Groupe de tarvail Réseau
Request for Comments : 3694
Catégorie : Information

Traduction Claude Brière de L'Isle

M. Danley & D. Mulligan,
Samuelson Law, Technology & Public Policy Clinic
J. Morris, Center for Democracy & Technology
J. Peterson, NeuStar
février 2004

Analyse des menaces sur le protocole Geopriv

Résumé
Le présent document fait une analyse des menaces contre l'architecture du protocole Geopriv. Il se concentre sur les menaces sur le protocole, les menaces qui résultent de la mémorisation des données par les entités de l'architecture, et les menaces posées par l'abus des informations données parGeopriv. Certaines propriétes de sécurité qui répondent à ces menaces sont énumérées comme référence aux exigences de Geopriv.

Table of Contents

1. Vue d'ensemble

La prolifération de services fondés sur la localisation qui intègrent des capacités de traçage et de navigation soulève des problèmes significatifs de confidentialité et de sécurité. De tels services pemettent aux utilisateurs d'identifier leur propre localisation ainsi que de déterminer la localisation d'autres usagers. Dans certains échanges d'homologue à homologue, l'identification des appareils a lieu automatiquement au sein d'un périmètre de localisation défini, informant les appareils homologues de l'identité et de la disponibilité d'un certain utilisateur. De plus, des échanges d'enregistrements de localisation peuvent révéler des informations significatives sur les habitudes, les tenants et aboutissants, et les associations des utilisateurs individuels.

Les exigences pour Geopriv permettent à l'objet de localisation (LO, *Location Object*) de prendre en charge une grande variété d'utilsations des informations de localisation (LI, *Location Information*) ; l'objet Geopriv lui-même est destiné à être technologiquement neutre, permettant à une grande variété d'appareils de fournir des LI sous la forme d'un LO. Geopriv exige aussi que de nombreuses classes de visionneurs soient capables de demander des LI à un serveur de localisation. Les exigences pour Geopriv tiennent compte des circonstances dans lesquelles la cible a une relation contractuelle avec les entités qui transmettent et reçoivent les LI et celles dans lesquelles aucun contrat n'existe. Exiger que l'objet Geopriv prenne

en charge une certaine technologie, relation cible-visionneur, ou cadre légal sous-jacent gouvernant le LI, complique la protection de la confidentialité et de la sécurité des LI.

Le présent document analyse les menaces aux LI dans la transmission et la mémorisation. La possibilité que les LI soient compromises par ces menaces varie selon les circonstances. Un serveur qui vend les informations de localisation à des démarcheurs potentiels fait peser un risque distinctement inférieur à ceux d'un intercepteur interne individuel de la localisation présente d'une cible pour commettre une attaque physique. Il est important que ces menaces soient prises en considération lorsque on travaille à la définition du LO.

Certaines des menaces discutées dans le présent document peuvent sortir du domaine d'application du mandat de Geopriv, par exemple, les menaces qui résultent de l'échec à satisfaire des obligations contractuelles. Néanmoins, une discussion complète des menaces est nécessaire pour identifier les propriétés de sécurité désirables et les contre-mesures qui vont améliorer la sécurité du LO, et par là mieux protéger les LI.

2. Domaine du protocole Geopriv

L'architecture Geopriv sera déployée dans l'Internet ouvert - dans un environnement de sécurité dans lequel des attaquants potentiels peuvent inspecter les paquets sur le réseau, imiter des adresses Internet, et lancer des attaques de déni de service à grande échelle. Dans certaines architectures, des portions du trafic Geopriv (en particulier le trafic entre le générateur de localisation et un serveur de localisation initial) peuvent se produire sur des réseaux gérés qui n'ont pas d'interface avec l'Internet public.

Le protocole lui-même suppose une interaction entre un certain nombre de rôles logiques, dont beaucoup seront normalement mis en œuvre sur des appareils répartis dans le réseau (une liste complète des rôles et entités Geopriv avec leurs definitions se trouve dans la [RFC3693]). Les points d'extrémité des transactions Geopriv courantes sont le générateur de localisation (la source des informations de localisation du point de vue du réseau) et le receveur de localisation. Un générateur de localisation et un receveur de localisation peuvent tous deux avoir une relation avec un serveur de localisation ; le générateur de localisation publie des données sur un serveur de localisation (qui peut fournir une fonction d'intendance/filtrage pour les informations de localisation) et le receveur de localisation demande et/ou reçoit les informations du serveur de localisation. Cela donne deux points où les informations Geopriv requièrent une protection à travers le réseau. Des règles peuvent aussi être passées sur le réseau d'un détenteur de règle à un serveur de localisation ; cela donne un autre point où l'architecture requiert la sécurité.

