Extended Incident Handling Working Group — Kathleen M. Moriarty
Internet-draft — RSA, The Security Division of EMC
Intended status: Standards Track — Brian H. Trammell
draft-moriarty-post-inch-rid-soap-04.txt — CERT Network Situational
Expires: August 25, 2008 — Awareness
February 25, 2008

IODEF/RID over SOAP

Status of this Memo

Abstract

Documents intended to be shared among multiple constituencies must share a common format and transport mechanism. The Incident Object Description Exchange Format (IODEF) defines a common XML format for document exchange. This draft outlines the SOAP wrapper for all IODEF documents and extensions to facilitate an interoperable and secure communication of documents. The SOAP wrapper allows for flexibility in the selection of a transport protocol. The transport protocols will be provided through existing standards and SOAP binding, such as SOAP over HTTP/TLS and SOAP over BEEP.

TABLE OF CONTENTS

1. Terminology

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

1.1 Introduction

The Incident Object Description Exchange Format (IODEF) [RFCXXXX] describes an XML document format for the purpose of exchanging data between Computer Security Incident Response Teams (CSIRTs) or those responsible for security incident handling for network providers (NPs). The defined document format provides an easy way for CSIRTs to exchange data in a way which can be easily parsed. In order for the IODEF documents to be shared between entities, a uniform method for transport is necessary. SOAP [3] will provide a layer of abstraction and enable the use of multiple transport protocol bindings. IODEF documents and extensions will be contained in an XML Real-time Inter-network Defense (RID) [RFCYYYY] envelope inside the body of a SOAP message.

HTTP/TLS [RFC4346] has been selected as the REQUIRED SOAP binding for exchanging IODEF/RID messages. The primary reason for selecting HTTP/TLS is due to the existence of multiple successful implementations of SOAP over HTTP/TLS, and to its being widely understood, despite the additional overhead associated with this combination. The Transport Layer Security (TLS) Protocol [RFC4346] MUST be followed for the implementation and deployment of this protocol. Excellent tool support exists to ease the development of applications using SOAP over HTTP. BEEP may optionally be supported following the SOAP over BEEP standard [RFC4227].

2. SOAP Wrapper

IODEF/RID documents, including all supported extensions, intended to be shared between CSIRTS or NPs MUST use a SOAP wrapper, along with a supported transport protocol binding, for transport. The transport is independent of the wrapper. SOAP will be used to provide the messaging framework and can make distinctions as to how messages should be handled by each participating system. SOAP has been selected because of the flexibility it provides for binding with transport protocols, which can be independent of the IODEF/RID messaging system.

The SOAP body of the message will contain the appropriate contents for the respective RID message type and will be structured according to the SOAP messaging specifications [4]. The SOAP

header contains information pertinent to all participating systems that receive the message, including the ultimate destination, any intermediate hosts, and message processing policy information and is provided through RIDPolicy in the RID schema [RFCYYYY].

Depending on the message or document being transported, there may be a case, such as with RID messages, in which a host may only need to view the SOAP header and not the SOAP body and is, therefore, acting as a SOAP intermediary node. An example of this would be if one RID system was sending a communication to a RID system for which there was no direct trust relationship, an intermediate RID system may be used to provide the trusted path between the communicating systems. This intermediate system may not need to see the contents of the SOAP body. Therefore, the elements or classes needed by all participating systems MUST be in the SOAP header, specifically the RIDPolicy class. Each participating system receiving an incident handling IODEF/RID document is an ultimate destination and has to parse and view the entire IODEF/RID document to make necessary decisions.

The SOAP specifications for intermediate and ultimate nodes MUST be Followed; for example, a message destined for an intermediate node would contain the attribute env:role with the value http://www.w3c.org/2003/05/soap-envelope/role/next. Also in accordance with the SOAP specifications, the attribute of env:mustUnderstand has a value of "true" to ensure each node processes the header blocks consistent with the specifications for IODEF/RID.

