RFC 6545 : Real-time Inter-network Defense (RID)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 avril 2012

Date de publication du RFC : Avril 2012

https://www.bortzmeyer.org/6545.html

La sécurité, face aux innombrables attaques que connaissent les réseaux tous les jours, nécessite un échange d'information permanent. Ce RFC normalise donc un format permettant d'échanger et de traiter ce genre d'informations. Il sera donc peut-être un outil technique utile pour les CSIRT et les opérateurs.

La section 1 résume les problèmes de la sécurité des réseaux auxquels les opérateurs font face. Une fois l'attaque détectée, que ce soit un hameçonnage, une DoS ou une pénétration réussie dans un système connecté au réseau, il faut rédiger un rapport, transmettre à l'opérateur d'origine de l'attaque, demander à un opérateur amont de prendre des mesures pour limiter les dégâts, demander de continuer l'enquête en suivant la trace de l'attaquant, etc. Par exemple, si on veut suivre une trace de paquets dont l'adresse IP source est mensongère, et que le filtrage recommandé par le RFC 2827 [1] n'est pas en place, il faut repérer par quel câble sont entrés ces paquets et envoyer ensuite à l'opérateur situé derrière une demande de continuation de l'enquête. Il n'y a pas de mécanisme formel pour cela. Ça se fait typiquement par téléphone ou par envoi d'un courrier en langue naturelle, ce qui augmente les coûts de traitement.

Le nouveau format, normalisé dans ce RFC 6545, se nomme **RID** pour "*Real-time Inter-network Defense*" et se base sur le format IODEF du RFC 5070 (désormais RFC 7970), qui lui-même utilise XML. L'apport par rapport à l'IODEF de base est de cibler la circulation d'informations en « temps réel ». RID avait d'abord été spécifié dans le RFC 6045, que notre RFC met à jour. À part le changement de statut (RID est désormais sur le chemin des normes), les changements (résumés dans la section 1.1) sont de peu d'importance.

RID vise donc à permettre la réponse immédiate à une attaque. Par exemple, lorsqu'une dDoS est perpétrée par un "*botnet*", il faut certes retrouver les zombies mais aussi identifier le contrôleur qui les commande. RID permet de demander un suivi de la trace des premiers, puis ensuite du second.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2827.txt

L'opérateur a typiquement un système de gestion centralisé de son réseau, un NMS. Le futur **IHS** ("*Incident Handling System*") qui recevra et enverra les messages RID devra être intégré à ce NMS. La détection de l'attaque pourra se faire manuellement, ou via un IDS mais cette question est hors-sujet pour RID, qui se contente de permettre le signalement d'attaques, une fois celles-ci détectées.

Quelles sont les obstacles que rencontrent les tentatives de remonter à la source d'une attaque ? La section 2 en donne une liste, et c'est une lecture très recommandée pour comprendre la variété des problèmes auxquels fait face l'opérateur réseau lors d'une attaque. Par exemple, certaines attaques utilisent tellement peu de paquets qu'il est difficile de les répérer. D'autre part, pour prendre rapidement une « empreinte » des paquets utilisés pour l'attaque, les techniques à base d'une fonction de hachage ont souvent été utilisées (cf. « "*Hash-Based IP Traceback*" `<http://www.acm.org/sigcomm/sigcomm2001/p1-snoeren.pdf>` »). Or, certaines attaques ont un contenu des paquets qui varie énormément et il est difficile de trouver une « signature » qui permettrait de dire à l'opérateur précédent « Voici ce que je cherche ». Les nombreuses techniques de "*traceback*" pour IP ont été utilisées pour déterminer quelles étaient les informations importantes à inclure dans RID. Ainsi, il est essentiel d'inclure beaucoup d'informations dans le message RID car les champs significatifs et l'attaque, permettant de repérer les paquets, peuvent être n'importe lesquels. RID permet même d'envoyer la totalité du paquet, si nécessaire.

Une fois que le message RID est prêt, que fait-on pour la communication avec les autres opérateurs et avec les CSIRT ? Les sections 3.1 et 3.2 font remarquer que le courrier électronique n'est pas forcément adapté car il peut être trop lent. Mais, de toute façon, il faut prévoir plusieurs canaux de communication car, en cas d'attaque, certains deviendront peut-être inutilisables. Un réseau distinct de celui utilisé pour le trafic « normal » peut donc être nécessaire (voir plus loin le commentaire de la section 9). Le RFC suggère qu'on peut profiter des négociations qui précèdent un accord de "*peering*" pour mettre en place un canal de communication sécurisé.