Il est important de noter que les générateurs de localisation et les receveurs de localisation peuvent être mis en œuvre sur des appareils bon marché pour lesquels une forte sécurité cryptographique est actuellement interdite par les coûts du calcul.

3. Motivations de l'attaquant de Geopriv

La motivation la plus évidente pour un attaquant de Geopriv est d'apprendre la localisation d'un sujet qui souhaite garder sa position confidentielle, ou même pour des visionneurs autorisés de s'assurer des informations de localisation avec un degré de précision supérieur à ce que le faiseur de règles désire. Cependant, il y a plusieurs autres motivations potentielles qui posent problème. Les attaquants peuvent aussi souhaiter empêcher que la localisation d'une cible soit distribuée, ou modifier ou corrompre les informations de localisation afin de fausser la localisation de la cible, ou de rediriger les informations de localisation de la cible sur un tiers qui n'est pas autorisé à conaître ces informations. Les attaquants peuvent vouloir identifier les associés d'une cible, ou apprendre les habitudes ou routines d'une cible. Les attaquants peuvent vouloir apprendre l'identité de toutes les parties qui sont dans une certaine localisation. Finalement, des attaquants peuvent simplement vouloir bloquer le fonctionnement d'un système Geopriv entier à travers des attaques de déni de service.

Il y a aussi une classe d'attaquants qui peuvent être autorisés comme participants légitimes dans un échange de protocole Geopriv mais qui abusent des informations de localisation. Cela inclut la distribution ou l'accumulation des informations de localisation en dehors des paramètres de l'accord entre les principaux, éventuellement pour des raisons commerciales ou comme un acte de surveillance illégale.

4. Attaques représentatives contre Geopriv

4.1 Attaques contre le protocole

4.1.1 Espionnage et/ou interception

Imaginons un jeu informatique fondé sur la localisation, inspiré du jeu de cache cache traditionnel, dans lequel un serveur centralisé fournit des indications sur la localisation du "caché" à un ensemble de "chercheurs". Les chercheurs ont accès à des données de localisation très grossières, tandis qu'un seul arbitre est donné pour l'accès aux informations de localisation non filtrées et précises du caché. Chaque chercheur a un appareil sans fil (dans l'architecture Geopriv, un receveur de localisation) qui l'alimente en données de positionnement grossières provenant du serveur de localisation. Le caché porte un appareil (un générateur de localisation employant le GPS) qui transmet les informations de localisation au serveur de localisation.

Si un des chercheurs souhaite tricher en attaquant le protocole Geopriv, il y a un certain nombre de façons de monter une telle attaque dans le but d'apprendre la localisation précise du caché. Ce peut être en espionnant sur une des deux connexions réseau – soit la connexion entre le générateur de localisation et le serveur de localisation, soit la connexion entre le serveur de localisation et le receveur de localisation de l'arbitre (qui reçoit les informations précises). Ce peut être aussi en tentant de se faire passer pour l'arbitre auprès du serveur de localisation, afin de recevoir les informations de localisation non filtrées. Autrement, on peut se faire passer pour le serveur de localisation auprès du générateur de localisation porté par le caché, ce qui lui donnerait aussi l'accès aux informations de localisation précises. Finalement, le tricheur pourrait tenter d'agir comme faiseur de règles, fournissant comme cela des règles au serveur de localisation qui lui permettraient de recevoir les informations de localisation non floutées.

De ces menaces, on peut déduire le besoin de plusieurs propriété de sécurité de l'architecture.
- o La confidentialité est nécessaire sur les deux connexions entre le générateur de localisation et le serveur de localisation, ainsi que entre le serveur de localisation et tout receveur de localisation.
- o Le serveur de localisations doit être capable d'authentifier et autoriser les receveurs de localisations pour empêcher les usurpations d'identité.
- o De même, les générateurs de localisations doivent être capables d'authentifier et autoriser les serveurs de localisations afin d'empêcher les usurpations d'identité.
- o Finalement, le serveur de localisation doit être capable d'authentifier les faiseurs de règles, pour s'assurer que des parties non autorisées ne peuvent pas changer les règles.

4.1.2 Usurpation d'identité

Considérons un cas dans lequel le même patron emploie deux rivaux. Un va en voyage d'affaires à Cleveland. Les deux rivaux portent des appareils qui sont tracés par un générateur de localisation (comme des téléphones cellulaires que l'opérateur peut trianguler) et les deux rivaux permettent à leur patron d'avoir accès à leurs (grossières) informations de localisation. Le rival qui est resté à la maison veut pirater le protocole Geopriv pour faire apparaître que le rival en voyage est en fait en train de se prélasser à la plage plutôt que de participer à l'ennuyeuse conférence technique à Cleveland. Comment va t-il monter une telle attaque ?