SOAP messages are typically a one-way conversation. Transmittal of incident information to another RID host in the form of a Report message is the single case within RID where a one way communication is specified. The arrival of an IODEF Report document in a RID message is simply an assertion that a described incident occurred. In the case of other RID message types, two or more SOAP messages may be exchanged to enable bi-directional communication. Request/response pairs defined by RID include:

TraceRequest/TraceAuthorization/Result,
Investigation/Result, and
IncidentQuery/Report.

3. Transport Protocol Bindings

The SOAP binding will be used for message transport. One agreed-upon protocol, HTTP/TLS, MUST be implemented by all RID systems and other protocols are optional. The use of a single transport binding supported by all systems sending and receiving RID messages and will enable interoperability between participating CSIRTS and NPs. Other protocol bindings may be defined in separate documents.

3.1 SOAP over HTTP/TLS

SOAP over HTTP/TLS is widely supported, as are ancillary tools such

as the Web Services Description Language (WSDL), hence the selection of SOAP over HTTP/1.1 over TLS as Mandatory for transport of RID communications. Security is provided through the RID specification. TLS offers additional security at the transport

layer to ensure the integrity of the session.

BCP 56 [RFC3205] contains a number of important considerations when using HTTP for application protocols. These include the size of the payload for the application, whether the application will use a web browser, whether the protocol should be defined on a port other than 80, and if the security provided through HTTP/TLS suits the needs of the new application.

It is acknowledged within the scope of these concerns that HTTP/TLS is not ideally suited for IODEF/RID transport, as the former is a client-server protocol and the latter a message-exchange protocol; however, the ease of implementation for services based on SOAP over HTTP outweighs these concerns. Consistent with BCP 56, IODEF/RID over SOAP over HTTP/TLS will require its own TCP port assignment from IANA.

Every RID system participating in a consortium MUST listen for HTTP/TLS connections on the assigned port, as the requests and responses in a RID message exchange transaction may be significantly separated in time. If a RID message is answered immediately, or within a generally accepted HTTP client timeout (about thirty seconds), the listening system SHOULD return the reply message in the HTTP response body; otherwise, it must initiate a connection to the requesting system and send its reply in an HTTP request.

If the HTTP response body sent in reply to a RID message does not contain a RID message itself, the response body SHOULD be empty, and RID clients MUST ignore any response body that is not an expected RID message. This provision applies ONLY to HTTP response bodies; unsolicited HTTP requests (such as Reports not preceded by an IncidentQuery) are handled according to the message exchange pattern described in RID.

RID systems SHOULD use HTTP/1.1 persistent connections as described in [RFC2616] to minimize TCP connection setup overhead. RID systems SHOULD support chunked transfer encoding on the HTTP server side to allow the implementation of clients that do not need to precalculate message sizes before constructing HTTP headers.

3.2 SOAP over BEEP

SOAP over BEEP is an optional transport binding for IODEF/RID. A RID system supporting BEEP [RFC3080] MAY attempt to use SOAP over BEEP on first connection with a peer; if the peer does not support SOAP over BEEP, the initiating peer MUST fall back to SOAP over HTTPS, and SHOULD note that the peer does not support BEEP, to

avoid attempting to use BEEP in future communications. The state table for the support of alternate protocols may be maintained for a period of one week or less depending on system resources. The duration and size of the state table should be a configurable

option.

BEEP has certain implementation advantages over HTTP/TLS for this application; however, the protocol has not been widely implemented. Communication between participating RID systems is on a server-to-server basis, for which BEEP is better suited than HTTP. Incident handling may at times require immediate action; thus, a protocol with low overhead and minimum bandwidth requirements is desirable.

To provide equivalent transport-layer security to HTTP/TLS, the BEEP TLS profile MUST be supported if BEEP is implemented and SHOULD be used.

4. Examples

The examples below, parallel to the examples in section 4.5 of RID, demonstrate how the structure of RID messages fit into SOAP containers as outlined in this document for each message type. Of particular note in each is the use of the RID policy information in the SOAP header. The RID schema was designed to enable the use of RIDPolicy to stand alone in the SOAP header and to enable the use of the RID class, RequestStatus to stand alone in the SOAP body without the need for an IODEF document. When the RID class called IncidentSource is used, it is combined with an associated IODEF document in the SOAP body to provide all of the necessary information in response to an incident handling request. The first example includes the full IODEF/RID message and associated IODEF-Document; following examples omit the IODEF-Document and Refer to it in a comment. Where indicated, the IODEF-Document must be present, following the requirements listed in the IODEF and RID specifications.

