RFC 6772 : Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 janvier 2013

Date de publication du RFC : Janvier 2012

https://www.bortzmeyer.org/6772.html

Toute information sur la position physique d'une personne ou d'une machine (la géolocalisation) est évidemment très sensible et il est normal que les considérations de protection de la vie privée jouent un grand rôle dès qu'on parle de géolocalisation. Le RFC 6280 [1] fixait un cadre général pour la protection de la vie privée face à cette géolocalisation. Ce nouveau RFC étend les techniques des RFC 4119 et RFC 4745 pour permettre d'exprimer les autorisations concernant la géolocalisation, **en fonction de la position** : ce qu'on peut faire de l'information, à qui on peut la transmettre, etc.

Le principe est que le document suivant le format de ce RFC va poser des **conditions** (« si je suis en tel lieu », cf. section 4) et que, en fonction de ces conditions, on aura des **actions** (non spécifiées ici) et surtout des **transformations** (section 6), qui vont changer les valeurs spécifiées par le langage du RFC 4119 : autoriser ou interdire la retransmission de l'information, modifier la durée d'expiration, indiquer un texte décrivant une politique, et enfin délibérement faire perdre de la précision, afin de protéger sa vie privée. Ainsi, pour les localisations civiles (exprimées par rapport aux constructions humaines et pas par rapport à la Terre), on peut utiliser le vocabulaire du RFC 5139 pour spécifier que la localisation doit être limitée en précision à une rue, une ville, voire un pays.

Tirés de la section 7, voici quelques exemples (comme vous le voyez, la syntaxe est du XML, le schéma figure en sections 8 et 9) :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6280.txt

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy">

  <rule id="AA56i09">
    <conditions>
      <gp:location-condition>
        <gp:location
          profile="civic-condition"
          xml:lang="en"
          label="Siemens Neuperlach site 'Legoland'"
          xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
          <country>DE</country>
          <A1>Bavaria</A1>
          <A3>Munich</A3>
          <A4>Perlach</A4>
          <A6>Otto-Hahn-Ring</A6>
          <HNO>6</HNO>
        </gp:location>
      </gp:location-condition>
    </conditions>
    <actions/>
    <transformations/>
  </rule>
</ruleset>
```

Qu'est-ce que cela dit ? Que si la localisation civile actuelle est « 6, Otto-Hahn-Ring, dans le quartier de Perlach à Munich », alors, on ne fait rien de particulier (les éléments `<actions>` et `<transformations>` sont vides). Les conditions auraient pu être exprimées en géodésique et pas en civil, par exemple :

```
<gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
              <gml:pos>-33.8570029378 151.2150070761</gml:pos>
              <gs:radius uom="urn:ogc:def:uom:EPSG::9001">1500
              </gs:radius>
            </gs:Circle>
```

(C'est l'opéra de Sydney.)

Maintenant, avec une transformation qui interdit la retransmission, change la durée de vie de l'information, et limite la précision géodésique à 500 mètres :

```
<transformations>
        <gp:set-retransmission-allowed>false
        </gp:set-retransmission-allowed>

        <gp:set-retention-expiry>86400</gp:set-retention-expiry>

        <gp:provide-location
          profile="geodetic-transformation">
          <lp:provide-geo radius="500"/>
        </gp:provide-location>
</transformations>
```

Attention, si la protection de votre vie privée est cruciale, lisez bien la section 13, qui expose les limites de la protection qu'offrent ces techniques. Par exemple, imaginez que, lorsque vous êtes chez vous, vous réduisez la précision à 200 mètres, pour empêcher qu'on localise votre maison. Imaginons maintenant que le logiciel vous place donc au hasard quelque part dans un cercle de rayon 200 m centré sur votre maison. Un attaquant malin pourrait relever votre position pendant quelques jours, faire l'intersection de ces informations, et trouver la maison avec une bonne précision... Une bonne mise en œuvre de ce RFC devrait donc servir toujours la même information à un demandeur donné, mais, si vous étiez programmeur, vous auriez pensé à ce piège ? Aléatoire n'est dons pas synonyme de sécurité, bien au contraire.

Même sans cela, des informations externes peuvent guider celui qui cherche à vous pister. Si la précision est de mille mètres pendant votre déplacement de Paris à Lyon, l'observateur pourra remarquer que vous utilisez le TGV et réduire ainsi drastiquement l'imprécision.

Pire, le danger peut venir des règles de protection de la vie privée elle-même. Si la configuration par défaut est d'une précision de 100 m, et que quelqu'un indique une dégradation à 1000 m en certains endroits, il indique que ces endroits sont particulièrement sensibles et donc intéressants pour une personne mal intentionnée envers lui.