RFC 7378 : Trustworthy Location

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 décembre 2014

Date de publication du RFC : Décembre 2014

https://www.bortzmeyer.org/7378.html

Il existe des applications de communication (de téléphonie, par exemple), qui indiquent la localisation de l'appelant, et cette localisation est cruciale lorsque il s'agit d'appels d'urgence, par exemple aux pompiers ou à la police, ou, moins dramatique, d'assistance routière (« ma voiture est en panne et je ne sais pas exactement où je suis », comme cela m'est arrivé sur la N 1 ce mois d'août). Ce nouveau RFC décrit le problème de la sécurité et de la fiabilité de la localisation, ainsi que des solutions pour améliorer cette sécurité et cette fiabilité.

Pour envoyer sa localisation à son correspondant, il y a deux sous-problèmes : 1) déterminer la localisation 2) la transmettre de manière sûre. Pour la téléphonie traditionnelle, la localisation est déterminée par le récepteur à partir du numéro de téléphone présenté. Cela veut dire notamment qu'un faux numéro peut entraîner une mauvaise localisation (cf. RFC 7340 [1] et les autres documents du groupe STIR <https://tools.ietf.org/wg/stir>). Il y a plusieurs mécanismes pour s'assurer du numéro de téléphone comme le rappel (qui permet aussi de confirmer l'urgence, cf. RFC 7090). Mais quand l'appelant est mobile, même lorsqu'on est sûr du numéro de téléphone présenté, le problème n'est pas résolu. Ce RFC se focalise sur les cas où le numéro de téléphone de l'appelant est raisonnablement authentifié mais où il reste des doutes sur la localisation physique de la cible (oui, c'est comme cela qu'on désigne la personne ou l'objet dont on cherche à connaître la localisation). Le mode normal d'obtention de la localisation est de faire appel à un LIS ("*Location Information Server*") qui, connaissant les caractéristiques du réseau utilisé, va l'indiquer à son client. Un malveillant peut faire en sorte qu'une mauvaise localisation soit indiquée de trois façons :

— Changement d'endroit ("*place shifting*"), lorsque l'attaquant arrive à placer un faux objet PIDF-LO (" *Presence Information Data Format Location Object*", voir le RFC 4119). Dans certains cas, il y a une limite à la triche, par exemple l'attaquant peut indiquer une fausse position mais qui doit rester dans la zone couverte par un relais donné.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7340.txt

— Changement de moment ("*time shifting*"), où l'attaquant réussit à ré-utiliser une information de localisation qui était vraie dans le passé, mais ne l'est plus.
— Vol de localisation ("*location theft*"), lorsque on présente un objet de localisation qui est correct et valide mais concerne une autre personne.

La première façon est la plus puissante, mais n'est pas toujours accessible aux attaquants.

Pour comprendre complètement le problème, il faut aussi connaître l'architecture des services d'urgence (section 1.2) sur l'Internet. Son cadre général figure dans le RFC 6443. Les bonnes pratiques à suivre pour faire un service d'urgence qui marche sont dans le RFC 6881. Ces services d'urgence nécessitent des informations sur l'appelant (comme sa localisation, qu'il n'a pas toujours le temps ou la possibilité de donner, lorsqu'il est en situation d'urgence). Lorsqu'un service d'urgence reçoit l'appel, il doit donc déterminer la localisation, en déduire à qui transmettre l'appel (ce qu'on nomme un PSAP pour "*Public Safety Answering Point*") et router l'appel (en SIP, transmettre un `INVITE`, contenant la localisation, cf. RFC 6442).

Le problème de tout service d'urgence, ce sont les faux appels. Ils existent depuis bien avant l'Internet. Comme ils détournent les services d'urgence des vrais appels, ils peuvent littéralement tuer, si quelqu'un qui avait besoin d'un secours urgent ne l'obtient pas car tous les services sont occupés à traiter des canulars. (Il est recommandé de consulter le document EENA sur les faux appels <`http://www.eena.org/ressource/static/files/2012_05_04-3.1.2.fc_v1.1.pdf`>.) Parmi les faux appels, l'un est particulièrement dangereux, le "*swatting*". Il doit son nom au SWAT états-unien et consiste à appeler les services de police en prétendant qu'il y a une situation d'extrême danger nécessitant de faire appel à la force (prise d'otages, par exemple). Cet appel amènera à un déploiement policier intense, style cow-boys, chez la victime. Le FBI a documenté ce phénomène <`http://www.fbi.gov/news/stories/2008/february/swatting020408`>. De telles actions étant sévèrement punies, les attaquants vont toujours essayer de cacher leur identité, par exemple en indiquant un faux numéro de téléphone, si leur fournisseur de services téléphoniques le permet. Plusieurs études ont montré que les faux appels étaient particulièrement nombreux si on ne pouvait pas authentifier l'appelant (cf. « "*Emergency services seek SIM-less calls block*" <`http://www.abc.net.au/elections/tas/2006/news/stories/1717956.htm?elections/tas/2006/`> » ou « "*Rapper makes thousands of prank 999 emergency calls to UK police*" <`http://www.digitaljournal.com/article/293796?tp=1`> »).

Place maintenant aux menaces sur la localisation. Le RFC 6280 décrit une architecture pour des services de localisation intégrant la notion de vie privée. D'autres RFC décrivent les exigences de tout service de localisation (RFC 3693), les menaces contre eux (RFC 3694), le cas particulier des services d'urgence (RFC 5069), et l'usurpation des numéros de téléphone (RFC 7375).