Note: for each example listed below, [RFC3330] addresses were used. Assume each IP address listed is actually a separate network range held by different NPs. Addresses were used from /27 network ranges.

4.1. Example TraceRequest message

This TraceRequest is identical to the TraceRequest example in Section 4.5.1.1 of RID and would be sent from a CSIRT reporting a denial-of-service attack in progress to its upstream NP. This request asks the upstream to continue the trace and to rate-limit traffic closer to the source.

```
<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
 <SOAP-ENV:Header>
  <iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
```

```
                xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef-rid:RIDPolicy MsgType="TraceRequest"
                           MsgDestination="RIDSystem">
```

```
       <iodef-rid:PolicyRegion region="IntraConsortium"/>
       <iodef:Node>
         <iodef:Address category="ipv4-addr">192.0.2.3</iodef:Address>
       </iodef:Node>
       <iodef-rid:TrafficType type="Attack"/>
       <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
         CERT-FOR-OUR-DOMAIN#207-1
       </iodef:IncidentID>
     </iodef-rid:RIDPolicy>
   </iodef-rid:RID>
 </SOAP-ENV:Header>
 <SOAP-ENV:Body>
   <iodef:IODEF-Document version="1.00"
          xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
     <iodef:Incident restriction="need-to-know" purpose="traceback">
       <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
         CERT-FOR-OUR-DOMAIN#207-1
     </iodef:IncidentID>
     <iodef:DetectTime>2004-02-02T22:49:24+00:00</iodef:DetectTime>
     <iodef:StartTime>2004-02-02T22:19:24+00:00</iodef:StartTime>
     <iodef:ReportTime>2004-02-02T23:20:24+00:00</iodef:ReportTime>
     <iodef:Description>Host involved in DOS attack</iodef:Description>
     <iodef:Assessment>
     <iodef:Impact severity="low" completion="failed" type="dos"/>
     </iodef:Assessment>
     <iodef:Contact role="creator" type="organization">
         <iodef:ContactName>Constituency-contact for 192.0.2.35
         </iodef:ContactName>
         <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
     </iodef:Contact>
       <iodef:EventData>
         <iodef:Flow>
          <iodef:System category="source">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.35
               </iodef:Address>
            </iodef:Node>
            <iodef:Service>
              <iodef:port>38765</iodef:port>
            </iodef:Service>
          </iodef:System>
           <iodef:System category="target">
            <iodef:Node>
             <iodef:Address category="ipv4-addr">192.0.2.67
               </iodef:Address>
            </iodef:Node>
            <iodef:Service>
              <iodef:port>80</iodef:port>
```

```
            </iodef:Service>
          </iodef:System>
        </iodef:Flow>
        <iodef:Expectation severity="high" action="rate-limit-host">
```

```
            <iodef:Description>
              Rate limit traffic close to source
            </iodef:Description>
          </iodef:Expectation>
          <iodef:Record>
            <iodef:RecordData>
              <iodef:Description>
              The IPv4 packet included was used in the described attack
              </iodef:Description>
              <iodef:RecordItem dtype="ipv4-packet">450000522ad9
                0000ff06c41fc0a801020a010102976d0050103e020810d9
                4a1350021000ad6700005468616e6b20796f7520666f7220
                6361726566756c6c7920726164696e6720746869732052
                46432e0a
              </iodef:RecordItem>
            </iodef:RecordData>
          </iodef:Record>
        </iodef:EventData>
        <iodef:History>
          <iodef:HistoryItem>
            <iodef:DateTime>2001-09-14T08:19:01+00:00</iodef:DateTime>
            <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
              CSIRT-FOR-OUR-DOMAIN#207-1
            </iodef:IncidentID>
            <iodef:Description>
              Notification sent to next upstream NP closer to 192.0.2.35
            </iodef:Description>
          </iodef:HistoryItem>
        </iodef:History>
      </iodef:Incident>
    </iodef:IODEF-Document>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
<!-- Digital signature accompanied by above RID and IODEF -->
<Envelope xmlns="urn:envelope"
          xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0"
          xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0">
  <iodef:IODEF-Document>
    <iodef:Incident>
      <iodef:EventData>
        <iodef:Record>
          <iodef:RecordData>
            <iodef:RecordItem type="ipv4-packet">450000522ad9
             0000ff06c41fc0a801020a010102976d0050103e020810d9
             4a1350021000ad6700005468616e6b20796f7520666f7220
             6361726566756c6c7920726164696e6720746869732052
             46432e0a
            </iodef:RecordItem>
```

```
          </iodef:RecordData>
        </iodef:Record>
      </iodef:EventData>
    </iodef:Incident>
```

```
  </iodef:IODEF-Document>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
       Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
                  20010315#WithComments"/>
      <SignatureMethod
       Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm=
           "http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod
         Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>KiI5+6SnFAs429VNwsoJjHPplmo=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>
      VvyXqCzjoW0m2NdxNeToXQcqcSM80W+JMW+Kn01cS3z3KQwCPeswzg==
    </SignatureValue>
    <KeyInfo>
      <KeyValue>
        <DSAKeyValue>
          <P>/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9j
             QTxeEu0ImbzRMqzVDZkVG9xD7nN1kuFw==</P>
          <Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>
          <G>Z4Rxsnqc9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/XPaF5
             Bpsy4pNWMOHCBiNU0NogpsQW5QvnlMpA==</G>
          <Y>VFWTD4I/aKni4YhDyYxAJozmj1iAzPLw9Wwd5B+Z9J5E7lHjcAJ+bs
             HifTyYdnj+roGzy4o09YntYD8zneQ7lw==</Y>
        </DSAKeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</Envelope>
```

