# RFC 7375 : Secure Telephone Identity Threat Model

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 octobre 2014

Date de publication du RFC : Octobre 2014

http://www.bortzmeyer.org/7375.html

---

Elle est loin, l'époque où l'Internet et le téléphone étaient deux mondes complètement séparés. Aujourd'hui, le téléphone n'est qu'une application parmi toutes celles tournant sur l'Internet. et les problèmes de sécurité du téléphone sont donc des problèmes Internet. D'où ce RFC qui décrit les menaces d'usurpation d'identité qui planent sur la téléphonie sur IP (cf. SIP, RFC 3261 [1]).

La plupart des attaques utilisant le téléphone commencent en effet par un mensonge sur le numéro d'appel : l'attaquant va se débrouiller pour présenter un numéro d'appel qui n'est pas le sien. Souvent, en effet, le numéro de l'appelant est utilisé pour mettre en œuvre une politique de sécurité : on décroche parce qu'on connait le numéro, ou bien on prend au sérieux un appel d'urgence parce qu'on sait qu'on pourra retrouver l'éventuel mauvais plaisant via son numéro ou encore on donne accès à un répondeur en n'utilisant pour toute authentification que le numéro d'appel. Bien sûr, quelqu'un qui ne veut pas révéler son numéro peut toujours ne pas le présenter. Mais beaucoup de correspondants ne décrocheront pas s'ils reçoivent un appel sans numéro. C'est pour cela que les spammeurs du téléphone préfèrent présenter un numéro, n'importe lequel. D'où la création du groupe de travail STIR <https://tools.ietf.org/wg/stir> de l'IETF, groupe qui est chargé de travailler sur ce problème (une description du problème figure dans le RFC 7340). Le but de STIR est de faire en sorte que, quand on voit un numéro entrant s'afficher, on soit raisonnablement sûr que ce soit bien un numéro que l'appelant est autorisé à utiliser.

On ne peut pas traiter le problème à la source : l'attaquant contrôle son téléphone et peut lui faire faire ce qu'il veut. Il faut donc traiter le problème dans le réseau téléphonique, ou bien à l'arrivée, et pouvoir distinguer les numéros autorisés des autres. Une fois qu'on aura cette distinction, on pourra appliquer les politiques de sécurité de son choix (par exemple ne pas décrocher si le numéro présenté n'est pas vu comme sérieusement authentifié).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3261.txt

Ce RFC se focalise sur la triche lors de l'appel. Une fois la connexion établie, d'autres attaques sont possibles (écouter le trafic en cours de route, rediriger les paquets IP vers une autre destination ou, tout simplement utiliser les nombreuses possibilités de SIP pour transférer un appel) mais elles nécessitent typiquement plus de moyens que l'usurpation de numéro, qui peut souvent être faite en n'ayant pas d'autres outils que son téléphone.

Autre piège qui n'est pas traité par le groupe STIR : des téléphones ont des fonctions de carnet d'adresses ou d'annuaire et peuvent donc afficher, à la place du numéro d'appel, le nom de la personne appelante. Cela permet d'autres attaques : par exemple, si l'annuaire n'est pas bien sécurisé, on peut imaginer que l'attaquant glisse un nom d'apparence légitime pour son numéro d'appel, et que le destinataire sera alors trompé, sans qu'il y ait eu usurpation de numéro. C'est une vraie possibilité mais elle nécessite des solutions très différentes (sécurisation des carnets d'adresse et des annuaires).

La section 2 de notre RFC décrit les différents acteurs. Il y a les utilisateurs, aux extrémités, avec leurs téléphones, simples engins sans trop de complications ou au contraire "*smartphones*" très riches. Il y a les intermédiaires, par exemple les relais SIP (on ne fait pas de la téléphonie en direct, en général, ne serait-ce que parce que le destinataire n'est pas forcément joignable en ce moment), et il y a les attaquants. Les intermédiaires peuvent modifier les caractéristiques de l'appel en cours de route, par exemple en jetant le numéro d'appel ou en substituant un autre. Ainsi, une passerelle entre la téléphonie IP et le PSTN pourra substituer au numéro indiqué dans un paquet IP son propre numéro, pour une meilleure traçabilité. Quant aux attaquants, on suppose qu'ils ont un téléphone (!) et peuvent passer un appel depuis le lieu de leur choix. Comme indiqué plus haut, ils peuvent indiquer un faux numéro (les téléphones traditionnels ne permettaient pas cela mais c'est possible avec les engins modernes). Pire, ayant accès à l'Internet, on suppose qu'ils peuvent envoyer des paquets IP quelconques, sans passer par un téléphone ou un "*softphone*". Enfin, notre RFC ne prend délibérement pas en compte le risque d'une trahison ou d'un piratage des intermédiaires. Certes, l'attaquant qui contrôlerait les serveurs intermédiaires pourrait faire beaucoup de dégâts mais ce n'est pas ce qui se fait aujourd'hui, dans la grande majorité des cas d'usurpation de numéro.