Recommandation utile ou vœu pieux ? En tout cas, la section 3.1 rappelle également que RID ne devrait être utilisé que pour lutter contre des attaques, et pas pour perpétuer des sabotages (en dénonçant un innocent dans l'espoir qu'il se fasse filtrer) ou pour censurer.

Maintenant, place au format utilisé (section 4), fondé sur IODEF (RFC 5070). Il y a cinq messages RID possibles :

- `Request` où on demande à un partenaire d'examiner son réseau pour voir d'où venait l'attaque (l'idée est que, partant de celui qui a détecté l'attaque, on envoit des `Request` successifs en remontant peu à peu vers la source de l'attaque). Le même message sert si on a déjà identifié la source et qu'on veut juste davantage d'information.
- `Report` où on transmet de l'information, sans demander d'action immédiate.
- `Query` où on demande des détails sur une attaque dont on a entendu parler (les deux derniers types de message sont typiquement pour la communication avec un CSIRT).
- `Acknowledgment` et `Result` servent à porter les résultats intermédiaires ou finaux.

La section 4.2 décrit plus en détail chacun de ces types.

La section 7 fournit plusieurs jolis exemples, que j'ai simplifié ici. Par exemple, une `Request` envoyé par un CSIRT qui a détecté une DoS et qui demande à un opérateur réseau de tracer l'attaque. Le message est composé d'un document RID puis du document IODEF qui décrit l'attaque :

```
<iodef-rid:RID> <!-- Le schéma est enregistré en
https://www.iana.org/assignments/xml-registry/ns.html -->
  <iodef-rid:RIDPolicy MsgType="TraceRequest"
                       MsgDestination="RIDSystem">
    <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>
<!-- IODEF-Document accompanied by the above RID -->
<iodef:IODEF-Document>
  <iodef:Incident restriction="need-to-know" purpose="traceback">
    <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:EventData>
      <iodef:Flow>
        <iodef:System category="source">
          <iodef:Node>
            <iodef:Address category="ipv4-addr">192.0.2.35
...
```

Et la première réponse, qui indique que la demande de traçage a été approuvée :

```
<iodef-rid:RID>
  <iodef-rid:RIDPolicy MsgType="RequestAuthorization"
                       MsgDestination="RIDSystem">
    <iodef-rid:TrafficType type="Attack"/>
  </iodef-rid:RIDPolicy>
  <iodef-rid:RequestStatus AuthorizationStatus="Approved"/>
</iodef-rid:RID>
```

Et enfin la réponse finale :

```
<iodef-rid:RID>
  <iodef-rid:RIDPolicy MsgType="Result"
                       MsgDestination="RIDSystem">
    <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>
<!-- IODEF-Document accompanied by the above RID -->
<iodef:IODEF-Document>
  <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: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
          6361726566756c6c792072656164696e6720746869732052
          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>
```

L'entièreté du schéma XML, en xsd, figure en section 5.

Comme déjà noté, l'utilisation de ces messages RID ne va pas sans risques. La section 9 les analyse. D'abord, il faut évidemment un canal sécurisé pour les transmettre. Sécurisé au sens de :

- Confidentiel, puisque les informations RID peuvent être très sensibles,
- Fiable (disponible), puisque l'attaque rendra peut-être inutilisable les canaux normaux,
- Authentifié, parce que ceux à qui on demande d'agir sur la base de messages RID voudront savoir à qui ils ont affaire.

Un canal physique dédié faciliterait l'obtention de ces propriétés mais n'est pas forcément réaliste. Le RFC recommande donc plutôt un tunnel chiffré. En combinant TLS sur le tunnel et les signatures XML du RFC 3275 sur le message, on atteint la sécurité désirée. Le protocole exact utilisé est normalisé dans un autre document, le RFC 6546. Bien qu'il utilise le chiffrement, RID ne repose pas uniquement sur la sécurité du canal et permet de chiffrer aussi le message par le chiffrement XML `<http://www.w3.org/TR/xmlenc-core/>`.

RID soulève aussi des questions liées à la protection de la vie privée et la section 9.5 les étudie. RID fournit le moyen de spécifier des détails comme l'extension du « domaine de confiance » à qui on peut envoyer les informations (élément `PolicyRegion`, section 4.3.3.3).