4.2 RequestAuthorization Message Example

This RequestAuthorization is identical to the RequestAuthorization example in section 4.5.1.2 of the RID specification and is sent in response to the TraceRequest to approve the request.

```
<SOAP-ENV:Envelope
   xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
 <SOAP-ENV:Header>
  <iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
                 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
```

```
<iodef-rid:RIDPolicy MsgType="RequestAuthorization"
                     MsgDestination="RIDSystem">
   <iodef-rid:PolicyRegion region="IntraConsortium"/>
   <iodef:Node>
```

```
          <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType type="Attack"/>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
      <iodef-rid:RequestStatus AuthorizationStatus="Approved"/>
    </iodef-rid:RID>
  </SOAP-ENV:Header>
</SOAP-ENV:Envelope>
```

4.3 Result Message Example

This Result message is identical to the Result example in section 4.5.1.3 of the RID. This message is the final response from the TraceRequest that has completed to notify the requestor of the results and actions taken from the request.

```
<SOAP-ENV:Envelope
   xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
 <SOAP-ENV:Header>
  <iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
                 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef-rid:RIDPolicy MsgType="Result"
                           MsgDestination="RIDSystem">
        <iodef-rid:PolicyRegion region="IntraConsortium"/>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">192.0.2.67</iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType type="Attack"/>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
      <iodef-rid:IncidentSource>
        <iodef-rid:SourceFound>true</iodef-rid:SourceFound>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">192.0.2.37</iodef:Address>
        </iodef:Node>
      </iodef-rid:IncidentSource>
    </iodef-rid:RID>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <iodef:IODEF-Document version="1.00"
           xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef:Incident restriction="need-to-know" purpose="traceback">
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
```

```
          CERT-FOR-OUR-DOMAIN#207-1
        </iodef:IncidentID>
        <iodef:DetectTime>2004-02-02T22:49:24+00:00</iodef:DetectTime>
        <iodef:StartTime>2004-02-02T22:19:24+00:00</iodef:StartTime>
```

```
        <iodef:ReportTime>2004-02-02T23:20:24+00:00</iodef:ReportTime>
        <iodef:Description>Host involved in DOS attack
          </iodef:Description>
        <iodef:Assessment>
          <iodef:Impact severity="low" completion="failed" type="dos"/>
        </iodef:Assessment>
        <iodef:Contact role="creator" type="organization">
          <iodef:ContactName>Constituency-contact for 192.0.2.35
       </iodef:ContactName>
          <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
        </iodef:Contact>
        <iodef:EventData>
          <iodef:Contact role="admin" type="organization">
            <iodef:ContactName>Admin-contact for 192.0.2.35
            </iodef:ContactName>
            <iodef:Email>Admin-contact@192.0.2.35</iodef:Email>
          </iodef:Contact>
          <iodef:Flow>
            <iodef:System category="intermediate">