L'attaquant peut tenter d'usurper le trafic réseau du générateur de localisation au serveur de localisation (en particulier si, par des moyens comme une attaque de déni de service, le générateur de localisation devient incapable de produire ses propres rapports). Le but de l'attaquant peut être de fournir des informations de localisation falsifiées appropriées pour quelqu'un qui se trouve à Miami, ou peut-être même de répéter un authentique objet de localisation provenant d'une visite antérieure du rival à Miami. L'attaquant peut aussi essayer d'usurper le trafic du serveur de localisation au patron du receveur de localisation.

De ces menaces, on peut déduire un besoin de plusieurs propriétés de sécurité de l'architecture :
- o il est nécesaire que le serveur de localisation authentifie le générateur de localisations,
- o le receveur de localisations doit être capable d'authentifier le serveur de localisations,
- o les informations de localisation doivent être protégées contre les attaques en répétition.

L'usurpation d'identité peut créer des menaces supplémentaires lorsque le protocole est attaqué. Dans de nombreuses circonstances, l'identité du visionneur est la base du contrôle de si les LI sont révélées et, si il en est ainsi, comment les LI sont filtrées. Si l'identité de cette entité est compromise, la confidentialité est menacée. Quiconque à l'intérieur ou à l'extérieur de la transaction est capable de se faire passer pour une entité autorisée peut obtenir l'accès à des informations confidentielles, ou d'initier de fausses transmissions au nom de l'entité autorisée. La capacité d'usurper l'identité du receveur de localisation, par exemple, va créer le risque qu'une entité non autorisée accède à la fois à l'identité et à la localisation de la cible au moment où le LO est envoyé.

4.1.3 Rassemblement des informations

L'espionnage et l'interception peuvent aussi créer des menaces d'analyse de trafic lorsque l'intercepteur collecte plus de données au fil du temps. Les menaces d'analyse de trafic sont renforcées par la détermination par l'espion, à partir du fait même d'une transmission réseau, des relations entre les diverses entités impliquées. Si un employeur envoie la localisation d'un employé à un client, un espion pourra déterminer que ces trois entités sont en train d'iuteragir avec quelqu'un d'autre. Si l'espionnage se poursuit dans le temps, la collecte des interactions va impliquer l'employeur, les employés, et tous leurs clients. Une telle masse d'informations va révéler que l'employeur et l'employé sont fréquemment associés à un autre, et va révéler quels clients traitent le plus fréquemment avec cette paire. Donc, la menace d'analyse de trafic crée le risque que les espions déterminent les associés de la cible.

L'analyse de trafic peut aussi permettre à un espion de s'assurer de l'identité ou des caractéristiques des cibles dans une localisation particulière. En observant les transmissions entre les générateurs de localisations dans une localisation particulière et des serveurs de localisations (peut-être en espionnant sur un LAN sans fil ou filaire dédié à la localisation en question) et en suivant éventuellement les données jusqu'aux divers receveurs de localisations, un attaquant peut être capable d'apprendre qui sont les associés, incluant l'employeur, des cibles de cette localisation, et peut-être d'extrapoler les informations d'identité.

Si les espions sont capables d'intercepter non seulement un LO chiffré, mais les LI en texte source elles-mêmes, d'autre menaces sont présentes. Retournons à l'exemple ci-dessus de l'employeur qui demande les informations de localisation d'un employé. Dans cette instance, l'interception d'une de ces transactions passées peut révéler l'identité et/ou les localisations des trois parties impliquées en plus de révéler leur association. Dans des circonstances où il y a un fichier de ces données, cependant, l'analyse pourrait révéler tous les chemins réguliers empruntés par l'employé pour visiter les clients, une zone générale dans laquelle l'employé travaille, les identités et localisations de la base de client complète des employés, et des informations sur les relations entre les entités.

Les menaces fondées sur l'analyse de trafic sont difficiles à concilier avec des mesures de sécurité du protocole, mais il est important de les noter.

