RFC 5070 : The Incident Object Description Exchange Format

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 décembre 2007

Date de publication du RFC : Décembre 2007

https://www.bortzmeyer.org/5070.html

Pour rendre plus facilement analysables les innombrables rapports d'incidents de sécurité qui circulent sur Internet tous les jours, ce RFC spécifie un format standard XML, nommé IODEF, pour décrire ces incidents. Ce RFC décrivait la version 1, une version 2, plus étendue, a ensuite été publiée dans le RFC 7970 [1].

Tous les jours, des organisations comme les CERT envoient et reçoivent des rapports détaillés concernant une attaque sur un réseau informatique ou un serveur. Ces rapports sont longs et détaillés mais, la plupart du temps, ce n'est pas une attaque isolée qui est intéressante, c'est l'image qui apparait lorsqu'on synthétise tous les rapports, et qu'on voit alors les tendances, par exemple l'arrivée d'un nouveau ver ou bien une attaque concertée contre un pays donné. D'où l'importance de pouvoir analyser automatiquement ces rapports, ce qui impose un modèle de données et un format standard, ce que fournit ce RFC.

Le modèle de données est proche des modèles objet, par exemple dans la descriptions des **classes** d'objets manipulés (comme la classe Incident en section 3.2, avec la cardinalité des attributs). Ces classes sont composés avec des données élémentaires (booléens, entiers, dates) décrits dans la section 2. Le schéma XML complet, écrit en W3C Schema, figure dans la section 8.

Une première tentative de normaliser un tel format avait été faite avec IDMEF, dans le RFC 4765 mais n'avait pas rencontré de consensus. Notre RFC représente désormais la solution standard.

Voici un exemple d'un rapport d'incident, tiré du RFC et qui décrit une reconnaissance menée par un agresseur potentiel :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7970.txt

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- This example describes reconnaissance activity: one-to-one and
     one-to-many scanning -->
<IODEF-Document version="1.00" lang="en"
  xmlns="urn:ietf:params:xml:ns:iodef-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">
  <Incident purpose="reporting">
    <IncidentID name="csirt.example.com">59334</IncidentID>
    <ReportTime>2006-08-02T05:54:02-05:00</ReportTime>
    <Assessment>
      <Impact type="recon" completion="succeeded" />
    </Assessment>
    <Method>
      <!-- Reference to the scanning tool "nmap" -->
      <Reference>
        <ReferenceName>nmap</ReferenceName>
        <URL>http://nmap.toolsite.example.com</URL>
      </Reference>
    </Method>
    <!-- Organizational contact and that for staff in that
         organization -->
    <Contact role="creator" type="organization">
      <ContactName>CSIRT for example.com</ContactName>
      <Email>contact@csirt.example.com</Email>
      <Telephone>+1 412 555 12345</Telephone>
      <!-- Since this <Contact> is nested, Joe Smith is part of the
          CSIRT for example.com -->
      <Contact role="tech" type="person" restriction="need-to-know">
        <ContactName>Joe Smith</ContactName>
        <Email>smith@csirt.example.com</Email>
      </Contact>
    </Contact>
    <EventData>
      <!-- Scanning activity as follows:
        192.0.2.1:60524 >> 192.0.2.3:137
               192.0.2.1:60526 >> 192.0.2.3:138
               192.0.2.1:60527 >> 192.0.2.3:139
               192.0.2.1:60531 >> 192.0.2.3:445
      -->
      <Flow>
        <System category="source">
          <Node>
            <Address category="ipv4-addr">192.0.2.200</Address>
          </Node>
          <Service ip_protocol="6">
            <Portlist>60524,60526,60527,60531</Portlist>
          </Service>
        </System>
        <System category="target">
          <Node>
            <Address category="ipv4-addr">192.0.2.201</Address>
          </Node>
          <Service ip_protocol="6">
            <Portlist>137-139,445</Portlist>
          </Service>
        </System>
      </Flow>
      <!-- Scanning activity as follows:
            192.0.2.2 >> 192.0.2.3/28:445 -->
      <Flow>
        <System category="source">
          <Node>
            <Address category="ipv4-addr">192.0.2.240</Address>
          </Node>
        </System>
        <System category="target">
          <Node>
```

```
            <Address category="ipv4-net">192.0.2.64/28</Address>
          </Node>
          <Service ip_protocol="6">
            <Port>445</Port>
          </Service>
        </System>
      </Flow>
    </EventData>
  </Incident>
</IODEF-Document>
```