              <iodef:Node>
                <iodef:Address category="ipv4-addr">192.0.2.35
          </iodef:Address>
              </iodef:Node>
            </iodef:System>
          </iodef:Flow>
          <iodef:EventData>
            <iodef:Contact role="admin" type="organization">
              <iodef:ContactName>Admin-contact for 192.0.2.3
              </iodef:ContactName>
              <iodef:Email>Admin-contact@192.0.2.3</iodef:Email>
            </iodef:Contact>
            <iodef:Flow>
              <iodef:System category="intermediate">
                <iodef:Node>
                  <iodef:Address category="ipv4-addr">192.0.2.3
                    </iodef:Address>
                </iodef:Node>
              </iodef:System>
            </iodef:Flow>
          </iodef:EventData>
        </iodef:EventData>
        <iodef:EventData>
          <iodef:Flow>
            <iodef:System category="source">
              <iodef:Node>
                <iodef:Address category="ipv4-addr">192.0.2.35
                  </iodef:Address>
              </iodef:Node>
```

```
        <iodef:Service>
          <iodef:port>38765</iodef:port>
        </iodef:Service>
      </iodef:System>
```

```
            <iodef:System category="target">
              <iodef:Node>
                <iodef:Address category="ipv4-addr">192.0.2.67
                  </iodef:Address>
              </iodef:Node>
              <iodef:Service>
                <iodef:port>80</iodef:port>
              </iodef:Service>
            </iodef:System>
          </iodef:Flow>
          <iodef:Expectation severity="high" action="rate-limit-host">
            <iodef:Description>
              Rate limit traffic close to source
            </iodef:Description>
          </iodef:Expectation>
          <iodef:Record>
            <iodef:RecordData>
              <iodef:Description>
              The IPv4 packet included was used in the described attack
              </iodef:Description>
              <iodef:RecordItem dtype="ipv4-packet">450000522ad9
                0000ff06c41fc0a801020a010102976d0050103e020810d9
                4a1350021000ad6700005468616e6b20796f7520666f7220
                6361726566756c6c7920726164696e6720746869732052
                46432e0a
              </iodef:RecordItem>
            </iodef:RecordData>
          </iodef:Record>
        </iodef:EventData>
        <iodef:History>
          <iodef:HistoryItem>
            <iodef:DateTime>2004-02-02T22:53:01+00:00</iodef:DateTime>
            <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
              CSIRT-FOR-OUR-DOMAIN#207-1
            </iodef:IncidentID>
            <iodef:Description>
              Notification sent to next upstream NP closer to 192.0.2.35
            </iodef:Description>
          </iodef:HistoryItem>
          <iodef:HistoryItem action="rate-limit-host">
            <iodef:DateTime>2004-02-02T23:07:21+00:00</iodef:DateTime>
            <iodef:IncidentID name="CSIRT-FOR-NP3">
              CSIRT-FOR-NP3#3291-1
            </iodef:IncidentID>
            <iodef:Description>
              Host rate limited for 24 hours
            </iodef:Description>
          </iodef:HistoryItem>
```

```
        </iodef:History>
      </iodef:Incident>
    </iodef:IODEF-Document>
  </SOAP-ENV:Body>
```

```
</SOAP-ENV:Envelope>
```

