Publish-Subscribe <https://xmpp.org/extensions/xep-0060.html>.

8 Internationalization Considerations

The <jid/> element qualified by the 'urn:xmpp:incident:2' namespace is a "JID slot" as described in rfc6122bis [12].
Note: Definition of the <jid/> element might be moved to a separate specification.

9 Security Considerations

It is RECOMMENDED for a server deployment to exchange incident reports only with peer servers that it trusts, for example peers that are in its "server roster" as described in Server Buddies (XEP-0267) [13].
This technology is designed to help mitigate attacks on the XMPP network. However, incident reporting is itself vulnerable to the following attacks:

- False reports could lead a server to deny service to legitimate users or peer servers (see also Best Practices to Discourage Denial of Service Attacks (XEP-0205) [14]). To help mitigate such attacks, a server SHOULD treat with caution any incident reports that it might receive from untrusted entities.
- If traffic between two servers is not protected using Transport Layer Security (TLS), a passive eavesdropper could gain access to incident reports and therefore adjust its behavior in response. To prevent such attacks, servers SHOULD use TLS.

Use of the XMPP channel is convenient for communication among XMPP servers; however, if a denial of service attack is severe enough then that channel itself might be unusable.
Unless explicitly configured to do so, a receiving server SHOULD NOT automatically modify its configuration based on receipt of an incident report, even from a trusted server, but instead SHOULD prompt the human administrators so that they can take appropriate action.
A receiving server MAY accept incident reports from peers that are not on its "trust list", but SHOULD treat such reports with caution and provide them to the human administrator(s) of the server.
A receiving server MAY forward reports that it receives to other servers it trusts.

[12] Extensible Messaging and Presence Protocol (XMPP): Address Format <https://datatracker.ietf.org/doc/draft-ietf-xmpp-6122bis/>. Work in progress.

[13] XEP-0267: Server Buddies <https://xmpp.org/extensions/xep-0267.html>.

[14] XEP-0205: Best Practices to Discourage Denial of Service Attacks <https://xmpp.org/extensions/xep-0205.html>.

10 IANA Considerations

This document might require interaction with the Internet Assigned Numbers Authority (IANA) [15] to register various IODEF extensions, in accordance with draft-ietf-mile-template.

11 XMPP Registrar Considerations

11.1 Protocol Namespaces

This specification defines the following XML namespace:

- urn:xmpp:incident:2
- urn:xmpp:jid:0

Upon advancement of this specification from a status of Experimental to a status of Draft, the XMPP Registrar [16] shall add the foregoing namespace to the registry located at <https://xmpp.org/registrar/namespaces.html>, as described in Section 4 of XMPP Registrar Function (XEP-0053) [17].
Note: Registration of the 'urn:xmpp:jid:0' namespace might be moved to a separate specification.

11.2 Protocol Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

12 XML Schemas

12.1 Incident Namespace

[15] 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/>.

[16] 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/>.

[17] XEP-0053: XMPP Registrar Function <https://xmpp.org/extensions/xep-0053.html>.

```
<?xml version=’1.0’ encoding=’UTF-8’?>

<xs:schema
    xmlns:xs=’http://www.w3.org/2001/XMLSchema’
    targetNamespace=’urn:xmpp:incident:2’
    xmlns=’urn:xmpp:incident:2’
    elementFormDefault=’qualified’>

  <xs:import namespace=’urn:ietf:params:xml:ns:iodef-1.0’/>

  <xs:element name=’inquiry’ type=’IODEFContainerType’/>
  <xs:element name=’report’ type=’IODEFContainerType’/>
  <xs:element name=’request’ type=’IODEFContainerType’/>
  <xs:element name=’response’ type=’IODEFContainerType’/>

  <xs:complexType name=”IODEFContainerType”>
    <xs:sequence xmlns:i=’urn:ietf:params:xml:ns:iodef-1.0’>
      <xs:element ref=’i:Incident’ minOccurs=’1’ maxOccurs=’1’/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

12.2 JID Namespace

Note: This schema and associated text might be moved to a separate specification.

```
<?xml version=’1.0’ encoding=’UTF-8’?>

<xs:schema
    xmlns:xs=’http://www.w3.org/2001/XMLSchema’
    targetNamespace=’urn:xmpp:jid:0’
    xmlns=’urn:xmpp:jid:0’
    elementFormDefault=’qualified’>

  <xs:element name=’jid’ type=’xs:string’/>

</xs:schema>
```