RFC 7203 : IODEF-extension for structured cybersecurity information

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 avril 2014

Date de publication du RFC : Avril 2014

https://www.bortzmeyer.org/7203.html

Le format IODEF permet l'échange de données structurées (et donc analysables par un programme) sur des incidents de sécurité. Ce nouvel RFC étend le format IODEF avec des informations utiles pour le monde de la « cybersécurité ».

Le RFC commence par prétendre que le nombre d'incidents de cybersécurité augmente tous les jours (alors qu'on n'en sait rien <https://www.bortzmeyer.org/compter-attaques.html>). Ce qui est sûr, c'est que la quantité d'informations échangées sur ces incidents augmente et qu'il existe une quantité impressionnante de formats structurés et de référentiels (quelques exemples au hasard, pris dans ceux cités par le RFC : CVSS, OVAL, SCAP, XCCDF...). Notre RFC en ajoute donc un, sous forme, non pas d'un format nouveau mais d'une extension de IODEF, un format fondé sur XML et qui avait été normalisé dans le RFC 5070 [1] (remplacé depuis par le RFC 7970). Signe des temps : un des auteurs du RFC travaille au ministère de l'intérieur états-unien...

La section 3 du RFC rappelle ses buts, et l'importance de ne pas repartir de zéro, d'agréger les formats cités plus haut au lieu d'essayer de les remplacer. Les extensions IODEF elles-mêmes figurent en section 4. En gros, il s'agit de permettre d'incorporer dans IODEF des descriptions issues de normes extérieures déjà existantes. Un nouveau registre IANA <https://www.iana.org/assignments/iodef/iodef.xhtml> stocke les spécifications ainsi incorporées. Pour l'instant, le registre n'en compte qu'une seule, urn:ietf:params:xml:ns:mile:mmdef:1.2 qui est fondée sur la norme IEEE MMDEF <http://standards.ieee.org/develop/indconn/icsg/mmdef.html>, qui permet de décrire des logiciels malveillants.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5070.txt

Chacune de ces entrées dans le nouveau registre dérivera d'une classe (notre RFC utilise le vocabulaire de la programmation objet, et le langage UML pour la modélisation) parmi les huit : `AttackPattern`, `Platform`, `Vulnerability`, `Scoring`, `Weakness`, `EventReport`, `Verification` et `Remediation`. Ainsi, MMDEF, la première entrée, hérite de `AttackPattern`. Chacune de ces classes est décrite en détail en section 4.5

Et voici, tiré du RFC, un exemple de rapport IODEF incorporant des éléments MMDEF, décrivant un "*malware*" de nom `eicar_com.zip` (un fichier de test connu) :

```
<?xml version="1.0" encoding="UTF-8"?>
<IODEF-Document version="1.00" lang="en"
 xmlns="urn:ietf:params:xml:ns:iodef-1.0"
 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0"
 xmlns:iodef-sci="urn:ietf:params:xml:ns:iodef-sci-1.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Incident purpose="reporting">
    <IncidentID name="iodef-sci.example.com">189493</IncidentID>
    <ReportTime>2013-06-18T23:19:24+00:00</ReportTime>
    <Description>a candidate security incident</Description>
    <Assessment>
      <Impact completion="failed" type="admin" />
    </Assessment>
    <Method>
      <Description>A candidate attack event</Description>
      <AdditionalData dtype="xml">
        <iodef-sci:AttackPattern
         SpecID="http://xml/metadataSharing.xsd">
          <iodef-sci:RawData dtype="xml">
            <malwareMetaData xmlns="http://xml/metadataSharing.xsd"
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
             xsi:schemaLocation="http://xml/metadataSharing.xsd
             file:metadataSharing.xsd" version="1.200000" id="10000">
              <company>N/A</company>
              <author>MMDEF Generation Script</author>
              <comment>Test MMDEF v1.2 file generated using genMMDEF
              </comment>
              <timestamp>2013-03-23T15:12:50.726000</timestamp>
              <objects>
                <file id="6ce6f415d8475545be5ba114f208b0ff">
                  <md5>6ce6f415d8475545be5ba114f208b0ff</md5>
                  <sha1>da39a3ee5e6b4b0d3255bfef95601890afd80709</sha1>
                  <sha256>e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca4
                          95991b7852b855</sha256>
                  <sha512>cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83
                          f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b9
                          31bd47417a81a538327af927da3e</sha512>
                  <size>184</size>
                  <filename>eicar_com.zip</filename>
                  <MIMEType>application/zip</MIMEType>
                </file>
                <file id="44d88612fea8a8f36de82e1278abb02f">
                  <md5>44d88612fea8a8f36de82e1278abb02f</md5>
                  <sha1>3395856ce81f2b7382dee72602f798b642f14140</sha1>
                  <sha256>275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4
                          538aabf651fd0f</sha256>
                  <sha512>cc805d5fab1fd71a4ab352a9c533e65fb2d5b885518f4e565e
                          68847223b8e6b85cb48f3afad842726d99239c9e36505c64b0
                          dc9a061d9e507d833277ada336ab</sha512>
                  <size>68</size>
                  <crc32>1750191932</crc32>
                  <filename>eicar.com</filename>
                  <filenameWithinInstaller>eicar.com
                  </filenameWithinInstaller>
                </file>
```

```
            </objects>
           <relationships>
             <relationship type="createdBy" id="1">
               <source>
                 <ref>file[@id="6ce6f415d8475545be5ba114f208b0ff"]</ref>
               </source>
               <target>
                 <ref>file[@id="44d88612fea8a8f36de82e1278abb02f"]</ref>
               </target>
               <timestamp>2013-03-23T15:12:50.744000</timestamp>
               </relationship>
             </relationships>
           </malwareMetaData>
         </iodef-sci:RawData>
       </iodef-sci:AttackPattern>
     </AdditionalData>
   </Method>
   <Contact role="creator" type="organization">
     <ContactName>iodef-sci.example.com</ContactName>
     <RegistryHandle registry="arin">iodef-sci.example-com
     </RegistryHandle>
     <Email>contact@csirt.example.com</Email>
   </Contact>
   <EventData>
     <Flow>
       <System category="source">
         <Node>
           <Address category="ipv4-addr">192.0.2.200</Address>
           <Counter type="event">57</Counter>
         </Node>
       </System>
       <System category="target">
         <Node>
           <Address category="ipv4-net">192.0.2.16/28</Address>
         </Node>
         <Service ip_protocol="4">
           <Port>80</Port>
         </Service>
       </System>
     </Flow>
     <Expectation action="block-host" />
     <Expectation action="other" />
   </EventData>
 </Incident>
</IODEF-Document>
```

On notera que bien des discussions préalables au RFC portaient sur cette plaie de l'appropriation intellectuelle, plusieurs des schémas référencés ayant des noms qui sont des marques déposées.