4.4 Example InvestigationRequest Message

This InvestigationRequest is identical to the InvestigationRequest example in section 4.5.2.1 of the RID specification and would be sent in a situation similar to that of example 4.1, when the source of the attack is known.

```
<SOAP-ENV:Envelope
   xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
 <SOAP-ENV:Header>
  <iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
                  xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef-rid:RIDPolicy MsgType="Investigation"
                           MsgDestination="SourceOfIncident">
        <iodef-rid:PolicyRegion region="PeerToPeer"/>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">192.0.2.98</iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType type="Attack"/>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#208-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
    </iodef-rid:RID>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <iodef:IODEF-Document version="1.00"
           xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef:Incident restriction="need-to-know" purpose="other">
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#208-1
        </iodef:IncidentID>
        <iodef:DetectTime>2004-02-05T08:13:33+00:00</iodef:DetectTime>
        <iodef:StartTime>2004-02-05T08:13:31+00:00</iodef:StartTime>
        <iodef:EndTime>2004-02-05T08:13:33+00:00</iodef:EndTime>
        <iodef:ReportTime>2004-02-05T08:13:35+00:00</iodef:ReportTime>
        <iodef:Description>Host involved in DOS attack
          </iodef:Description>
        <iodef:Assessment>
         <iodef:Impact severity="low" completion="failed" type="recon"/>
        </iodef:Assessment>
        <iodef:Contact role="creator" type="organization">
          <iodef:ContactName>Constituency-contact for 192.0.2.35
       </iodef:ContactName>
          <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
        </iodef:Contact>
```

```
        <iodef:EventData>
          <iodef:Flow>
            <iodef:System category="source">
              <iodef:Node>
```

```
              <iodef:Address category="ipv4-addr">192.0.2.35
                </iodef:Address>
            </iodef:Node>
            <iodef:Service>
              <iodef:port>41421</iodef:port>
            </iodef:Service>
          </iodef:System>
          <iodef:System category="target">
            <iodef:Node>
              <iodef:Address category="ipv4-addr">192.0.2.67
                </iodef:Address>
            </iodef:Node>
            <iodef:Service>
              <iodef:port>80</iodef:port>
            </iodef:Service>
          </iodef:System>
        </iodef:Flow>
        <iodef:Expectation severity="high" action="investigate">
          <iodef:Description>
            Investigate whether source has been compromised
          </iodef:Description>
        </iodef:Expectation>
      </iodef:EventData>
      <iodef:History>
        <iodef:HistoryItem>
          <iodef:DateTime>2004-02-05T08:19:01+00:00</iodef:DateTime>
          <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
            CSIRT-FOR-OUR-DOMAIN#208-1
          </iodef:IncidentID>
          <iodef:Description>
            Investigation request sent to NP for 192.0.2.35
          </iodef:Description>
        </iodef:HistoryItem>
      </iodef:History>
    </iodef:Incident>
  </iodef:IODEF-Document>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

4.5 Example Report

This Report is identical to the Report example in section 4.5.3.1 of the RID specification.

```
<SOAP-ENV:Envelope
   xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
 <SOAP-ENV:Header>
  <iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
```

```
                xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef-rid:RIDPolicy MsgType="Report" MsgDestination="RIDSystem">
        <iodef-rid:PolicyRegion region="PeerToPeer"/>
        <iodef:Node>
```