À partir de ces menaces on peut déduire le besoin de plusieurs propriétés de sécurité de l'architecture :
- o le faiseur de règles doit être capable de définir des règles concernant l'utilisation des LI,
- o la connexion entre le générateur de localisation et le serveur de localisation, et la connexion entre le serveur de localisation et le receveur de localisation doivent rester confidentielles,
- o le serveur de localisations doit être capable d'authentifier le receveur de localisations pour empêcher l'usurpation d'identité,
- o le serveur de localisations doit être capable d'authentifier les faiseurs de règles pour s'assurer que des entités non autorisées ne peuvent pas changer les règles.

4.1.4 Déni de service

Les parties qui souhaitent priver des réseaux entiers du service Geopriv, plutôt que juste cibler des usagers particuliers, vont probablement concentrer leurs efforts sur le serveur de localisation. Comme dans de nombreux scénarios le serveur de localisation joue le rôle central de gestion de l'accès aux informations de localisation pour de nombreux appareils, il est dans une telle architecture le seul point naturel de défaillance.

Le protocole Geopriv paraît avoir quelques opportunités d'amplification des attaques. Lorsque le générateur de localisation publie les informations de localisation, le serveur de localisation agit comme un exploseur, livrant potentiellement ces informations à de nombreuses cibles. Si le générateur de localisation devait fournir des mises à jour très rapides de position (autant que la vitesse de liaison pourrait accommoder, en particulier dans des environnements sans fils à haut débit) lorsque le serveur de localisation relaye les informations aux chercheurs à un débit similaire, cela pourrait alors devenir problématique lorsque de grands nombres de chercheurs traquent le même usager.

Noter aussi que la plupart des opérations associées au serveur de localisation exigent probablement une authentification cryptographique. Les opérations cryptographiques impliquent un coût de calcul de la part du serveur de localisation. Cela pourrait fournir un moyen attrayant pour des attaquants d'inonder le serveur de localisation avec des informations Geopriv fantoches qui seraient maquillées pour apparaître comme provenant d'un générateur de localisation, d'un receveur de localisation, ou d'un faiseur de règles. Parce que le serveur de localisation doit dépenser des ressources pour vérifier les accréditifs présentés par ces messages Geopriv, des inondations d'informations Geopriv pourraient avoir un plus fort impact que des attaques de déni de service fondées sur une inondation de paquets génériques.

De ces menaces, on peut déduire un besoin de plusieurs propriétés de sécurité de l'architecture :

- o les serveurs de localisations doivent utiliser des défis d'authentification sans état et des mesures similaires pour s'assurer que les tentatives d'authentification ne vont pas consommer inutilement les ressources du système,
- o le faiseur de règles doit être capable de provisionner des politiques qui limitent le taux d'envoi des informations de localisation pour empêcher les attaques d'amplification.

4.2 Attaques contre les hôtes

4.2.1 Données mémorisées aux serveurs

Les LI conservées dans un serveur sont sujettes à de nombreux risques potentiels. D'abord, il peut y avoir une mauvaise utilisation accidentelle des LI par le serveur. Que ce soit par négligence, inattention, ou ignorance, le serveur peut accidentellement livrer des LI au mauvais receveur de localisation, ou échouer à filtrer correctement les LI qu'il envoie. Ensuite, le serveur peut intentionnellement faire un mauvais usage des LI. Un serveur peut décider de vendre un "profil" qu'il a compilé d'une cible ou receveur de localisation en dépit des dispositions contraires de la règle du faiseur de règles. Autrement, un individu qui travaille pour le serveur peut, pour son gain personnel, mésuser de l'accès au serveur pour obtenir les LI. Troisièmement, même avec le serveur le plus sécurisé et de confiance, il y a un risque que quelqu'un d'extérieur au système s'y introduise afin de récupérer les LI. Enfin, il y a aussi un potentiel que quelqu'un utilise le système légal pour soutirer des enregistrements sur un individu à un serveur. Un tel processus résulterait probablement en la révélation des informations de localisation de la cible sans notification à la cible ou le consentement de la cible.

Les données mémorisées au serveur peuvent révéler la localisation présente de la cible si les données sont utilisées ou interceptées au moment ou à proximité du moment de transmission. Si une cible demande une carte de sa localisation présente à un magasin du voisinage, et si le serveur de localisation envoie cette information au mauvais receveur de localisation, le visionneur pourrait savoir l'identité de la cible, la localisation actuelle de la cible, et la localisation où la cible pourrait se diriger.

Les données mémorisées au serveur de localisation peuvent aussi créer beaucoup des menaces d'analyse de trafic discutées au paragraphe 4.1. Si l'accès est obtenu non seulement du fait de la transmission du LO, mais aussi des LI transmises, quiconque a accès à ces informations peut constituer un historique des lieux de présence de cette cible, pendant combien de temps, et avec qui.