Notre RFC s'attaque aux menaces en distinguant d'abord trois classes d'attaquants :
— Les attaquants externes, ne disposant d'aucun privilège particulier,
— Les attaquants situés dans l'infrastructure de téléphonie, et qui en contrôlent une partie, par exemple le LIS ("*Location Information Server*"),
— Les attaquants situés sur la machine de l'utilisateur.

Évidemment, les deux dernières classes peuvent faire des dégats plus facilement.

Outre la tricherie sur son numéro de téléphone, un attaquant peut aussi tricher sur sa localisation, soit en en inventant une de toutes pièces, soit en « rejouant » une localisation authentique, mais dans le passé ou encore en « volant » une localisation authentique mais d'un autre utilisateur. Ce RFC se focalise sur ces risques liés à la localisation mais la tricherie sur l'identité n'est pas à oublier. En effet, l'auteur des faux appels cherche en général à éviter les représailles, et donc à dissimuler son identité, par exemple en appelant d'une cabine téléphonique.

Maintenant, que peut-on faire pour limiter les risques (section 3) ? Il y a trois mécanismes principaux :

— Signer les informations de localisation (les fichiers PIDF-LO décrits dans le RFC 4119) au départ de l'appel. Aucune norme n'existe pour cela.
— Obtention de la localisation, non pas via l'émetteur mais depuis le récepteur, via le RFC 6753, en utilisant le protocole HELD ("*HTTP-Enabled Location Delivery*") RFC 5985. Dans ce cas, le destinataire de l'appel, le PSAP (le service d'urgence), contacte le serveur de localisation, le LIS.
— Obtention de la localisation, non pas via l'émetteur mais via le réseau (plus exactement un mandataire dans le réseau), en utilisant le RFC 6442. Cette dernière technique, elle, impose la participation du FAI (qui connait la localisation physique de ses abonnés, même si c'est avec une précision limitée, surtout pour les mobiles).

Une fois obtenue la localisation, encore faut-il en évaluer la fiabilité. Ce niveau de fiabilité est une information cruciale pour le processus de décision. Par exemple, un appel d'urgence où la localisation est marquée comme « absolument sûre » peut être traité instantanément, alors qu'on passera un peu plus de temps à vérifier un appel depuis une localisation douteuse (section 4). La localisation dépend d'un certain nombre de partenaires, et cette fiabilité va donc varier selon la confiance qu'on accorde à ces partenaires. Par exemple, dans le deuxième mécanisme cité plus haut (le PSAP interroge le LIS), si le LIS est connu, de confiance, et qu'on l'utilise depuis longtemps avec succès, on se fiera facilement à lui. À l'inverse, dans le cas du troisième mécanisme (interrogation d'un mandataire géré par le FAI), s'il y a eu peu d'appels d'urgence depuis ce FAI et qu'on n'a jamais pu vérifier la fiabilité de ses informations, la localisation sera marquée comme douteuse.

Pour déterminer la validité des informations de localisation, on peut aussi faire des vérifications croisées. Lors d'un appel SIP, une fois qu'on a reçu une localisation physique de l'émetteur, on peut comparer avec la localisation qu'indique l'adresse IP dans les champs `Via:` ou `Contact:`, ou celle dans les paquets de données. Si les deux localisations coïncident, on est rassuré. Sinon, on note la localisation comme étant douteuse.

La section 5 résume tous les problèmes de sécurité liés à la localisation fiable. Il faut notamment se rappeler que cette fiabilité peut être en opposition avec d'autres critères de sécurité, comme la protection de la vie privée (la section 6 détaille ce problème). D'autre part, toutes les mesures envisagées ne sont guère efficaces face au problème spécifique de l'attaque par déni de service : un attaquant qui effectuerait un très grand nombre d'appels pourrait toujours perturber le PSAP (le service d'urgence), ne serait-ce que via les vérifications faites. Effectuer un tel nombre d'appels est évidemment plus facile avec la téléphonie sur IP qu'avec le téléphone traditionnel. Et cela permet plus facilement de franchir les frontières, pour attaquer les services d'urgence d'un autre pays.

Ces appels en masse peuvent être faits par des zombies mais aussi par du code non sécurisé, par exemple un "*malware*" JavaScript, chargé automatiquement par le navigateur Web, et qui ferait des appels via WebRTC (RFC 8825). Il peut donc être prudent d'empêcher ce genre de code non sécurisé d'appeler les services d'urgence.

Pour analyser la résistance d'un service d'urgence aux attaques par déni de service, il faut séparer les cas des trois ressources finies dont disposent ces services : l'infrastructure informatique (réseaux et serveurs), les humains qui répondent à l'appel, et les services de secours eux-mêmes (police, pompiers, etc). Par exemple, si le réseau marche bien et que les preneurs d'appel répondent bien, mais qu'il n'y a plus aucun pompier disponible car tous sont partis combattre des incendies imaginaires, l'attaque par déni de service a malheureusement réussi. Les contre-mesures doivent donc veiller à traiter les cas d'abus de ces trois ressources. Par exemple, faire des vérifications automatiques poussées sur la vraisemblance de l'information de localisation va stresser la première ressource (l'infrastructure informatique) mais cela préservera les deux autres (qui sont souvent limitées : on n'a pas des ressources humaines abondantes et qualifiées).

Apparemment, il n'existe pas encore de mise en œuvre de ce système.