```
          <iodef:Address category="ipv4-addr">192.0.2.3</iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType type="Attack"/>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#209-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
    </iodef-rid:RID>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <iodef:IODEF-Document version="1.00"
           xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef:Incident restriction="need-to-know" purpose="reporting">
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#209-1
        </iodef:IncidentID>
        <iodef:DetectTime>2004-02-05T10:21:08+00:00</iodef:DetectTime>
        <iodef:StartTime>2004-02-05T10:21:05+00:00</iodef:StartTime>
        <iodef:EndTime>2004-02-05T10:35:00+00:00</iodef:EndTime>
        <iodef:ReportTime>2004-02-05T10:27:38+00:00</iodef:ReportTime>
        <iodef:Description>Host illicitly accessed admin account
        </iodef:Description>
        <iodef:Assessment>
          <iodef:Impact severity="high" completion="succeeded"
                 type="admin"/>
          <iodef:Confidence rating="high"/>
        </iodef:Assessment>
        <iodef:Contact role="creator" type="organization">
          <iodef:ContactName>Constituency-contact for 192.0.2.35
       </iodef:ContactName>
          <iodef:Email>Constituency-contact@192.0.2.35</iodef:Email>
        </iodef:Contact>
        <iodef:EventData>
          <iodef:Flow>
            <iodef:System category="source">
              <iodef:Node>
                <iodef:Address category="ipv4-addr">192.0.2.35
                  </iodef:Address>
              </iodef:Node>
              <iodef:Service>
                <iodef:port>32821</iodef:port>
              </iodef:Service>
            </iodef:System>
            <iodef:System category="target">
              <iodef:Node>
                <iodef:Address category="ipv4-addr">192.0.2.67
                  </iodef:Address>
              </iodef:Node>
```

```
        <iodef:Service>
          <iodef:port>22</iodef:port>
        </iodef:Service>
      </iodef:System>
```

```
          </iodef:Flow>
        </iodef:EventData>
        <iodef:History>
          <iodef:HistoryItem>
            <iodef:DateTime>2004-02-05T10:28:00+00:00</iodef:DateTime>
            <iodef:IncidentID name="CSIRT-FOR-OUR-DOMAIN">
              CSIRT-FOR-OUR-DOMAIN#209-1
            </iodef:IncidentID>
            <iodef:Description>
              Incident report sent to NP for 192.0.2.35
            </iodef:Description>
          </iodef:HistoryItem>
        </iodef:History>
      </iodef:Incident>
    </iodef:IODEF-Document>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

4.6 Example IncidentQuery

This IncidentQuery is identical to the IncidentQuery example in Section 4.5.4.1 of the RID specification.

```
<SOAP-ENV:Envelope
   xmlns:SOAP-ENV="http://www.w3.org/2001/12/soap-envelope">
 <SOAP-ENV:Header>
  <iodef-rid:RID xmlns:iodef-rid="urn:ietf:params:xml:ns:iodef-rid-1.0"
                 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef-rid:RIDPolicy MsgType="IncidentQuery"
                           MsgDestination="RIDSystem">
        <iodef-rid:PolicyRegion region="PeerToPeer"/>
        <iodef:Node>
          <iodef:Address category="ipv4-addr">192.0.2.3</iodef:Address>
        </iodef:Node>
        <iodef-rid:TrafficType type="Attack"/>
        <iodef:IncidentID name="CERT-FOR-OUR-DOMAIN">
          CERT-FOR-OUR-DOMAIN#210-1
        </iodef:IncidentID>
      </iodef-rid:RIDPolicy>
    </iodef-rid:RID>
 </SOAP-ENV:Header>
</SOAP-ENV:Envelope>
```

5. Security Considerations

All security considerations of related documents MUST be considered, including those in the following documents: the Incident Object Description Exchange (IODEF), [RFCXXXX] and Real-time Inter-network Defense (RID) [RFCYYYY]. The SOAP wrappers described herein are built upon the foundation of these documents; the security considerations contained therein are incorporated by reference.

Security guidelines such as those described in, "Security in a Web Services World: A Proposed Architecture and Roadmap", [1] should be considered.

5.1 Privacy and Confidentiality

For transport confidentiality, TLS (whether HTTP/TLS or the BEEP TLS profile) MUST be supported and SHOULD be used.

Since multiple bindings for transport may be implemented, RID implementations MUST support XML encryption [5] to encrypt the SOAP body. Since XML encryption is performed at the IODEF document level, not only is the transport encrypted when a document is

sensitive or contains sensitive elements, but the stored document is also encrypted. Note that this encryption applies only to the SOAP body; policy information in the SOAP header should remain

unencrypted if it is necessary for the intermediate node to dispatch the message. XML encryption protects the IODEF/RID document in the SOAP body from being viewed by any involved SOAP intermediary node.