4.2.2 Données mémorisées dans les appareils

Parce que Geopriv doit travailler avec tous les types de technologies ou appareils, il est difficile de déterminer le potentiel particulier de menace des appareils individuels. Par exemple, tout appareil qui tient un journal des demandes de localisation envoyées, ou des LO reçus, va présenter une menace similaire pour les informations conservées chez un serveur de localisation, discutées précédemment. Une ordonnance judiciaire ou mandat pour l'appareil d'un individu pourrait de plus révéler un journal similaire.

De plus, selon l'appareil, il y a toujours une possibilité que les données soient compromises d'une certaine façon. Pour un appareil avec un écran, il est toujours possible qu'un autre individu ait l'opportunité de voir l'affichage de l'appareil sans que l'usager le sache. Un appareil qui donne un retour verbal (c'est-à-dire, qui donne des directives aux aveugles) crée un potentiel supplémentaire de compromission des LI. Si la cible/visionneur se trouve dans un endroit public et demande des directives à partir du domicile de la cible à une autre localisation, quiconque peut entendre le résultat de l'appareil peut être capable de déterminer l'identité de la cible, sa résidence, et éventuellement la localisation sur lesquelles elles sont dirigées.

De plus, si l'appareil a conservé des informations de localisation et si l'appareil est perdu ou volé, quelqu'un d'autre que le faiseur de règles pourrait éventuellement accèder aux informations disant quelles LI ont été envoyées et quant, ainsi qu'éventuellement la localisation de la cible durant chaque transaction. De telles informations pourraient permettre à une entité de déterminer des informations privées significatives sur la base de à qui le propriétaire de l'appareil s'est associé dans le passé, ainsi que chaque localisation où la cible a été et pendant combien de temps.

4.2.3 Données mémorisées chez le visionneur

Les menaces posées ici sont similaires à celles discutées ci-dessus en relation avec les serveurs et appareils de localisation. Le principal objet de la séparation des menaces posées par les données mémorisées chez le visionneur est de montrer que, selon la complexité de la transaction et les autres entités impliquées, la mémorisation des données en divers points de la transaction peut donner lieu aux mêmes types de risques pour la confidentialité.

4.2.4 Informations contenues dans les règles

Dans de nombreuses instances, les règles que crée un faiseur de règles vont révéler des informations sur le faiseur de règles ou sur la cible. Une règle qui dégrade toutes les informations envoyées d'approximativement 25 kilomètres peut dire à un intercepteur comment déterminer la vraie localisation de la cible. Une règle qui déclare, "Dire à mon patron dans quelle pièce je suis quand je suis dans le bâtiment, mais quand je suis sorti du bâtiment entre 9 heures et 17 heures. lui dire que je suis dans le bâtiment" révèlerait beaucoup plus que ce que la plupart des employés désireraient. Tout patron qui serait le receveur de localisation et recevrait des LI spécifiant "dans le bâtiment" réaliserait alors que l'employé est ailleurs.

De plus, si une entité a accès au journal des données au serveur de localisation ou sur un appareil, la connaissance du contenu des règles lui permettrait une sorte de "décodage" des informations de localisation de l'appareil en quelque chose de plus précis. Donc, mon patron pourrait non seulement dire où je suis à cet instant, mais pourrait dire pendant combien de temps durant l'année écoulée j'ai été en dehors du bâtiment entre 9 heures et 17 heures.

Les règles elles-mêmes peuvent aussi révéler des informations sur la cible. Une règle comme celle ci-dessus va clairement révéler la relation d'emploi entre les deux individus, ainsi que le fait que l'employé cache quelque chose à l'employeur.

En combinaison avec d'autres informations, les informations de localisation peuvent permettre l'identification de la cible.

4.3 Attaque contre l'usage

4.3.1 Menaces posées par la sur-collecte

Des règles de confidentialité par défaut faibles ou absentes compromettraient aussi les LI. Sans règle par défaut pour les LO, il est probable que par défaut un grand nombre d'appareils révèleraient les LI. Les règles de confidentialité devraient contrôler la collecte, l'utilisation, la divulgation, et la rétention des informations de localisation. Ces règles doivent se conformer à des pratiques d'information équitables – ces pratiques sont exposées au paragraphe 5.1.

Alors que des utilisateurs techniquement expérimentés d'appareils peuvent créer des règles de confidentialité pour protéger leurs LI, de nombreux individus ne vont pas avoir les connaissances ou la motivation pour le faire. Donc, en face de leur propre appareil, de nombreux individus vont probablement rester sans règle de confidentialité pour leurs LI. Cela va alors laisser les LI de ces utilisateurs entièrement vulnérables aux diverses attaques. Des règles par défaut sont nécessaires pour traiter ce problème.

