RFC 4765 : The Intrusion Detection Message Exchange Format (IDMEF)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 mars 2007

Date de publication du RFC : Mars 2007

https://www.bortzmeyer.org/4765.html

Ce RFC décrit un format XML d'échanges de données concernant des incidents de sécurité. Il permet aux entités concernées par un incident de sécurité de s'échanger de l'information structurée, donc plus facilement analysable.

Le groupe de travail IDWG de l'IETF a eu une histoire longue et compliquée. Le travail sur ce RFC a commencé il y a longtemps et de curieux archaïsmes y apparaissent (comme l'utilisation de DTD pour décrire le schéma XML ou bien comme l'utilisation du protocole ident, spécifié dans le RFC 1413[1]). Finalement, le groupe n'a pas pu conclure et a été dissous. Les documents déjà prêts ont été publiés, comme notre RFC, avec le statut « Expérimental ». Un autre effort a porté sur un autre format, IODEF, finalement publié dans le RFC 5070 (et depuis mis à jour dans le RFC 7970).

Le problème était de toute façon très difficile : il existe des tas de façons de modéliser un incident de sécurité et une grande hétérogénéité des concepts. Le groupe de travail s'est attelé à une tâche d'ampleur. Le résultat est une modélisation en UML (système peu utilisé à l'IETF) de tous les concepts, accompagné d'un schéma XML écrit en DTD (un autre schéma, non officiel, écrit en W3C XML Schema figure égalemen dans le RFC mais c'est celui en DTD qui fait foi).

Voici un exemple d'un incident décrit dans ce langage, une attaque "*teardrop*" menée par `192.0.2.50` le 9 septembre 2000 :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1413.txt`

```
<idmef:IDMEF-Message xmlns:idmef="http://iana.org/idmef"
                     version="1.0">
     <idmef:Alert messageid="abc123456789">
       <idmef:Analyzer analyzerid="hq-dmz-analyzer01">
         <idmef:Node category="dns">
           <idmef:location>Headquarters DMZ Network</idmef:location>
           <idmef:name>analyzer01.example.com</idmef:name>
         </idmef:Node>
       </idmef:Analyzer>
       <idmef:CreateTime ntpstamp="0xbc723b45.0xef449129">
         2000-03-09T10:01:25.93464-05:00
       </idmef:CreateTime>
       <idmef:Source ident="a1b2c3d4">
         <idmef:Node ident="a1b2c3d4-001" category="dns">
           <idmef:name>badguy.example.net</idmef:name>
           <idmef:Address ident="a1b2c3d4-002"
                          category="ipv4-net-mask">
             <idmef:address>192.0.2.50</idmef:address>
             <idmef:netmask>255.255.255.255</idmef:netmask>
           </idmef:Address>
         </idmef:Node>
       </idmef:Source>
       <idmef:Target ident="d1c2b3a4">
         <idmef:Node ident="d1c2b3a4-001" category="dns">
           <idmef:Address category="ipv4-addr-hex">
             <idmef:address>0xde796f70</idmef:address>
           </idmef:Address>
         </idmef:Node>
       </idmef:Target>
       <idmef:Classification text="Teardrop detected">
         <idmef:Reference origin="bugtraqid">
           <idmef:name>124</idmef:name>
           <idmef:url>http://www.securityfocus.com/bid/124</idmef:url>
         </idmef:Reference>
       </idmef:Classification>
     </idmef:Alert>
</idmef:IDMEF-Message>
```

Notez l'utilisation systématique d'identificateurs (les attributs `ident` pour pouvoir référencer les objets de manière non ambigüe.