5.2 Authentication and Identification

For transport authentication and identification, TLS (whether HTTP/TLS or the BEEP TLS profile) with mutual authentication MUST be supported and SHOULD be used. Each RID consortium SHOULD use a trusted public key infrastructure (PKI) to manage identities for TLS connections. The public/private key pairs used for XML encryption and digital signatures provide authentication for the RID message [RFC3275], [2]. The session encryption keys are also used to identify the communicating hosts and provide integrity for the session.

Since multiple bindings for transport may be implemented, RID implementations MUST support XML digital signatures [RFC3275] to sign the SOAP body; the rationale and implementation here is parallel to that for XML encryption discussed in section 5.1.

6. IANA Considerations

The IANA is requested to assign TCP ports in the Registered Port Numbers set for RID over SOAP over HTTPS and for RID over SOAP over BEEP.

7. Summary

SOAP provides the wrapper to facilitate the exchange of RID messages. The IETF and W3C standards provide detailed implementation details for SOAP and SOAP protocol bindings. The use of existing standards assists with development and interoperability between RID systems exchanging IODEF documents for incident handling purposes. HTTP/TLS is the mandatory transport binding for SOAP to be implemented and BEEP with a TLS profile is optional.

8. Informative References

[RFC3330] "Special-Use IPv4 Addresses." IANA. September 2002.

[1] "Security in a Web Services World: A Proposed Architecture and Roadmap". IBM and Microsoft, April 2002. http://www-106.ibm.com/developerworks/webservices/library/ws-secmap

[2] XML-Signature Syntax and Processing, W3C Recommendation, M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, February

2002. http://www.w3.org/TR/xmldsig-core/#sec-Design

8.1 Normative References

[RFC2119] "Key Words for Use in RFCs to Indicate Requirement Levels," S. Bradner, March 1997.

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

[RFC3080] "The Blocks Extensible Exchange Protocol Core," M. Rose. March 2001.

[RFC3205] "On the Use of HTTP as a Substrate," K. Moore, February 2002. (BCP56)

[RFC3275] "(Extensible Markup Language) XML-Signature Syntax and Processing", D. Eastlake 3rd, J. Reagle, D. Solo. March 2002.

[RFC4227] "Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP)," E. O'Tuathail, and M. Rose, January 2006. http://www.faqs.org/rfcs/rfc4227.html

[RFC4346] "The Transport Layer Security (TLS) Protocol Version 1.1," T. Dierks, E. Rescorla. April 2006.

[RFCXXXX] "The Incident Object Data Exchange Format Data Model and XML Implementation," J. Meijer, R. Danyliw, and Y. Demchenko, August 2006.
http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-14.txt

[RFCYYYY] "Real-time Inter-network Defense," K. Moriarty, December 2007. http://www.ietf.org/internet-drafts/draft-moriarty-post-inch-rid-02.txt

[3] SOAP Version 1.2 Part 0: Primer, W3C Recommendation, http://www.w3c.org/TR/REC-soap12-part0-20030624/, 24 June 2004.

[4] SOAP Version 1.2 Part 1:Messaging Framework. W3C Recommendation, 24 June 2004.
http://www.w3c.org/TR/REC-soap12-part1-20030624/

[5] XML Encryption Syntax and Processing, W3C Recommendation. T. Imamura, B. Dillaway, and E. Simon, December 2002.

[5] XML-Signature Syntax and Processing, W3C Recommendation, M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, February 2002. http://www.w3.org/TR/xmldsig-core/#sec-Design

8.2 Acknowledgments

Funding for the RFC Editor function is currently provided by the

Internet Society.

8.3 Author Information

Kathleen M. Moriarty
RSA, The Security Division of EMC
174 Middlesex Turnpike
Bedford, MA 01730
Email: Kathleen.Moriarty@RSA.com

Brian H. Trammell
CERT Network Situational Awareness
4500 Fifth Avenue
Pittsburgh, PA 15213
Email: bht@cert.org

Intellectual Property Statement

Full Copyright Statement

Sponsor Information

This work was sponsored by the Air Force under Air Force Contract FA8721-05-C-0002 while Kathleen worked at MIT Lincoln Laboratory.

"Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government."