Sans règles par défaut, par exemple, un appareil peut signaler n'importe qui dans le voisinage à des intervalles réguliers, répondre à n'importe qui dans les environs qui l'interroge, ou envoyer des signaux à des entités inconnues.

Le manque d'une règle par défaut disant "ne pas redistribuer" permettrait au serveur de localisation de passer les informations de localisation de la cible à d'autres. L'absence d'une règle par défaut limitant la rétention des LI pourrait augmenter le risque présenté par une utilisation inappropriéte et l'accès aux données mémorisées.

Bien que la définition de règles de confidentialité par défaut sorte du domaine d'application du présent document, des règles par défaut sont nécessaires pour limiter les risques présentés pour la confidentialité par l'utilisation des services et appareils qui utilisent des LI.

5. Contre-mesures pour les violations d'usage

5.1 Pratique d'information équitables

Les principes des pratiques d'information équitables exigent des entités qui traitent des informations personnelles qu'elles satisfassent à certaines obligations par rapport à leurs collecte, utilisation, maintenance et sécurité, et donnent aux individus dont les informations personnelles sont collectées certains droits de regard sur le traitement de leurs informations. Les pratiques d'information équitables sont conçues pour empêcher des menaces spécifiques présentées par la collecte des informations personnelles sur les individus. Pour cette raison, les pratiques d'information équitables sont des "contre-mesures" qui devraient être reflétées dans les systèmes techniques qui traitent les informations personnelles et les règles qui gouvernent leur utilisation. Une brève discussion des pratiques d'information équitables peuvent être bénéfiques pour formuler les exigences pour le LO.

Il y a sept principes majeurs des pratiques d'information équitables :

1. Ouverture : l'existence d'un système de conservation des enregistrements pour les informations personnelles doit être connue, ainsi qu'une description de l'objet et l'utilisation principale des données. Donc, toute entité qui collecte des LI devrait informer les individus que ces informations sont collectées et les informer sur la raison de la collecte des LI. L'ouverture est conçue pour empêcher la création de systèmes secrets.

2. Participation individuelle : les individus devraient avoir le droit de voir toutes les informations collectées sur eux, et d'être capables de corriger ou supprimer les données qui ne sont pas à jour, correctes, pertinentes, ou complètes. La pratique de la participation individuelle tient compte du fait que parfois les informations qui sont collectées peuvent être inexactes ou inappropriées.

3. Limitation de collecte : les données devraient être collectées par des moyens légaux et équitables et devraient être collectées, lorsque c'est approprié, en toute connaissance ou consentement du sujet. La collecte des données devrait être minimisée à ce qui est nécessaire pour prendre en charge la transaction. Poser des limites à la collecte aide à protéger les individus des dangers de la sur-collecte – à la fois en termes de collecte de trop d'informations, et de collecte d'informations pendant trop longtemps.

4. Qualité des données : les données personnelles devraient être pertinentes pour l'objet pour lequel elles sont collectées et utilisées ; les informations personnelles devraient être précises, complètee, et à jour. L'exigences de qualité des données est conçue pour empêcher les sortes de dommages particuliers qui peuvent découler de l'utilisation (appropriée ou non) d'informations personnelles.

5. Finalité : il devrait y avoir des limites à l'utilisation et à la divulgation de données personnelles : les données devraient n'être utilisées que pour les besoins spécifiés au moment de la collecte ; les données ne devraient pas être utilisées ou divulguées autrement sans le consentement du sujet des données ou d'une autre autorité légale. Un consommateur qui fournit des LI à une entreprise afin d'en recevoir des directives, par exemple, ne fournit pas ces informations pour autre chose. L'entreprise ne devrait alors utiliser ces LI que pour fournir des directives, et pas pour d'autres objets.

6. Sécurité : les données personnelles devraient être protégées par des souvegarde de sécurité raisonnables contre des risques comme la perte, l'accès non autorisé, la destruction, l'utilisation, la modification, ou la divulgation. Alors que certaines mesures de sécurité peuvent être prises en-dehors du LO (c'est-à-dire, en limitant l'accès des employés aux serveurs de localisation) d'autres mesures peuvent être prises à travers le LO ou les applications de LO.

7. Responsabilité : ceux qui tiennent des registres de données personnelles devraient être responsables du respect des pratiques d'information équitables. Il sera normalement plus facile à un individu de mettre en œuvre ces pratiques si elles sont explicitement écrites – soit dans les règles écrites par le faiseur de règles, soit dans les contrats entre l'individu et une entité de confiance.