Après les acteurs, place aux attaques (section 3). L'attaquant peut chercher à usurper un numéro de téléphone donné (par exemple pour se faire passer pour une personne précise) ou bien il peut juste chercher à usurper n'importe quel numéro de téléphone valide (pour ne pas exposer le sien, qui permettrait de remonter jusqu'à lui). Un exemple du premier cas est celui de l'accès à une boîte vocale, lorsque l'authentification se fait uniquement sur la base du numéro présenté. Certes, il serait sans doute préférable d'utiliser (en plus, ou à la place du numéro présenté) une authentification plus forte mais, en pratique, un certain nombre de systèmes n'authentifient qu'avec le numéro appelant, surtout les services commerciaux comme la vidéoconférence où on ne souhaite pas trop embêter le client. Ajouter une authentification par, par exemple, un code numérique à taper, compliquerait les choses pour l'utilisateur. Si le système appelé pouvait savoir si le numéro de téléphone a été correctement authentifié, il pourrait, par exemple, n'imposer la frappe du code numérique que dans le cas où le numéro n'est pas fiable. Comme ces services sont souvent appelés de manière répétitive, on peut aussi compter sur l'historique, par exemple savoir s'il est normal ou pas que tel numéro entrant soit authentifié.

Et le spam, plaie du téléphone comme il l'est du courrier électronique ? Comment empêcher les appels automatiques ("*robocallers*") ? Pour éviter les plaintes, et qu'on remonte jusqu'à eux, les spammeurs ne veulent pas présenter leur vrai numéro. Par exemple, Bouygues Telecom m'appele toujours depuis une ligne qui ne présente pas le numéro d'appelant. Résultat, je ne décroche plus pour de tels appels. Les spammeurs ont donc intérêt à présenter un numéro, mais qui ne soit pas le leur. Leur tâche est donc plus facile que dans le cas précédent, où ils devaient usurper un numéro précis. Par contre, cette fois, l'appelé ne peut pas compter sur l'historique pour évaluer l'appel.

Un des problèmes de l'authentification des appels entrants est le manque de temps. Si c'est une machine qui est appelée (comme dans le cas précédent, celui du répondeur), on peut la faire patienter,

le temps qu'on vérifie. Si c'est un humain qu'il faut contacter, c'est plus délicat. Faut-il lui signaler un appel qu'on n'a pas encore eu le temps d'authentifier ? Cette nécessité d'agir en temps réel peut rendre certaines techniques (par exemple de longs calculs cryptographiques) difficiles à faire accepter. Les SMS n'ont pas ce problème : on peut retarder leur distribution sans conséquences sérieuses.

La téléphone connait aussi des attaques par déni de service. Un attaquant peut appeler simplement pour épuiser des ressources limitées, et déguiser alors son numéro pour éviter des représailles (ou tout simplement pour éviter d'être mis en liste noire). Il peut être capable d'utiliser plusieurs fournisseurs et plusieurs téléphones, pour faire une dDoS. Comme le "*robocaller*", l'attaquant qui vise un déni de service n'a pas besoin d'usurper un numéro de téléphone particulier. Tout numéro qui n'est pas le sien conviendra (il voudra probablement le faire varier rapidement, pour éviter les contre-mesures fondées sur des listes noires). Une exception est le cas de l'attaque par réflexion, où l'attaquant veut faire croire à la culpabilité d'un tiers, et usurpe donc le numéro de ce tiers.

Les contre-mesures sont donc les mêmes que pour les appels automatiques des spammeurs : vérifier que les numéros présentés sont des numéros possibles (cela bloque les attaques les moins sophistiquées, celles où l'attaquant met n'importe quoi au hasard), et traiter différemment les appels où on peut être sûr que les numéros sont légitimes (dans le cas d'une attaque, jeter systématiquement les numéros non garantis, par exemple). Un tel traitement différencié n'est toutefois pas acceptable pour les appels d'urgence, qui ont l'obligation de répondre à tout.

Et, pour finir le RFC, les scénarios d'attaque possibles (section 4). Si l'attaquant et sa victime (l'appelant et l'appelé) sont tous les deux en SIP, l'attaquant n'a qu'à mettre le numéro qu'il veut dans le champ `From:` de la requête SIP `INVITE`. Si les deux sont au contraires connectés au PSTN (la téléphonie traditionnelle), l'attaquant doit avoir le contrôle du PABX qu'utilise son téléphone. Le PABX envoie une requête Q.931 `SETUP` avec le numéro de son choix qui va se retrouver dans l'appel SS7, champ "*Calling Party Number*". Et si l'attaquant est en IP et la victime sur le PSTN ? Comme dans le premier cas, il met le numéro qu'il veut dans le message SIP et la passerelle IP¡-¿PSTN va le transmettre à l'appelé. Arrivé là, vous vous demandez sans doute quelles sont les solutions possibles à ces attaques, qui semblent si simples à faire ? Mais ce RFC ne fait que l'analyse des menaces, les solutions seront dans des RFC futurs.