6. Propriétés de sécurité du protocole Geopriv

Les contre-mesures suggérées ci-dessous reflètent les menaces discutées dans le présent document. Il y a donc un certain recouvrement entre les propriétés de sécurité proposées ci-dessous, et les exigences de la [RFC3693].

6.1 Les règles comme contre-mesures

Les paragraphes qui suivent sont destinés à illustrer que dans de nombreuses instances les menaces sur les LI peuvent être limitées par des règles claires, inévitables, déterminées par les faiseurs de règles.

6.1.1 Le faiseur de règles devrait définir les règles

Le faiseur de règles pour un certain appareil va généralement être l'utilisateur, ou le propriétaire, de l'appareil. Dans certaines circonstances, le faiseur de règles peut être ces deux entités. Selon l'appareil, le faiseur de règles peut être ou non l'individu le plus étroitement aligné sur la cible. Par exemple, un enfant qui porte un téléphone cellulaire peut être la cible, mais les parents de cet enfant seront probablement le faiseur de règles pour l'appareil. Donner le contrôle au faiseur de règles est une opportunité potentielle de conforter la composante consentement de la limitation de collecte et des principes de finalité discutés ci-dessus.

6.1.2 Geopriv devrait avoir des règles par défaut

Parce que certains faiseurs de règles peuvent n'être pas informés du rôle des règles dans la divulgation de leurs LI, Geopriv devrait inclure des règles par défaut. Le faiseur de règles est, bien sûr, toujours libre de changer ses règles pour fournir plus ou moins de protection. Pour protéger la confidentialité et la sûreté physique, les règles par défaut devraient, au minimum, limiter la divulgation et la rétention des LI.

Les règles par défaut sont aussi nécessaires pour ce qu'on appelle un générateur de localisations (LG) "sourd". Si un LG est

incapable de déterminer les règles établies par le faiseur de règles avant de publier le LO sur un serveur de localisation, il est important que des règles par défaut protègent ce LO en transit, et assurent que le LO n'est finalement envoyé qu'au receveur de localisations autorisé. Ces règles de LG par défaut vont aider à empêcher beaucoup des menaces discutées dans ce document. Le faiseur de règles devrait être capable de déterminer le contenu de ces règles par défaut à tout moment.

6.1.3 Le receveur de localisation ne devrait pas être informé de toutes les règles

Un visionneur ne devrait pas être informé de toutes les règles définies par le faiseur de règles. Le visionneur a seulement besoin de connaître les règles qu'il doit respecter (c'est-à-dire, celles qui concernent son utilisation et la rétention des LI). Les autres règles, comme celles qui spécifient la précision ou le filtrage des LI, ou les règles qui ne couvrent pas l'interaction concernée ne devraient pas être révélées au visionneur. Cette contre-mesure est cohérente avec le composant de minimisation du principe de limitation de la collecte et assure que le faiseur de règles révèle seulement ce qu'il a l'intention de révéler.

6.1.4 Certaines règles devraient voyager avec l'objet de localisation

La sécurité des LI au niveau de l'appareil est un peu compliquée, car le faiseur de règles n'a pas de réel contrôle sur ce qui est fait des LI une fois arrivées au receveur de localisation. Si certaines règles voyagent avec le LO, le faiseur de règles peut encourager la conformité du visionneur à ses règles. Potentiellement, une règle pourrait voyager avec le LO et indiquer quand il est temps de purger les données, empêchant la compilation d'un "journal" des LI de la cible sur tous les appareils impliqués dans la transmission du LO. Permettre aux règles de voyager avec le LO a le potentiel de limiter l'opportunite d'attaques d'analyses de trafic.

6.2 Protection des identités

Les identités sont un composant extrêmement important du LO. Bien que dans de nombreuses instances, une certaine forme d'identification de la cible, du faiseur de règles, et du visionneur soit nécessaire pour l'authentification, il y a diverses méthodes pour séparer ces "accréditifs" d'authentification de la véritable identité de ces appareils. Ces contre-mesures sont particulièrement utiles en ce que la compromission d'un journal des LI, quelle qu'en soit la source, est moins menaçante pour la confidentialité lorsque l'identité de la cible est cachée.

6.2.1 Des identifiants à courte durée de vie peuvent protéger l'identité de la cible

Des identifiants à courte durée de vie vont permettre au protocole utilisateur de cacher la véritable identité du faiseur de règles et de la cible au serveur de localisations ou au receveur de localisations. Ces identifiants vont quand même permettre l'authentification, assurant que seul un receveur de localisations approprié reçoit le LO. En même temps, cependant, abréger la durée de vie de ces identifiants aide à empêcher toute association de la vraie identité d'une cible à des habitudes et associés particuliers.

6.2.2 Des pseudonymes sans lien peuvent protéger l'identité des receveurs de localisation

Les pseudonymes sans lien protègent l'identité du receveur de localisations de la même manière que les identifiants à courte durée de vie protègeraien l'identité de la cible. Lorsque on utilise les deux, tout enregistrement d'une transaction qu'a un serveur de localisation va avoir deux "accréditifs" associés à une transmission de LI : un lié à la cible et un lié au receveur de localisation. Ces accréditifs vont permettre au serveur de localisation d'authentifier la transmission sans avoir jamais connaissance des vraies identités des individus associés à chaque côté de la transaction.

6.3 Sécurité de la transmission des données

Les attaques décrites dans le présent document motivent les propriétes de sécurité suivantes pour les connexions entre le générateur de localisation et le serveur de localisation, le serveur de localisation et le faiseur de règles, et le serveur de localisation et le receveur de localisation :

6.3.1 Les règles peuvent interdire une certaine fréquence de demandes

Le faiseur de règles peut être capable d'établir une règle qui interdit un certain nombre de demandes faites dans un délai spécifique. Ce type d'arrangement va permettre au faiseur de règles d'empêcher que des attaquants détectent les schémas dans des données rendues aléatoirement plus grossières. Pour un receveur de localisation qui n'est pas "de confiance", par exemple, à qui le faiseur de règles veut révéler seulement les LI grossies au niveau de la ville, une seule demande sera honorée toutes les deux heures. Cela va empêcher le receveur de localisations d'envoyer des demandes répétées pour

obtenir des informations de présence plus précises.

De même, des seuils de notifications d'informations de localisation peuvent aider à combattre les attaques d'amplification.

6.3.2 Authentification mutuelle de point d'extrémité

L'authentification est cruciale pour la sécurité des LI durant la transmission. Le serveur de localisation doit être capable d'authentifier le receveur de localisations pour empêcher l'usurpation d'identité. Le générateur de localisations doit être capable d'authentifier le serveur de localisations pour s'assurer que les informations de localisation brutes ne sont pas envoyées à des entités inappropriées. De plus, le serveur de localisations doit être capable d'authentifier les faiseurs de règles pour s'assurer que des entités non autorisées ne peuvent pas changer les règles.

6.3.3 Intégrité & confidentialité de l'objet de données

Le LO doit conserver son intégrité en tous les points de communication entre le serveur de localisations et le receveur de localisations. La confidentialité est requise sur les deux connexions entre le générateur de localisation et le serveur de localisation, et entre le serveur de localisation et tout receveur de localisation. La confidentialité des règles envoyées sur le réseau au serveur de localisation est d'une importance comparable.

6.3.4 Protection contre la répétition

La protection contre la répétition empêche un attaquant de capturer un élément particulier d'informations de localisation et de le rejouer ultérieurement afin de convaincre les visionneurs d'une localisation erronée de la cible. Les receveurs de localisation et les serveurs de localisation, selon leurs capacités, peuvent tous deux avoir besoin de protection contre la répétition.

7. Considérations pour la sécurité

Ce document d'information caractérise les menaces potentielles contre la sécurité qui ciblent l'architecture Geopriv.

8. Considérations relatives à l'IANA

Le présent document n'introduit aucune considération relative à l'IANA.

9. Références

[RFC3693] J. Cuellar et autres, "Exigences pour Geopriv", février 2004. *(Information)*

10. Adresse des auteurs

John B. Morris, Jr.
Center for Democracy & Technology
1634 I Street NW, Suite 1100
Washington, D.C. 20006 USA
mél : jmorris@cdt.org
URI: http://www.cdt.org

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 5707
Concord, CA 94520 USA
mél : jon.peterson@neustar.biz
URI: http://www.neustar.biz/

Deirdre K. Mulligan
Samuelson Law, Technology & Public Policy Clinic
Boalt Hall School of Law
University of California
Berkeley, CA 94720 USA
mél : dmulligan@law.berkeley.edu
URI: http://www.law.berkeley.edu/cenpro/samuelson/

Michelle Engelhardt Danley
Samuelson Law, Technology & Public Policy Clinic
Boalt Hall School of Law
University of California
Berkeley, CA 94720
mél : mre213@nyu.edu
URI : http://www.law.berkeley.edu/cenpro/samuelson/

11. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.